

การพัฒนาแอปพลิเคชันที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง



บทคัดย่อและแฟ้มข้อมูลฉบับเต็มของวิทยานิพนธ์ตั้งแต่ปีการศึกษา 2554 ที่ให้บริการในคลังปัญญาจุฬาฯ (CUIR)
เป็นแฟ้มข้อมูลของนิสิตเจ้าของวิทยานิพนธ์ ที่ส่งผ่านทางบัณฑิตวิทยาลัย

The abstract and full text of theses from the academic year 2011 in Chulalongkorn University Intellectual Repository (CUIR)
are the thesis authors' files submitted through the University Graduate School.

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2557
ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

PRIVACY-AWARE APPLICATION DEVELOPMENT FOR INFORMATION CENTRAL
REPOSITORY

Mr. Yotsapon Lertladechanon



A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Software Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2014
Copyright of Chulalongkorn University

หัวข้อวิทยานิพนธ์	การพัฒนาแอปพลิเคชันที่ตระหนักถึงไพรเวซีสำหรับคลัง สารสนเทศกลาง
โดย	นายยศพนธ์ เลิศห้ำาเดชานนท์
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้หัวข้อวิทยานิพนธ์ฉบับนี้เป็นส่วน
หนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.บัณฑิต เอื้ออาภรณ์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(รองศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล)

.....กรรมการ
(รองศาสตราจารย์ ดร.พรศิริ หมั่นไชยศรี)

.....กรรมการภายนอกมหาวิทยาลัย
(ดร.เฉลิมศักดิ์ เลิศวงศ์เสถียร)

ยศพนธ์ เลิศหล้าเดชาขนนท์ : การพัฒนาแอปพลิเคชันที่ตระหนักถึงไพรเวซีสำหรับคลัง
 สารสนเทศกลาง (PRIVACY-AWARE APPLICATION DEVELOPMENT FOR
 INFORMATION CENTRAL REPOSITORY) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. นครทิพย์
 พร้อมพูล, 220 หน้า.

การจัดการคลังสารสนเทศกลางมีวัตถุประสงค์หลักคือ จัดเก็บข้อมูลที่รวบรวมมาจากหลาย
 แหล่ง ประมวลผล และนำเสนอรายงานอย่างเหมาะสม ตามความต้องการของผู้ใช้งานในบทบาทที่
 แตกต่างกันไป เช่น ผู้บริหาร นักวิจัย นักพัฒนา เป็นต้น หนึ่งในปัจจัยสำคัญที่ผู้บริหารคลังสารสนเทศ
 กลางต้องนำมาพิจารณาคือ การรักษาไพรเวซีของข้อมูลเพื่อป้องกันการเข้าถึงและการนำข้อมูลในคลัง
 สารสนเทศกลางไปใช้งานโดยไม่ได้รับอนุญาต

งานวิจัยนี้นำเสนอการพัฒนาแอปพลิเคชันที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง
 ซึ่งเป็นเครื่องมือสนับสนุนการจัดการคลังสารสนเทศกลาง โดยการประยุกต์ใช้แนวปฏิบัติจากกรอบ
 งานพีดีพีไอเอ ที่เหมาะสมกับบริบทของคลังสารสนเทศกลางของหน่วยงานเป้าหมาย เพื่อนำมา
 สร้างเป็นนโยบายและแนวปฏิบัติการใช้งานคลังสารสนเทศกลาง ฟังก์ชันหลักที่ได้รับจากการใช้งาน
 เครื่องมือสนับสนุน เช่น กำหนดสิทธิของผู้ใช้งานจากนโยบายการใช้งานคลังสารสนเทศกลางของ
 องค์กร กำหนดบทบาทของผู้ใช้งานในการเข้าถึงข้อมูล กำหนดระยะเวลาการรักษาข้อมูลที่อยู่ในคลัง
 สารสนเทศกลาง อนุญาตหรือปฏิเสธการนำข้อมูลไปใช้งานโดยเจ้าของข้อมูลจากการร้องขอ เป็นต้น
 วิธีการการพัฒนาแอปพลิเคชันนี้สามารถนำไปประยุกต์ใช้กับคลังสารสนเทศกลางสำหรับสารสนเทศ
 ประเภทอื่นๆ ได้

จุฬาลงกรณ์มหาวิทยาลัย
 CHULALONGKORN UNIVERSITY

ภาควิชา วิศวกรรมคอมพิวเตอร์

ลายมือชื่อนิสิต

สาขาวิชา วิศวกรรมซอฟต์แวร์

ลายมือชื่อ อ.ที่ปรึกษาหลัก

ปีการศึกษา 2557

5470199521 : MAJOR SOFTWARE ENGINEERING

KEYWORDS: PRIVACY / POLICY / PRIVACY BY DESIGN / INFORMATION CENTRAL REPOSITORY

YOTSAPON LERTLADECHANON: PRIVACY-AWARE APPLICATION DEVELOPMENT FOR INFORMATION CENTRAL REPOSITORY. ADVISOR: ASST. PROF. NAKORNTHIP PROMPOON, 220 pp.

The main purpose of information central repository management is to capture data from various sources, processes and present appropriate reports to meet the user requirements in different roles such as manager, researcher and developer. One of the main important factors that the information central repository administrators must consider is maintaining data privacy to prevent unauthorized access and use of data.

This research proposes the development of a privacy-aware application for information central repository as a supporting tool for management by applying appropriate guidelines from the PBDPIA framework for target organization database context to create the data privacy policies and practices for information central repository usage. The main functions obtained from using this supporting tool include abilities to specify user privileges based on central information repository usage policy of the organization, to identify user role for data access, to define the period for retaining data in the information central database, and to allow data owner to allow or deny data usage from requests. The development method of this application may be applied to other types of information central repository.

Department: Computer Engineering Student's Signature

Field of Study: Software Engineering Advisor's Signature

Academic Year: 2014

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ประสบความสำเร็จและครบถ้วนสมบูรณ์ได้ด้วยความร่วมมือและความช่วยเหลือจาก ผู้ช่วยศาสตราจารย์นครทิพย์ พร้อมพูล ผู้ซึ่งเป็นอาจารย์ที่ปรึกษาที่คอยให้คำปรึกษาทั้งทางด้านวิชาการและความรู้ต่างๆ รวมไปถึงจนกระทั่งด้านคุณธรรมจริยธรรม ซึ่งถือเป็นสิ่งสำคัญที่ทำให้งานวิจัยและวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้

ขอขอบพระคุณ รองศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ ประธานกรรมการสอบวิทยานิพนธ์ รองศาสตราจารย์ ดร.พรศิริ หมื่นไชยศรี และ ดร.เฉลิมศักดิ์ เลิศวงศ์เสถียร กรรมการสอบวิทยานิพนธ์ สำหรับข้อชี้แนะและแนวทางต่างๆ ที่ช่วยเพิ่มพูนให้งานวิจัยมีคุณภาพและประสิทธิภาพที่ดีขึ้น

ขอขอบพระคุณคณาจารย์ในภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่าน ที่ให้ความรู้และคำสั่งสอนแก่ผู้วิจัย

ขอขอบคุณบุคลากรในภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่าน ที่คอยให้ข้อมูล คำปรึกษา และความช่วยเหลือต่างๆ ในระหว่างการสอบวิทยานิพนธ์ให้สำเร็จลุล่วงไปด้วยดี

ขอขอบคุณ ผู้บังคับบัญชา เพื่อนร่วมงานที่สถาบันสารสนเทศทรัพยากรน้ำและการเกษตร (องค์การมหาชน) เพื่อนๆ พี่ๆ และน้องๆ ทุกคน ที่คอยให้กำลังใจและอยู่เคียงข้างผู้วิจัยเสมอมา ซึ่งเป็นสิ่งสำคัญที่ส่งผลให้ผู้วิจัยสามารถทำงานวิจัยได้สำเร็จดังที่ปรารถนา

ขอขอบพระคุณพระเจ้าที่ทรงประทานสติปัญญา เรี่ยวแรงกำลัง คำอวยพร ทุกสิ่งอย่างสุดท้ายนี้ ขอกราบขอบพระคุณบิดา มารดา พี่สาว ที่คอยสนับสนุนและให้กำลังใจแก่ผู้วิจัยเสมอมา

สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	ง
บทคัดย่อภาษาอังกฤษ.....	จ
กิตติกรรมประกาศ.....	ฉ
สารบัญ.....	ช
สารบัญตาราง.....	ฅ
สารบัญรูป.....	ฉม
บทที่ 1 บทนำ.....	1
1.1 ความสำคัญและที่มาของปัญหา.....	1
1.2 ปัญหาของงานวิจัย.....	2
1.3 วัตถุประสงค์ของงานวิจัย.....	2
1.4 ขอบเขตของงานวิจัย.....	2
1.5 ประโยชน์ของงานวิจัย.....	4
1.6 ขั้นตอนและวิธีการดำเนินการวิจัย.....	4
1.7 โครงสร้างของเนื้อหาวิทยานิพนธ์.....	4
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง.....	5
2.1 ทฤษฎีที่เกี่ยวข้อง.....	5
2.1.1 สารสนเทศด้านไพรเวซี.....	5
2.1.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.....	6
2.1.3 โพรไฟล์ความมั่นคงและไพรเวซี.....	6
2.1.4 มาตรฐานไพรเวซีระดับสากลหรือจีพีเอส (The Global Privacy Standard: GPS).....	7
2.1.5 กรอบการทำงานพื้นฐานสำหรับไพรเวซีบายดีไซน์ การประเมินผลกระทบไพรเวซี.....	11
2.1.6 สถาปัตยกรรมองค์กรของรัฐบาลกลาง ความมั่นคงและโพรไฟล์ไพรเวซี.....	13

2.2 งานวิจัยที่เกี่ยวข้อง.....	16
2.2.1 การควบคุมการเข้าถึงตามบทบาท	16
2.2.2 การควบคุมการเข้าถึงตามบทบาทด้านไฟเวซี.....	19
2.2.3 การรักษาไฟเวซีของคลังข้อมูลสำหรับบูรณาการข้อมูลผ่านบริการใช้ข้อมูลร่วมกัน ..	22
บทที่ 3 การสร้างนโยบายการใช้งานที่ตระหนักถึงไฟเวซี	24
3.1 การศึกษาระบบงานปัจจุบัน.....	24
3.1.1 กระบวนการรวบรวมและการเชื่อมโยงข้อมูลในคลังสารสนเทศกลาง	24
3.1.2 กระบวนการเชื่อมโยงนำเข้าข้อมูลในคลังสารสนเทศกลาง	24
3.1.3 กระบวนการแปลงข้อมูลให้อยู่ในรูปแบบเดียวกันเพื่อพร้อมใช้งาน	25
3.1.4 การให้บริการข้อมูล	25
3.1.5 สรุปปัญหาจากการศึกษาระบบงานคลังสารสนเทศกลางปัจจุบัน	26
3.2 ขั้นตอนการทำงานวิจัย.....	26
3.3 การสร้างนโยบายการใช้งานที่ตระหนักถึงไฟเวซีสำหรับคลังสารสนเทศกลาง	32
3.3.1 ข้อมูลนำเข้า.....	32
3.3.2 ขั้นตอนการสร้างนโยบายการใช้งานคลังสารสนเทศกลาง	33
3.3.3 ข้อมูลนำออก	41
3.4 วิเคราะห์ออกแบบและพัฒนาเครื่องมือสนับสนุน	42
3.5 การสกัดเอนทิตีและจัดเก็บนโยบาย	45
3.6 สรุปผลการประยุกต์แนวปฏิบัติพีพีไอเอกับคลังสารสนเทศกลาง	48
บทที่ 4 การวิเคราะห์ออกแบบและพัฒนาเครื่องมือสนับสนุน.....	49
4.1 การวิเคราะห์ความต้องการของเครื่องมือสนับสนุน.....	49
4.1.1 รายการความต้องการเชิงหน้าที่ของเครื่องมือสนับสนุน	52
4.1.2 รายการความต้องการเชิงคุณภาพของเครื่องมือสนับสนุน	53

4.2 การออกแบบและพัฒนาเครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลาง.....	53
4.2.1 การกำหนดสิทธิผู้ใช้งานเครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลาง.....	53
4.2.2 การออกแบบฟังก์ชันงานเครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลาง.....	55
4.2.3 การออกแบบเชิงโครงสร้างของเครื่องมือสนับสนุนโดยใช้แผนภาพคลาส.....	58
4.2.4 สถาปัตยกรรมการออกแบบที่ใช้ในการพัฒนาเครื่องมือสนับสนุน	59
4.2.5 เครื่องมือที่ใช้ในการออกแบบและพัฒนาเครื่องมือสนับสนุนคลังสารสนเทศกลาง.....	63
4.2.6 แบบจำลองข้อมูลในการอิมพลีเมนต์ของเครื่องมือสนับสนุนคลังสารสนเทศกลาง.....	63
4.2.7 การออกแบบฟังก์ชันงานและส่วนต่อประสานผู้ใช้งาน	66
4.3 การทดสอบเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา	74
4.3.1 การทดสอบเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางระดับหน่วยย่อย.....	74
4.3.2 การทดสอบเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางระดับรวมหน่วย	76
4.3.3 การทดสอบเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางระดับระบบ	78
4.3.4 ผลการทดสอบเครื่องมือสนับสนุนคลังสารสนเทศกลาง	81
บทที่ 5 สรุปผลการวิจัย.....	82
5.1 สรุปผลการวิจัย.....	82
5.2 ข้อจำกัด.....	83
5.3 งานวิจัยในอนาคต.....	83
5.4 ผลงานตีพิมพ์จากวิทยานิพนธ์.....	84
ภาคผนวก ก อภิธานศัพท์และรายการความต้องการของเครื่องมือสนับสนุน	85
ภาคผนวก ข คำอธิบายตารางแบบจำลองข้อมูล.....	89
ภาคผนวก ค ส่วนต่อประสานของเครื่องมือสนับสนุน.....	102
ค.1 ส่วนต่อประสานเครื่องมือสนับสนุนหลังบ้านสำหรับเจ้าหน้าที่คลังสารสนเทศกลาง	102
ค.2 ส่วนต่อประสานสำหรับผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลาง	118

ภาคผนวก ง รายการคำถามพีบีดีพีไอเอ.....	125
ง.1 รายการแนวปฏิบัติพีบีดีพีไอเอ.....	125
ง.2 ตารางรายการแนวปฏิบัติที่ผ่านการพิจารณาประยุกต์ใช้กับคลังสารสนเทศกลาง	137
ง.3 ฟังก์ชันงานเครื่องมือสนับสนุนที่อิมพลีเมนต์ตามรายการแนวปฏิบัติพีบีดีพีไอเอ.....	174
ง.4 แผนภาพคลาสและคำอธิบายที่ผ่านการวิเคราะห์จากรายการแนวปฏิบัติพีบีดีพีไอเอ.....	194
ภาคผนวก จ ตัวอย่างคำอธิบายแผนภาพยูสเคส.....	207
รายการอ้างอิง	218
ประวัติผู้เขียนวิทยานิพนธ์	220



สารบัญตาราง

ตารางที่ 2.1 อธิบายคลาสมาตรฐานไพโรเวซีระดับสากลจากรูปที่ 2.1.....	9
ตารางที่ 2.2 อธิบายคลาสพีบีดีจากรูปที่ 2.1	10
ตารางที่ 2.3 หลักการปฏิบัติเกี่ยวกับสารสนเทศที่เป็นธรรม [6]	15
ตารางที่ 3.1 ตัวอย่างแนวปฏิบัติที่สอดคล้องกับบริบทคลังสารสนเทศกลาง	35
ตารางที่ 3.2 ตัวอย่างลักษณะข้อมูลที่จัดเก็บในคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา.....	37
ตารางที่ 3.3 ตัวอย่างนโยบายการใช้งานคลังสารสนเทศกลางเบื้องต้นของหน่วยงานกรณีศึกษา	38
ตารางที่ 3.4 ตัวอย่างกลุ่มผู้ใช้งานในคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา.....	38
ตารางที่ 3.5 ตัวอย่างร่างนโยบายการใช้งานคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา.....	39
ตารางที่ 3.6 ตัวอย่างนโยบายการใช้งานคลังสารสนเทศกลางของหน่วยงานหน่วยงานกรณีศึกษา ..	41
ตารางที่ 3.7 พังก์ชันงานเครื่องมือสนับสนุนและนโยบายการใช้งานคลังสารสนเทศกลาง.....	43
ตารางที่ 3.8 ตัวอย่างการสกัดเอนทิตีนโยบายการใช้งานคลังสารสนเทศกลางของหน่วยงาน กรณีศึกษา.....	47
ตารางที่ 3.9 สรุปการรายการแนวปฏิบัติที่นำประยุกต์ใช้กับคลังสารสนเทศกลางจากรายการ ง.2.....	48
ตารางที่ 4.1 ตัวอย่างรายการความต้องการเชิงหน้าที่ของเครื่องมือสนับสนุนคลังสารสนเทศกลาง ของหน่วยงานกรณีศึกษา.....	52
ตารางที่ 4.2 รายการความต้องการเชิงคุณภาพของเครื่องมือสนับสนุนคลังสารสนเทศกลางของ หน่วยงานกรณีศึกษา.....	53
ตารางที่ 4.3 กลุ่มผู้ใช้งาน บทบาท สิทธิของผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลาง.....	54
ตารางที่ 4.4 คำอธิบายแผนภาพคลาสเครื่องมือสนับสนุนจากรูปที่ 4.5.....	58
ตารางที่ 4.5 รายละเอียดสถาปัตยกรรมการออกแบบเอ็มวีซี.....	59
ตารางที่ 4.6 ตัวอย่างรายละเอียดสถาปัตยกรรมเอ็มวีซีของเครื่องมือสนับสนุนคลังสารสนเทศ กลาง	60
ตารางที่ 4.7 ชื่อตารางและคำอธิบายในการอิมพลีเมนต์ระบบ	65
ตารางที่ 4.8 บทบาทผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลาง	67

ตารางที่ 4.9 ความสัมพันธ์ระหว่างผู้ใช้งานและฟังก์ชันงานของเครื่องมือสนับสนุน	67
ตารางที่ 4.10 ตัวอย่างกรณีการบันทึกนโยบายการใช้งานเข้าสู่ระบบ	75
ตารางที่ 4.11 ตัวอย่างกรณีทดสอบการค้นหานโยบายโดยระบุค่าค้นหา	76
ตารางที่ 4.12 ตัวอย่างกรณีทดสอบการบันทึกประวัติข้อมูล	77
ตารางที่ 4.13 ตัวอย่างกรณีทดสอบการบันทึกเข้ารับการอบรม.....	78
ตารางที่ 4.14 ตัวอย่างกรณีทดสอบระบบการมอบหมายสิทธิให้ผู้ใช้งาน.....	79
ตารางที่ 4.15 ตัวอย่างกรณีทดสอบระบบการร้องขอข้อมูล.....	80
ตารางที่ 4.16 สรุปผลตัวอย่างการทดสอบหน้าที่การทำงานของระบบ	81
ตารางที่ ก.1 อภิธานศัพท์.....	85
ตารางที่ ก.2 รายการความต้องการของเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงาน กรณีศึกษา.....	85
ตารางที่ ข.1 โครงสร้างตารางข้อมูล tbl_user_training.....	89
ตารางที่ ข.2 โครงสร้างตารางข้อมูล tbl_logs	89
ตารางที่ ข.3 โครงสร้างตารางข้อมูล tbl_privacy.....	90
ตารางที่ ข.4 โครงสร้างตารางข้อมูล tbl_role_user.....	90
ตารางที่ ข.5 โครงสร้างตารางข้อมูล tbl_training	91
ตารางที่ ข.6 โครงสร้างตารางข้อมูล tbl_usergroup	91
ตารางที่ ข.7 โครงสร้างตารางข้อมูล tbl_user.....	92
ตารางที่ ข.8 โครงสร้างตารางข้อมูล tbl_agency.....	93
ตารางที่ ข.9 โครงสร้างตารางข้อมูล tbl_retain	93
ตารางที่ ข.10 โครงสร้างตารางข้อมูล tbl_schedule.....	94
ตารางที่ ข.11 โครงสร้างตารางข้อมูล tbl_dispose.....	94
ตารางที่ ข.12 โครงสร้างตารางข้อมูล tbl_department.....	95
ตารางที่ ข.13 โครงสร้างตารางข้อมูล tbl_transfer.....	95

ตารางที่ ข.14	โครงสร้างตารางข้อมูล tbl_role	96
ตารางที่ ข.15	โครงสร้างตารางข้อมูล tbl_role_policy	96
ตารางที่ ข.16	โครงสร้างตารางข้อมูล tbl_policy.....	96
ตารางที่ ข.17	โครงสร้างตารางข้อมูล tbl_rbac_policy.....	97
ตารางที่ ข.18	โครงสร้างตารางข้อมูล tbl_purpose.....	97
ตารางที่ ข.19	โครงสร้างตารางข้อมูล tbl_data	97
ตารางที่ ข.20	โครงสร้างตารางข้อมูล tbl_frequencydata	98
ตารางที่ ข.21	โครงสร้างตารางข้อมูล tbl_action	98
ตารางที่ ข.22	โครงสร้างตารางข้อมูล tbl_ministry	98
ตารางที่ ข.23	โครงสร้างตารางข้อมูล tbl_disclose.....	99
ตารางที่ ข.24	โครงสร้างตารางข้อมูล tbl_frequency	99
ตารางที่ ข.25	โครงสร้างตารางข้อมูล tbl_condition	100
ตารางที่ ข.26	โครงสร้างตารางข้อมูล tbl_src_table.....	100
ตารางที่ ข.27	โครงสร้างตารางข้อมูล tbl_src_field	101
ตารางที่ ข.28	โครงสร้างตารางข้อมูล tbl_obligation.....	101
ตารางที่ ค.1	ฟังก์ชันการใช้งานส่วนการจัดการหลังบ้านของเจ้าหน้าที่คลังสารสนเทศกลาง	102
ตารางที่ ค.2	ฟังก์ชันการใช้งานสำหรับผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลาง	118
ตารางที่ ง.1	รายการแนวปฏิบัติพีบีดีพีไอเอ	125
ตารางที่ ง.2	แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีดีรวมไปถึงเหตุผลและประโยชน์	138
ตารางที่ ง.3	แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.40 ด้าน Proactive not Reactive.....	194
ตารางที่ ง.4	แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.41 ด้าน Privacy as Default	197
ตารางที่ ง.5	แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.42 ด้าน Embedded into Design.....	198
ตารางที่ ง.6	แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.43 ด้าน Positive-Sum	200
ตารางที่ ง.7	แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.44 ด้าน Full Life Cycle Protection	202

ตารางที่ ง.8 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.45 ด้าน Visibility and Transparency ..	203
ตารางที่ ง.9 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.46 ด้าน Respect for User Privacy	205
ตารางที่ จ.1 คำอธิบายแผนภาพยูสเคสบันทึกคำร้องขอส่งต่อข้อมูล.....	207
ตารางที่ จ.2 คำอธิบายแผนภาพยูสเคสสกัดเอาต์นโยบายการใช้งานคลังสารสนเทศกลาง	208
ตารางที่ จ.3 คำอธิบายแผนภาพยูสเคสการเรียกดูข้อมูล	209
ตารางที่ จ.4 คำอธิบายแผนภาพยูสเคสการบันทึกมอบหมายสิทธิบทบาท.....	210
ตารางที่ จ.5 คำอธิบายแผนภาพยูสเคสการบันทึกค่าไพรเวซีข้อมูลเริ่มต้น.....	211
ตารางที่ จ.6 คำอธิบายแผนภาพยูสเคสการกำหนดผู้รับผิดชอบนโยบาย	212
ตารางที่ จ.7 คำอธิบายแผนภาพยูสเคสการสร้างหลักสูตรอบรม	213
ตารางที่ จ.8 คำอธิบายแผนภาพยูสเคสบันทึกเข้ารับการอบรม	214
ตารางที่ จ.9 คำอธิบายแผนภาพยูสเคสการบันทึกการเก็บรักษาและทำลายข้อมูล	215
ตารางที่ จ.10 คำอธิบายแผนภาพยูสเคสการบันทึกนโยบายการใช้งาน	216

สารบัญรูป

รูปที่ 2.1	ภาพรวมของจีพีเอสและการพัฒนาต่อยอดของพีบีดี	9
รูปที่ 2.2	ภาพรวมกรอบการทำงานของพีบีดี [8]	12
รูปที่ 2.3	กลุ่มของรูปแบบอาร์บีเอซี [10].....	17
รูปที่ 2.4	แบบจำลองอาร์บีเอซี [10]	18
รูปที่ 2.5	แนวความคิดของแบบจำลอง พีอาร์บีเอซี [11].....	19
รูปที่ 2.6	ภาพรวมงานวิจัยการรักษาไพรเวซีของคลังข้อมูล [12].....	22
รูปที่ 3.1	ภาพรวมการเชื่อมโยงข้อมูลสำหรับคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา.....	25
รูปที่ 3.2	โครงสร้างองค์กรและภาระหน้าที่ของกรณีศึกษาคลังสารสนเทศกลาง	27
รูปที่ 3.3	แนวคิดการสร้างและการนำนโยบายการใช้งานคลังสารสนเทศกลางไปใช้งาน.....	31
รูปที่ 3.4	ภาพรวมการสร้างนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี.....	32
รูปที่ 3.5	กิจกรรมการสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซี	34
รูปที่ 4.1	ขั้นตอนวิเคราะห์ออกแบบและพัฒนาเครื่องมือสนับสนุน.....	49
รูปที่ 4.2	การวิเคราะห์รายการความต้องการของเครื่องมือสนับสนุน	50
รูปที่ 4.3	บทบาทผู้ใช้งานเครื่องมือสนับสนุนการใช้งานคลังสารสนเทศกลาง	54
รูปที่ 4.4	แผนภาพยูสเคสของเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลาง	57
รูปที่ 4.5	แผนภาพคลาสของเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลาง.....	58
รูปที่ 4.6	ความสัมพันธ์ระหว่างเอนทิตีของเครื่องมือสนับสนุนคลังสารสนเทศกลาง	64
รูปที่ 4.7	ขั้นตอนการสกัดเอนทิตีนโยบายการใช้งานคลังสารสนเทศกลาง	69
รูปที่ 4.8	การจัดเตรียมบทบาทผู้ใช้งานเครื่องมือสนับสนุน	70
รูปที่ 4.9	รายการผู้ใช้งานเครื่องมือสนับสนุนทั้งหมด	71
รูปที่ 4.10	รายชื่อผู้รับผิดชอบนโยบายการใช้งานคลังสารสนเทศกลาง	71
รูปที่ 4.11	รายชื่อหน่วยงานเชื่อมโยงข้อมูลในคลังสารสนเทศกลาง	72
รูปที่ 4.12	การเรียกดูข้อมูลในคลังสารสนเทศกลางตามบทบาทนักวิจัย.....	73

รูปที่ 4.13 ตัวอย่างการร้องขอข้อมูลเปิดเผยข้อมูลผ่านเครื่องมือสนับสนุน.....	73
รูปที่ 4.14 รายการผลการพิจารณาการร้องขอข้อมูล.....	74
รูปที่ ค.1 การค้นหาตามบทบาท	104
รูปที่ ค.2 การค้นหาตามข้อมูล	104
รูปที่ ค.3 แสดงการค้นหาตามหน่วยงาน	105
รูปที่ ค.4 หน้านโยบายคลังสารสนเทศกลาง.....	106
รูปที่ ค.5 ขั้นตอนการสกัดเอนทิตีนโยบายการใช้งาน	107
รูปที่ ค.6 การจัดเตรียมบทบาทผู้ใช้งานในคลังสารสนเทศกลาง	108
รูปที่ ค.7 รายการผู้ใช้งานในคลังสารสนเทศกลางทั้งหมด.....	109
รูปที่ ค.8 รายชื่อผู้รับผิดชอบนโยบายในคลังสารสนเทศกลาง	109
รูปที่ ค.9 รายชื่อหน่วยงานทั้งหมดในคลังสารสนเทศกลาง.....	110
รูปที่ ค.10 สถิติการใช้งานคลังสารสนเทศกลาง.....	111
รูปที่ ค.11 รายงานการใช้งานคลังสารสนเทศกลาง	111
รูปที่ ค.12 หน้าตารางการอบรม	112
รูปที่ ค.13 การตั้งค่าโปรเวซี	113
รูปที่ ค.14 การตั้งค่าความมั่นคง	114
รูปที่ ค.15 การตั้งค่าบัญชี	114
รูปที่ ค.16 ตารางพีบีดีพีไอเอ	115
รูปที่ ค.17 ข้อมูลช่วยเหลือในการใช้งานคลังสารสนเทศกลาง	116
รูปที่ ค.18 ฟังก์ชันงานในคลังสารสนเทศกลาง.....	117
รูปที่ ค.19 หน้าค้นหาผู้ใช้ในระบบตามบทบาทของผู้ใช้งาน	119
รูปที่ ค.20 หน้าค้นหาหน่วยงานตามชื่อข้อมูล.....	119
รูปที่ ค.21 หน้าค้นหาข้อมูลตามหน่วยงาน.....	120
รูปที่ ค.22 การเรียกดูข้อมูลตามบทบาทนักวิจัย.....	121

รูปที่ ค.23 ตัวอย่างการร้องขอข้อมูล.....	121
รูปที่ ค.24 รายการคำร้องขอข้อมูล.....	122
รูปที่ ค.25 หน้าพิจารณาคำร้องขอข้อมูล	122
รูปที่ ค.26 รายการผลการพิจารณาการร้องขอข้อมูล	123
รูปที่ ค.27 รายการหลักสูตรอบรม	124
รูปที่ ค.28 หน้าการตั้งค่าความมั่นคง	124
รูปที่ ง.1 การมอบหมายบุคคลให้ทำหน้าที่ด้านต่างๆ.....	174
รูปที่ ง.2 อพฺโหลตเอกสารความมุ่งมั่นว่าได้รับความร่วมมือจากกลุ่มผู้ใช้งานและผู้ส่วนได้เสีย	174
รูปที่ ง.3 บุคคลที่เกี่ยวข้องยอมรับข้อตกลงการใช้งาน.....	175
รูปที่ ง.4 อพฺโหลตเอกสารเกี่ยวข้องกับการรักษาความลับในคลังสารสนเทศกลาง.....	175
รูปที่ ง.5 รายการเอกสารที่อพฺโหลตเพื่อให้ผู้เกี่ยวข้องรับทราบ	176
รูปที่ ง.6 รายการเอกสารเผยแพร่ส่วนผู้ใช้งาน	177
รูปที่ ง.7 จัดทำหลักสูตรอบรมพร้อมกำหนดกลุ่มผู้รับการอบรม แนบเอกสารคำสั่งการอบรม.....	177
รูปที่ ง.8 รายการหัวข้ออบรมพร้อมเอกสารแนบ.....	178
รูปที่ ง.9 แสดงรายการสิทธิบทบาท ขอบเขตการใช้งาน.....	178
รูปที่ ง.10 กำหนดโปรเวซีค่าเริ่มต้นสำหรับใช้งานคลังสารสนเทศกลาง.....	179
รูปที่ ง.11 กำหนดบทบาทให้กับผู้ใช้งาน.....	179
รูปที่ ง.12 การสร้างรหัสผ่านที่ยากต่อการคาดเดา	180
รูปที่ ง.13 คำแนะนำในการสร้างรหัสผ่านที่ยากต่อการคาดเดา.....	180
รูปที่ ง.14 ผู้ใช้งานสามารถเพิกถอนการยินยอมการใช้งานข้อมูล	181
รูปที่ ง.15 อภิธานศัพท์ที่ใช้ในคลังสารสนเทศกลาง.....	181
รูปที่ ง.16 ฟังก์ชันงานของแอปพลิเคชัน	182
รูปที่ ง.17 รายการบันทึกประวัติการใช้งานและการเข้าถึงข้อมูล.....	182
รูปที่ ง.18 กำหนดช่วงเวลาการเก็บรักษาข้อมูล	183

รูปที่ ง.19 แสดงช่วงเวลาการเก็บรักษาข้อมูลเพื่อให้ผู้ใช้งานรับทราบ	183
รูปที่ ง.20 รายการนโยบายการใช้งานข้อมูล	184
รูปที่ ง.21 แสดงรายการข้อมูล หน่วยงานที่จัดเก็บในคลังสารสนเทศกลาง.....	184
รูปที่ ง.22 ขั้นตอนในการร้องขอข้อมูลจากหน่วยงานเจ้าของข้อมูล.....	185
รูปที่ ง.23 เจ้าของข้อมูลพิจารณาเพื่อดำเนินการต่อคำร้องขอ	185
รูปที่ ง.24 ช่องทางการติดต่อกับเจ้าหน้าที่ในองค์กรที่รับผิดชอบด้านนโยบาย	186
รูปที่ ง.25 อพฺโหลตเอกสารขั้นตอนการรักษาความลับและข้อกำหนดการแบ่งปันข้อมูลคลัง สารสนเทศกลาง	186
รูปที่ ง.26 อพฺโหลตเอกสารชี้แจงช่วงเวลากำหนดบทวนนโยบายความเป็นส่วนตัวและความมั่นคงในคลัง สารสนเทศกลาง	187
รูปที่ ง.27 อพฺโหลตเอกสารแผนงานโครงการการพัฒนา ไร้ดีไซน์เทคโนโลยีของคลังสารสนเทศ กลาง	187
รูปที่ ง.28 อพฺโหลตเอกสารมาตรฐานสำหรับการประเมินการออกแบบด้านความเป็นส่วนตัว.....	188
รูปที่ ง.29 อพฺโหลต เอกสารขั้นตอนการดำเนินการประเมินการตรวจสอบการปฏิบัติตาม นโยบายความเป็นส่วนตัวและความมั่นคงของคลังสารสนเทศกลาง.....	188
รูปที่ ง.30 อพฺโหลตเอกสารตรวจสอบด้านความเป็นส่วนตัวและความมั่นคง.....	189
รูปที่ ง.31 อพฺโหลตเอกสารการออกแบบและสถาปัตยกรรมเทคโนโลยีสารสนเทศ กระบวนการ ทางธุรกิจของคลังสารสนเทศกลาง	189
รูปที่ ง.32 อพฺโหลตเอกสารชี้แจงวัตถุประสงค์การเก็บข้อมูลในคลังสารสนเทศกลาง.....	190
รูปที่ ง.33 อพฺโหลต เอกสารตรวจสอบการใช้ข้อมูลและวัตถุประสงค์ที่กำหนด	190
รูปที่ ง.34 อพฺโหลตเอกสารข้อกำหนดการขอใช้งานข้อมูลในคลังสารสนเทศกลางสำหรับ บุคคลภายนอก.....	191
รูปที่ ง.35 อพฺโหลต เอกสารตัวชี้วัดประโยชน์การใช้งานข้อมูลและวัตถุประสงค์ของคลัง สารสนเทศกลาง.....	191
รูปที่ ง.36 อพฺโหลตเอกสารประเมินความเสี่ยง	192

รูปที่ ง.37 อัปโหลดเอกสารชี้แจงสิทธิเพื่อทำการเพิกถอน ระบุการใช้งานและเปิดเผยข้อมูลใน
คลังสารสนเทศกลาง และขั้นตอนการร้องเรียนด้านไอพีแอสซี..... 192

รูปที่ ง.38 อัปโหลดเอกสารประเมินความถูกต้องของข้อมูล 193

รูปที่ ง.39 อัปโหลดเอกสารผลการประเมินความคาดหวังของผู้ให้ข้อมูลแก่คลังสารสนเทศกลาง . 193

รูปที่ ง.40 แผนภาพคลาสหลักการที่ 1 Proactive not Reactive 194

รูปที่ ง.41 แผนภาพคลาสหลักการที่ 2 Privacy as Default 196

รูปที่ ง.42 แผนภาพคลาสหลักการที่ 3 Embedded into Design 198

รูปที่ ง.43 แผนภาพคลาสหลักการที่ 4 Positive-Sum..... 200

รูปที่ ง.44 แผนภาพคลาสหลักการที่ 5 Full Life Cycle Protection 201

รูปที่ ง.45 แผนภาพคลาสหลักการที่ 6 Visibility and Transparency 203

รูปที่ ง.46 แผนภาพคลาสหลักการที่ 7 Respect for User Privacy 204



บทที่ 1 บทนำ

1.1 ความสำคัญและที่มาของปัญหา

การจัดการคลังสารสนเทศกลางมีวัตถุประสงค์หลักคือ จัดเก็บข้อมูลที่รวบรวมมาจากหลายแหล่ง ประมวลผล และนำเสนอรายงานอย่างเหมาะสม ตามความต้องการของผู้ใช้งานในบทบาทที่แตกต่างกัน

ในประเทศไทยมีแหล่งสารสนเทศด้านทรัพยากรน้ำขนาดใหญ่แห่งหนึ่ง ซึ่งต่อไปในงานวิจัยนี้จะเรียกว่า “คลังสารสนเทศกลาง” เป็นแหล่งให้บริการข้อมูลทรัพยากรน้ำเพื่อใช้ในงานวิจัย พัฒนาสร้างเป็นรายงานเพื่อใช้ในการประกอบการตัดสินใจเมื่อเกิดสถานการณ์ภัยพิบัติ [1] โดยมีกลุ่มบุคคลและบทบาทที่ใช้งานแตกต่างกัน เช่น ผู้บริหาร นักวิจัย นักพัฒนา ผู้ดูแลฐานข้อมูล เป็นต้น

การจัดการคลังสารสนเทศกลางที่ให้บริการหลายบริการรวมไปถึงการใช้งานจากผู้เกี่ยวข้องหลายบทบาท ปัญหาที่มักเกิดขึ้นในคลังสารสนเทศกลางเช่น ขาดนโยบายการใช้งานคลังสารสนเทศกลางที่ชัดเจน ขาดการกำหนดบทบาทการเข้าถึงข้อมูลของผู้ใช้งาน ขาดการกำหนดระยะเวลาการเก็บรักษาข้อมูล การนำข้อมูลในคลังสารสนเทศไปใช้งานโดยขาดการยินยอมเห็นชอบจากเจ้าของข้อมูล เป็นสาเหตุให้เกิดผลกระทบระหว่างผู้นำข้อมูลไปใช้งานกับเจ้าของข้อมูลที่ไม่ได้ยินยอมให้นำข้อมูลไปใช้งาน ขาดการตรวจสอบวัตถุประสงค์การเก็บข้อมูลการนำข้อมูลไปใช้งาน สิ่งเหล่านี้ทำให้ผู้บริหารคลังสารสนเทศกลางจำเป็นต้องพิจารณาคือ การสร้างนโยบายการใช้งานข้อมูลในคลังสารสนเทศกลางที่ตระหนักถึงความเป็นส่วนตัวของข้อมูลที่เป็นที่ยอมรับและเป็นมาตรฐาน เพื่อให้ผู้ที่เกี่ยวข้องรับทราบนโยบายดังกล่าวและใช้เป็นแนวทางปฏิบัติในทิศทางเดียวกัน สิ่งที่ต้องพิจารณาต่อมาคือ เมื่อมีนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงความเป็นส่วนตัวแล้ว ทำอย่างไรถึงจะแน่ใจได้ว่านโยบายการใช้งานที่ตระหนักถึงความเป็นส่วนตัวได้ถูกนำไปปฏิบัติใช้งานจริงในคลังสารสนเทศกลาง

จากปัญหาที่กล่าวมางานวิจัยนี้จึงนำเสนอการประยุกต์ใช้กรอบงานพีบีดีพีไอเอซึ่งประกอบด้วยรายการคำถามจากแนวปฏิบัติภายใต้หลักการพีบีดีซึ่งเป็นที่ยอมรับในระดับสากล เพื่อนำมาสร้างเป็นนโยบายการใช้งานที่ตระหนักถึงความเป็นส่วนตัวจากกรณีศึกษาในงานวิจัยนี้คือ คลังสารสนเทศกลางของหน่วยงานแห่งหนึ่ง เพื่อให้เกิดการใช้งานข้อมูลในคลังสารสนเทศกลางตระหนักถึงความเป็นส่วนตัวไปถึงการนำนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงความเป็นส่วนตัวเป็นข้อมูลนำเข้า เพื่อสร้างรายการความต้องการและพัฒนาเป็นแอปพลิเคชันที่ตระหนักถึงความเป็นส่วนตัวหรือเครื่องมือสนับสนุนสำหรับใช้งานในคลังสารสนเทศกลาง

1.2 ปัญหาของงานวิจัย

1. สามารถสร้างนโยบายที่ตระหนักถึงไพรเวซีในคลังสารสนเทศกลางได้อย่างไร
2. สร้างเครื่องมือสนับสนุน เพื่อใช้สำหรับการบังคับใช้นโยบายในคลังสารสนเทศได้อย่างไรในการใช้งานเพื่อให้เกิดความมั่นคงและมีประสิทธิภาพ

1.3 วัตถุประสงค์ของงานวิจัย

1. พัฒนาแอปพลิเคชันที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง ที่เป็นไปตามนโยบายการใช้งานที่กำหนด

1.4 ขอบเขตของงานวิจัย

พัฒนาแอปพลิเคชันที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง โดยประยุกต์ใช้กรอบการทำงานพีบีดีพีไอเอ โดยใช้คลังสารสนเทศกลางเป็นกรณีศึกษาประกอบด้วยความสามารถดังนี้

1. ความสามารถด้านการสนับสนุนการจัดการนโยบายคือ
 - 1.1 เพิ่ม/บันทึก/ค้นหา/แก้ไข นโยบายการใช้งาน
 - 1.2 ยกเลิก/ระงับ ใช้นโยบายการใช้งาน
 - 1.3 สกัดเอนทิตีนโยบายการใช้งาน
 - 1.4 เพิ่ม/บันทึก/แก้ไข/กำหนด ข้อมูลผู้รับผิดชอบนโยบายการใช้งาน
2. ความสามารถด้านการกำหนดค่าพื้นฐานการใช้งานข้อมูลคือ
 - 2.1 เพิ่ม/บันทึก/แก้ไข/กำหนด/ลบ รายการไพรเวซีข้อมูลค่าเริ่มต้น
 - 2.2 เรียกดูข้อมูลในคลังสารสนเทศกลาง
3. ความสามารถด้านการเรียกดูข้อมูลเข้าใช้งานระบบคือ
 - 3.1 บันทึก/ค้นหา รายการเข้าใช้ระบบ
 - 3.2 ออกรายงานการเข้าใช้ระบบ แบบรายวัน หรือกำหนดช่วงระยะเวลา
4. ความสามารถด้านการระบุตัวตนคือ
 - 4.1 บันทึกการลงทะเบียน/ตรวจสอบการเข้าสู่ระบบ เพื่อใช้งานเครื่องมือสนับสนุน
 - 4.2 แก้ไขข้อมูลส่วนตัวผู้ใช้งาน
 - 4.3 กู้รหัสผ่าน/แก้ไขรหัสผ่าน ผู้ใช้งาน

5. ความสามารถด้านการแนะนำรหัสผ่านคือ
 - 5.1 แสดงตัวอย่างรหัสผ่านให้ผู้ใช้งาน
 - 5.2 แสดงคำแนะนำในการสร้างรหัสผ่านที่เข้มแข็ง
 - 5.3 วัดความเข้มแข็งของรหัสผ่าน
6. ความสามารถด้านการสนับสนุนหลักสูตรอบรมด้านไอทีคือ
 - 6.1 เพิ่ม/บันทึก/แก้ไข/ลบ หลักสูตรการอบรม
 - 6.2 กำหนดกลุ่มเป้าหมายของหลักสูตรการอบรม
 - 6.3 บันทึกการเข้ารับหลักสูตรการอบรม
 - 6.4 ออกรายงานหลักสูตรการอบรม
7. ความสามารถด้านการบริหารการเปิดเผยข้อมูลคือ
 - 7.1 บันทึก/อนุมัติ/ตรวจสอบสถานะการพิจารณา/แสดงรายการ/ค้นหา คำร้องการขอใช้ข้อมูล
 - 7.2 แสดงรายงานคำขอใช้ข้อมูลที่ผ่านการพิจารณา
8. ความสามารถด้านการบริหารการส่งต่อข้อมูลคือ
 - 8.1 บันทึก/อนุมัติ/ตรวจสอบสถานะการพิจารณา/แสดงรายการ/ค้นหา คำร้องขอส่งต่อข้อมูล
 - 8.2 แสดงรายการคำขอส่งต่อข้อมูลที่ผ่านการพิจารณา
9. ความสามารถด้านการควบคุมสิทธิและบทบาทคือ
 - 9.1 เพิ่ม/บันทึก/แก้ไข/ลบ สิทธิและบทบาท
 - 9.2 บันทึกมอบหมาย/แก้ไขการมอบหมาย/สามารถตรวจสอบ สิทธิและบทบาท
10. ความสามารถด้านการสร้างตารางรายการสนับสนุนเพื่อการเก็บรักษาและทำลายข้อมูล
 - 10.1 เพิ่ม/บันทึก/แก้ไข/ลบ รายการเก็บรักษาและทำลายข้อมูล
 - 10.2 แสดงรายงานการเก็บรักษาและทำลายข้อมูล

11. ประเมินความถูกต้องของระบบว่าได้นำเอากรอบงานพีบีดีประกอบด้วย 7 หลักการได้ถูกนำมาใช้งาน

1.5 ประโยชน์ของงานวิจัย

1. สามารถนำนโยบายการใช้งานคลังสารสนเทศกลางเป็นตัวกำหนดสิทธิ บทบาท การมอบหมายสิทธิ การเข้าถึงข้อมูลในการใช้งานคลังสารสนเทศกลาง
2. คลังสารสนเทศกลางที่มีแอปพลิเคชันที่ตระหนักถึงไพรเวซี
3. ต้นแบบเครื่องมือสนับสนุนที่เกิดจากกรอบงานพีบีดีพีไอเอเอ เพื่อใช้เป็นแบบอย่างในงานอื่นที่มีลักษณะเดียวกัน

1.6 ขั้นตอนและวิธีการดำเนินการวิจัย

1. ศึกษาและทำความเข้าใจลักษณะการดำเนินงานของคลังสารสนเทศกลาง
2. ศึกษาและวิเคราะห์ประเด็นปัญหาที่ต้องพิจารณาในระบบคลังสารสนเทศกลาง
3. ศึกษาและวิเคราะห์ทำความเข้าใจแนวปฏิบัติที่ระบุในกรอบงานพีบีดีพีไอเอเอ ศึกษางานวิจัยและเอกสารที่เกี่ยวข้องกับไพรเวซี
4. ออกแบบและกำหนดคุณลักษณะภาพรวมของเครื่องมือสนับสนุน
5. เลือกเครื่องมือและพัฒนาระบบตามที่ได้ออกแบบ
6. ทดสอบและประเมินผลวิธีวิจัยและระบบที่พัฒนาขึ้นเพื่อสนับสนุนแนวคิดในงานวิจัยนี้
7. จัดทำและเผยแพร่บทความวิชาการ
8. สรุปผลแนวทางการวิจัยและข้อเสนอแนะ และจัดทำเล่มโครงการ

1.7 โครงสร้างของเนื้อหาวิทยานิพนธ์

เนื้อหาของวิทยานิพนธ์ฉบับนี้แบ่งออกเป็น 5 บทคือ บทที่ 1 เป็นบทนำ บทที่ 2 เป็นการกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง บทที่ 3 เป็นบทที่อธิบายถึงขั้นการสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซี ซึ่งประกอบด้วยกระบวนการสร้างนโยบาย กระบวนการสกัดนโยบาย และกระบวนการสร้างเครื่องมือสนับสนุน บทที่ 4 เป็นบทที่อธิบายการออกแบบและพัฒนาเครื่องมือสนับสนุน และบทที่ 5 เป็นบทสุดท้าย ซึ่งจะเป็นบทสรุปและข้อจำกัดของงานวิจัย รวมทั้งแนวทางการวิจัยในอนาคต และบทความวิชาการที่ตีพิมพ์

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

บทนี้กล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้องประกอบไปด้วย งานวิจัยด้านสารสนเทศด้าน
 ความเป็นส่วนตัว พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โพรไฟล์ความ
 มั่นคงและความเป็นส่วนตัว มาตรฐานความเป็นส่วนตัวระดับสากล กรอบการทำงานพื้นฐานสำหรับความเป็นส่วนตัวดีไซน์
 สถาปัตยกรรมองค์กรของรัฐบาลกลาง ความมั่นคงและโพรไฟล์ความเป็นส่วนตัว การควบคุมการเข้าถึงตาม
 บทบาท การควบคุมการเข้าถึงตามบทบาทด้านความเป็นส่วนตัวและการรักษาความเป็นส่วนตัวของคลังข้อมูลสำหรับ
 บูรณาการข้อมูลผ่านบริการใช้ข้อมูลร่วมกัน เพื่อใช้เป็นความรู้ในการทำวิทยานิพนธ์

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 สารสนเทศด้านความเป็นส่วนตัว

สารสนเทศด้านความเป็นส่วนตัว (Information Privacy) [2] หรือ ข้อมูลส่วนบุคคล (Personal Data) ซึ่ง Clarke [3] ได้ให้นิยามว่าเป็น “สิ่งที่บุคคลให้ความสนใจควบคุม หรือมีอิทธิพลอย่างมี
 นัยสำคัญต่อการจัดการข้อมูลส่วนบุคคล” อีกนิยามที่ Westin [4] ได้ให้ไว้คือ “การอ้างความเป็น
 ส่วนตัวของบุคคล กลุ่ม หรือสถาบันในการจัดการด้วยตัวเอง ไม่ว่าจะเมื่อไร อย่างไร และขอบเขตของ
 ข้อมูลเกี่ยวกับตัวเองที่ใช้ติดต่อกับผู้อื่น” นอกจากนี้ยังมีพระราชบัญญัติด้านความเป็นส่วนตัวของรัฐบาล
 ออสเตรเลีย [2] ที่กล่าวถึงหลักการสารสนเทศด้านความเป็นส่วนตัว ดังนี้คือ

- จะต้องบอกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล
- ต้องแจ้งให้เจ้าของข้อมูลให้รับทราบทั้งการจัดเก็บ การบันทึกข้อมูลส่วนบุคคล
- พุทธถึงการจัดเก็บการรักษาความมั่นคง (Security) ของข้อมูลส่วนบุคคล
- การเข้าถึงข้อมูลส่วนบุคคลจะต้องมีการเก็บบันทึกและใช้งานตามสิทธิที่ได้รับ
- การแก้ไขข้อมูลส่วนบุคคลจะต้องเป็นไปตามวัตถุประสงค์ที่กำหนด
- มีการกำหนดข้อจำกัดในการใช้งานข้อมูลส่วนบุคคล

เมื่อนำเอากรอบการทำงานพีบีดีพีไอเอมาใช้กับคลังสารสนเทศกลางจะเกิดความสอดคล้องกับ
 พระราชบัญญัติด้านความเป็นส่วนตัวของรัฐบาลออสเตรเลียทั้ง 6 ข้อ

ทฤษฎีของสารสนเทศด้านความเป็นส่วนตัว (Theories of Information Privacy) ทฤษฎีการจำกัด
 การเข้าถึง (Restricted Access Theory) [2] เป็นทฤษฎีเกี่ยวกับการจำกัดการเข้าถึงของสารสนเทศ

ด้านไพรเวซี โดยเจ้าของข้อมูลส่วนบุคคลสามารถกำหนดขอบเขต (Limit) หรือจำกัด (Restrict) การเข้าถึงข้อมูลส่วนบุคคล ซึ่งการทำตามทฤษฎีนี้ต้องมีการกำหนดบริเวณหรือโซนให้ชัดเจน ทฤษฎีการควบคุม (The Control Theory) นิยามโดย Rachel กล่าวว่า “ความสามารถในการควบคุมว่าเจ้าของข้อมูลส่วนบุคคลสามารถกำหนดการเข้าถึง ดูแลรักษาข้อมูลส่วนบุคคลได้” ซึ่งในหลักการนี้เป็นที่รู้จักคือการแบ่งเป็นบทบาทหน้าที่ เจ้าของข้อมูลส่วนบุคคลเลือกได้ว่าจะอยู่ในบทบาทไหน แต่ทฤษฎีนี้ยังมีข้อถกเถียงอยู่ เช่น ทฤษฎีนี้ยังไม่ชัดเจนในเรื่องของระดับของการควบคุม และทฤษฎีการควบคุมยังไม่ชัดเจนว่าชนิดของข้อมูลส่วนบุคคลใดบ้างที่จะต้องมีการควบคุม

ทฤษฎีการควบคุมจำกัดการเข้าถึงหรือการกำหนดขอบเขต (The Restricted Access/Limited Control-RALC Theory) [2] ถูกนำเสนอโดย Moor ซึ่งถูกแยกออกเป็นสองแนวความคิดคือ แนวคิดของไพรเวซี (Concept of Privacy) ได้นิยามไว้ว่า “การจำกัดและการกำหนดขอบเขต” และการจัดการของไพรเวซี (Management of Privacy) ซึ่งทำได้โดยการจำกัดการควบคุมการเข้าถึง ส่วนที่สำคัญอีกอย่างคือการกำหนดบริเวณหรือโซน เป็นการกำหนดและจำกัดขอบเขตการเข้าถึงโดยผู้อื่น

2.1.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 [5] ซึ่งได้ประกาศใช้วันที่ 18 กรกฎาคม พ.ศ. 2550 วัตถุประสงค์ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็เพื่อเป็นการควบคุมโครงสร้างพื้นฐานของแต่ละหน่วยงานให้มีความปลอดภัย ป้องกันความเสี่ยงที่อาจเกิดจากการคุกคามจากภายนอกองค์กร และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ยังเป็นการสร้างมาตรฐานให้เกิดขึ้นในองค์กร สามารถเอาผิดกับผู้ประสงค์ร้ายต่อระบบได้

2.1.3 โพรไฟล์ความมั่นคงและไพรเวซี

โพรไฟล์ความมั่นคงและไพรเวซี หรือ เอฟอีเอ-เอสพีพี (Federal Enterprise Architecture Security and Privacy Profile: FEA-SPP) [6] คือเอกสารหรือกรอบการทำงานสำหรับผู้ที่มีหน้าที่ในการรักษาความมั่นคงของสารสนเทศ (Information Security) และไพรเวซีข้อมูล (Data Privacy) ในบริบทของหน่วยงานที่มีโครงสร้างขนาดใหญ่ในเอกสารของเอฟอีเอ-เอสพีพี ได้จัดเตรียมวิธีปฏิบัติที่เป็นเลิศ (Best Practices) และคำแนะนำซึ่งจะช่วยให้เกิดความสำเร็จในการรวมเรื่องความมั่นคงสารสนเทศและไพรเวซีเพื่อใช้ในองค์กร

2.1.4 มาตรฐานไพรเวซีระดับสากลหรือจีพีเอส (The Global Privacy Standard: GPS)

มาตรฐานไพรเวซีระดับสากล:จีพีเอส[7] มีวัตถุประสงค์เพื่อรวบรวมประสานหลักการด้านไพรเวซีที่ใช้งานในระดับสากล หลักการไพรเวซีของจีพีเอสประกอบด้วย

1. ความยินยอม (Consent)

ความยินยอม เจ้าของข้อมูลส่วนบุคคลมีอิสระและสามารถกำหนดการยินยอมอนุญาตให้เก็บรวบรวม การใช้งาน การเปิดเผยข้อมูลส่วนบุคคลยกเว้นแต่ตามที่กฎหมายระบุไว้ การยินยอมนั้นเจ้าของข้อมูลส่วนบุคคลสามารถแก้ไขภายหลังได้

2. ภาระความรับผิดชอบ (Accountability)

ข้อมูลส่วนบุคคลที่เก็บรวบรวมมีการป้องกันที่เหมาะสม ภาระหน้าที่ความรับผิดชอบด้านไพรเวซีต้องมีการจัดทำเป็นเอกสารทั้งในด้านนโยบาย ขั้นตอนและต้องมีการสื่อสารให้บุคคลที่เกี่ยวข้องรับทราบ มอบหมายบุคคลในองค์กรให้รับผิดชอบด้านไพรเวซีและความมั่นคงในองค์กร ต้องมีการป้องกันที่เหมาะสมเมื่อมีการส่งต่อข้อมูลส่วนบุคคลให้กับบุคคลที่สาม

3. วัตถุประสงค์ (Purpose)

องค์กรต้องกำหนดวัตถุประสงค์ในการเก็บรวบรวม ใช้งาน รักษาและเปิดเผยข้อมูลส่วนบุคคลและต้องสื่อสารวัตถุประสงค์เหล่านั้นให้เจ้าของข้อมูลรับทราบก่อนที่จะเก็บข้อมูลส่วนบุคคล วัตถุประสงค์ที่กำหนดต้องชัดเจนมีการกำหนดขอบเขตและเป็นปัจจุบัน

4. ขอบเขตการเก็บรวบรวม (Collection Limitation)

การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องมีความยุติธรรมเป็นไปตามกฎหมาย มีขอบเขตชัดเจนและเป็นไปตามวัตถุประสงค์ที่กำหนด

5. การใช้งาน เก็บรักษาและขอบเขตการเปิดเผย (Use, Retention, and Disclosure Limitation)

องค์กรจะต้องมีการกำหนดขอบเขตการใช้งาน รักษา และเปิดเผยข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับวัตถุประสงค์ที่กำหนดไว้ ยกเว้นแต่มีระบุไว้ในกฎหมาย ข้อมูลส่วนบุคคลต้องมีการปกป้องรักษาที่เหมาะสม หลังจากเลิกใช้งานต้องมีขั้นตอนการทำลายที่ปลอดภัย

6. ความแม่นยำ (Accuracy)

องค์กรต้องทำให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นมีความถูกต้อง สมบูรณ์ และมีความเป็นปัจจุบันเป็นไปตามวัตถุประสงค์ที่กำหนด

7. ความมั่นคง (Security)

องค์กรต้องรับผิดชอบด้านความมั่นคงของข้อมูลส่วนบุคคลทั้งวงจรการใช้งานโดยต้องมีการนำมาตรฐานระดับสากลมาปรับใช้ในองค์กร ข้อมูลส่วนบุคคลที่อ่อนไหวได้รับการป้องกันที่เหมาะสมทั้งในด้านกายภาพและด้านเทคนิค

8. ความโปร่งใส (Openness)

การเปิดเผยและความโปร่งใสเป็นหัวใจสำคัญของภาระรับผิดชอบในองค์กร สารสนเทศที่เกี่ยวข้องกับนโยบายและการนำข้อมูลส่วนบุคคลไปใช้งานจะต้องมีการเปิดเผยให้รับทราบโดยทั่วกัน

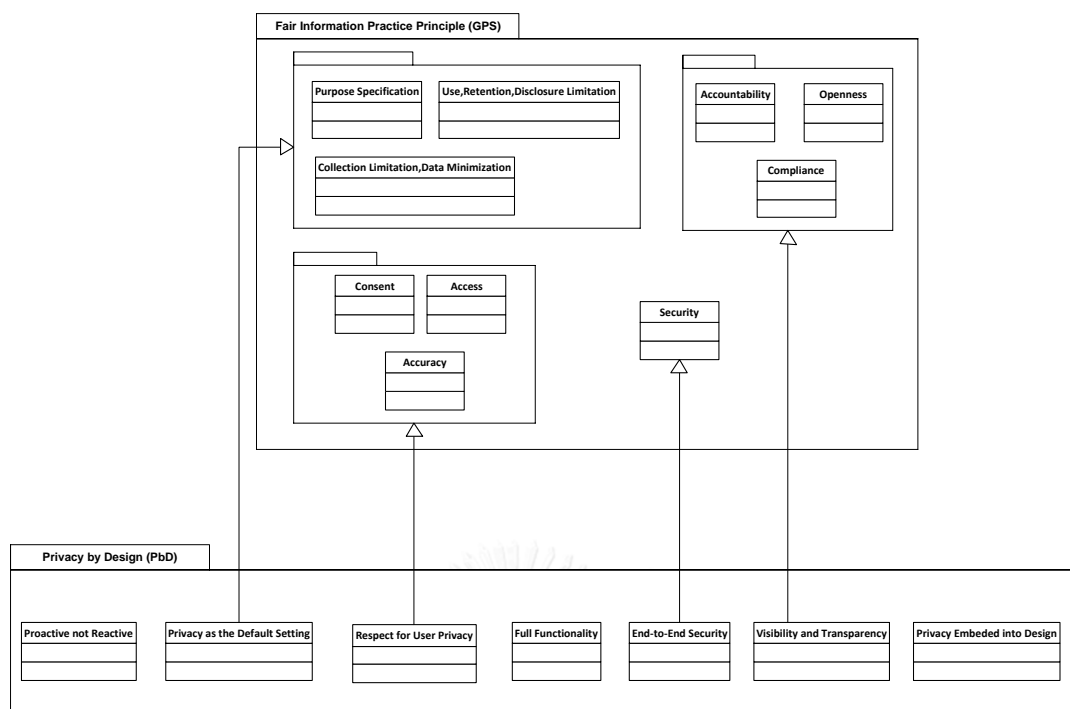
9. การเข้าถึง (Access)

เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลเหล่านั้นและสามารถใช้งานหรือเปิดเผยได้ เจ้าของข้อมูลสามารถปรับแก้ไขข้อมูลส่วนบุคคลให้เกิดความสมบูรณ์ตามความเหมาะสมได้

10. การปฏิบัติตาม (Compliance)

องค์กรต้องสร้างกลไกในการร้องเรียนและสื่อสารกลไกเหล่านั้นให้ทราบทั่วทั้งองค์กร รวมถึงวิธีการฟ้องร้องในแต่ละระดับ รวมถึงองค์กรต้องตรวจสอบขั้นตอนการประเมิน การทวนสอบว่ากลไกเหล่านั้นเป็นไปตามนโยบายที่กำหนด

สรุปได้ว่าจีพีเอสเป็นหลักการระดับสากล ซึ่งเป็นมาตรฐานที่พีบีทีได้เลือกนำมาเป็นแนวทางสร้างเป็นหลักการพีบีทีไปด้วย 7 หลักการ โดยพิจารณาจากมาตรฐานจีพีเอสที่ประกอบด้วย 10 ข้อดังกล่าวมาแล้วดังปรากฏดังรูปที่ 2.1



รูปที่ 2.1 ภาพรวมของจีพีเอสและการพัฒนาต่อยอดของพีบีดี

ตารางที่ 2.1 อธิบายคลาสมาตรฐานไพรเวซีระดับสากลจากรูปที่ 2.1

ลำดับ	ชื่อคลาส	คำอธิบาย
1.	Purpose Specification	กลุ่มคลาสเกี่ยวข้องกับวัตถุประสงค์ของการเก็บข้อมูลส่วนบุคคล
2.	Use, Retention, Disclosure, Limitation	กลุ่มคลาสเกี่ยวกับข้อจำกัดในการใช้งาน เก็บรักษา และเปิดเผยข้อมูลส่วนบุคคล โดยต้องสอดคล้องกับวัตถุประสงค์ที่กำหนด
3.	Collection Limitation, Data Minimization	กลุ่มคลาสเกี่ยวกับขอบเขตการเก็บข้อมูล ความเป็นธรรมในการเก็บข้อมูล และเป็นตามกฎหมายที่กำหนด
4.	Accountability	กลุ่มของคลาสเกี่ยวกับหน้าที่ความรับผิดชอบเมื่อเก็บข้อมูลส่วนบุคคลจะต้องมีการป้องกันข้อมูลเหล่านั้น รวมไปถึงจัดทำเอกสารเพื่อสื่อสารกับเจ้าของข้อมูล
5.	Openness	กลุ่มคลาสเกี่ยวข้องกับการเปิดเผยและความโปร่งใสในการดำเนินการกับข้อมูลที่จัดเก็บ

ตารางที่ 2.1 อธิบายคลาสมาตรฐานไพรเวซีระดับสากลจากรูปที่ 2.1 (ต่อ)

ลำดับ	ชื่อคลาส	คำอธิบาย
6.	Compliance	กลุ่มคลาสเกี่ยวข้องกับการสร้างกลไกในการร้องเรียน การชดเชยใช้ค่าเสียหาย รวมถึงการสื่อสารข้อมูลเหล่านี้ในพื้นที่สาธารณะ
7.	Consent	กลุ่มคลาสเกี่ยวข้องกับการยินยอมให้เก็บรวบรวม ใช้งาน หรือเปิดเผยข้อมูลส่วนบุคคล
8.	Access	กลุ่มคลาสเกี่ยวข้องกับการเข้าถึงข้อมูลส่วนบุคคล รวมไปถึงแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการใช้งาน การเปิดเผยข้อมูลส่วนบุคคล
9.	Accuracy	กลุ่มคลาสเกี่ยวข้องกับความถูกต้อง ความเป็นปัจจุบัน ความสมบูรณ์ของข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามวัตถุประสงค์ที่กำหนด
10.	Security	กลุ่มคลาสเกี่ยวข้องกับการสร้างความมั่นคงให้กับข้อมูลส่วนบุคคลตลอดทั้งวงจรชีวิตข้อมูลส่วนบุคคล

ตารางที่ 2.2 อธิบายคลาสพีบีดีจากรูปที่ 2.1

ลำดับ	ชื่อคลาส	คำอธิบาย
1.	Proactive not Reactive	กลุ่มคลาสด้านการป้องกันและคาดการณ์ก่อนที่จะเกิดการรุกรานด้านไพรเวซี
2.	Privacy as the Default Setting	กลุ่มคลาสด้านไพรเวซีจะได้รับการกำหนดเป็นการดำเนินการที่จำเป็น ต้องมีมาตรฐาน แม้ไม่มีการกำหนดโดยผู้ใช้งาน
3.	Respect for User Privacy	กลุ่มคลาสที่เกี่ยวข้องกับไพรเวซีจะต้องสนับสนุนเพื่อให้ไพรเวซีเกิดประโยชน์สูงสุดต่อผู้ใช้งาน
4.	Full Functionality	กลุ่มคลาสที่ให้ความสำคัญกับกฎระเบียบและวัตถุประสงค์โดยพิจารณาทั้งเรื่องไพรเวซีและความมั่นคง
5.	End-to-End Security	กลุ่มคลาสเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล ตั้งแต่เริ่มกิจกรรมจนถึงสิ้นสุดกิจกรรม

ตารางที่ 2.2 อธิบายคลาสพีบีดีจากรูปที่ 2.1 (ต่อ)

ลำดับ	ชื่อคลาส	คำอธิบาย
6.	Visibility and Transparency	กลุ่มคลาสด้านความโปร่งใสในการดำเนินการกิจกรรมด้านไพรเวซีภายในองค์กรตามนโยบายที่ได้กำหนด
7.	Privacy Embedded into Design	กลุ่มคลาสด้านไพรเวซีได้ถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอทีและการดำเนินกิจกรรมในองค์กร

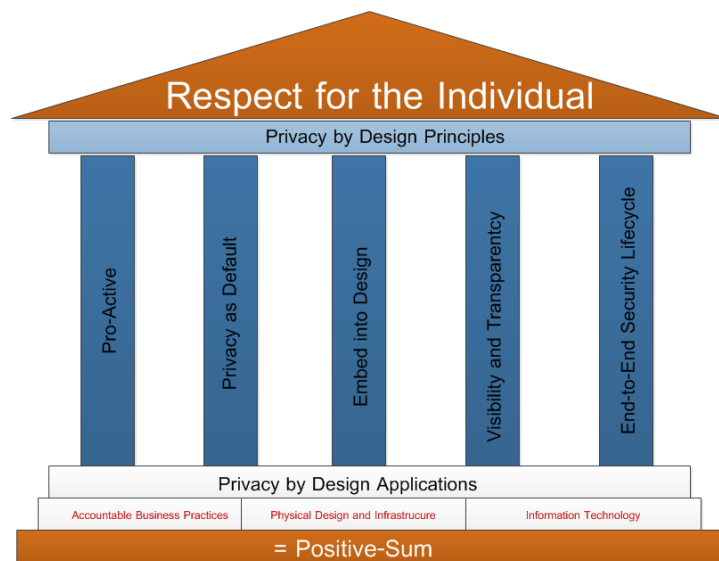
2.1.5 กรอบการทำงานพื้นฐานสำหรับไพรเวซีบายดีไซน์ การประเมินผลกระทบไพรเวซี

กรอบการทำงานพื้นฐานสำหรับไพรเวซีบายดีไซน์ การประเมินผลกระทบไพรเวซี (Foundation Framework for a Privacy by Design Privacy Impact Assessment: PbD-PIA) [8] ซึ่งต่อไปจะเรียกว่า “พีบีดีพีไอเอ” โดยในพีบีดีพีไอเอ ได้กล่าวถึงไพรเวซีบายดีไซน์-พีบีดี (Privacy by Design :PbD) และการประเมินผลกระทบด้านไพรเวซี โดยพีบีดีพีไอเอจะประกอบไปด้วยคำแนะนำและแนวปฏิบัติเพื่อแต่ละองค์กรสามารถนำไปใช้งานตามความเหมาะสม พีบีดีถูกนำเสนอโดยคณะกรรมการสิทธิการไพรเวซีและสารสนเทศ (Information & Privacy Commissioner) ออนตาริโอ ประเทศแคนาดา โดยได้กล่าวว่าการกรอบการทำงานนี้เป็นตัวแทนของการเปลี่ยนผ่านในเรื่องแนวคิดด้านการปกป้องไพรเวซี โดยการทำให้เกิดมาตรฐานในการบริหารจัดการกับสารสนเทศ และกรอบการทำงานนี้ยังได้จัดเตรียมการลดการละเมิดเรื่องไพรเวซี โดยพิจารณาไพรเวซีผ่านวงจรชีวิตเทคโนโลยี โดยเริ่มจากขั้นตอนแรกๆ ของการออกแบบ การนำไปใช้งานจนกระทั่งการยกเลิกหรือการทำลายข้อมูล พีบีดีพีไอเอได้มีจัดเตรียมเครื่องมือเพื่อใช้ในการนำไปปฏิบัติจริง โดยให้ความสำคัญกับการเคารพสิทธิของผู้ใช้งาน มีแนวความคิดให้ผู้ใช้งานเป็นศูนย์กลางซึ่งพิจารณาทั้งในเชิงสาธารณะ (Public) และในเชิงส่วนบุคคล (Private) เพื่อให้เกิดความเหมาะสมกับการคาดหวังของผู้ใช้งานที่คาดหวังในเรื่องไพรเวซี กรอบการทำงานนี้ยังได้อ้างว่าเป็นแนวคิดเชิงรุกในการป้องกันการละเมิดด้านไพรเวซี โดยที่องค์กรจะต้องมีการนำเอาหลักการทำงาน 7 ประการของพีบีดีไปประยุกต์ใช้ ซึ่งกรอบการทำงานพีบีดีนี้มีความตั้งใจให้ผลลัพธ์ที่จะเกิดกับองค์กรคือได้ผลลัพธ์แบบ วิน-วิน (Win-Win Solution) คือเป็นการได้ประโยชน์ทั้งในองค์กรและผู้ใช้งาน ขอบเขตของกรอบการทำงานพีบีดีคือ

- เพื่อให้แน่ใจว่ามีการป้องกันด้านไพรเวซีได้โดยบรรจุอยู่ในเทคโนโลยีสารสนเทศ (Information Technology) กระบวนการทางธุรกิจที่รับผิดชอบ (Accountability)

Business Process) การออกแบบทางด้านกายภาพและโครงสร้างพื้นฐานเครือข่าย (Networked Infrastructure)

- เพื่อให้มั่นใจได้ว่าองค์กรได้นำเอาหลักการของพีบีดีบรรจุอยู่ในทุกมุมมองของการดำเนินการขององค์กรทั้งการเก็บ การใช้ การเปิดเผย การรักษา การส่งต่อ และการทำลายข้อมูล



รูปที่ 2.2 ภาพรวมกรอบการทำงานของพีบีดี [8]

กรอบการทำงานทั้ง 7 ประการของพีบีดีที่ปรากฏในรูปที่ 2.2 มีดังนี้

หลักการที่ 1: Proactive not Reactive

การป้องกันและคาดการณ์ ก่อนที่จะเกิดการรุกรานด้านไพรเวซี

หลักการที่ 2: Privacy as the Default Setting

ไพรเวซีจะได้รับการกำหนดเป็นการดำเนินการที่จำเป็น ต้องมีมาตรฐาน แม้ไม่มีการกำหนดโดยผู้ใช้งาน

หลักการที่ 3: Privacy Embedded into Design

ไพรเวซีได้ถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินกิจกรรมในองค์กร

หลักการที่ 4: Full Functionality – Positive-Sum, not Zero-Sum

ให้ความสำคัญกับกฎระเบียบและวัตถุประสงค์โดยพิจารณาทั้งเรื่องไพรเวซีและความมั่นคง

หลักการที่ 5: End-to-End Security – Full Life Cycle Protection

ไพรเวซีได้ถูกฝังอยู่ระบบตั้งแต่เริ่มกิจกรรมจนถึงสิ้นสุดกิจกรรม

หลักการที่ 6: Visibility and Transparency – Keep it Open

ความโปร่งใสในการดำเนินกิจกรรมด้านไพรเวซีภายในองค์กรตามนโยบายที่ได้กำหนด

หลักการที่ 7: Respect for User Privacy – Keep it Individual Centric

ผู้เกี่ยวข้องด้านไพรเวซีจะต้องสนับสนุนเพื่อให้ไพรเวซีเกิดประโยชน์สูงสุดกับผู้ใช้งาน

สรุปพีบีดีพีไอเอเป็นกรอบการทำงานซึ่งประกอบด้วย 7 หลักการซึ่งเป็นการแมป (Mapping) มาจากหลักปฏิบัติเกี่ยวกับสารสนเทศที่เป็นธรรม (Fair Information Practice Principles-GPS) [9] ซึ่งแต่ละองค์ประกอบของพีบีดีพีไอเอจะประกอบด้วยแนวปฏิบัติผ่านคำถามโดยคำถามเหล่านั้นสามารถนำมาปรับใช้ให้เหมาะสมกับบริบทในแต่ละองค์กร คำถามทั้งหมดปรากฏอยู่ในภาคผนวก ง ตารางที่ ง.1 และแผนภาพคลาสของคำถามในแต่ละหลักการปรากฏอยู่ในรูปที่ ง.40-ง.46

2.1.6 สถาปัตยกรรมองค์กรของรัฐบาลกลาง ความมั่นคงและโปรไฟล์ไพรเวซี

สถาปัตยกรรมองค์กรของรัฐบาลกลาง ความมั่นคงและโปรไฟล์ไพรเวซี เวอร์ชัน 3.0 [6] คือเอกสารที่จัดทำโดยผู้เชี่ยวชาญที่มาจากทั้งหน่วยงานภาครัฐ ภาคอุตสาหกรรม และนักวิชาการ เพื่อร่วมกันจัดทำเอกสารที่มีความสำคัญและสร้างเป็นวิธีปฏิบัติที่เป็นเลิศทั้งในด้านสาธารณะและภาคส่วนบุคคลเนื้อหาในเอกสารพูดถึงการจัดเตรียมกรอบการทำงานในลักษณะข้ามหน่วยงานไว้หลายกรอบการทำงาน แต่ในกรอบการทำงานที่เอกสารนี้พูดถึงคือ โปรไฟล์ของความมั่นคงและไพรเวซี ซึ่งก็คือ กรอบการทำงานที่สามารถรองรับโครงสร้างขนาดใหญ่กรอบการทำงานที่สามารถทำซ้ำได้นอกจากนั้นกรอบการทำงานยังพูดถึงความมั่นคงของสารสนเทศและความต้องการของไพรเวซีข้อมูลในบริบทของสถาปัตยกรรมหน่วยงานราชการ ซึ่งในเอกสารนี้ได้จัดเตรียมคำแนะนำซึ่งจะช่วยให้ประสบความสำเร็จเรื่องของความมั่นคงของสารสนเทศและไพรเวซีเข้าไปเป็นส่วนหนึ่งของสถาปัตยกรรมในองค์กรโดยรายละเอียดดังต่อไปนี้

- จัดเตรียมแนวทางเพื่อให้หน่วยงานราชการบูรณาการเรื่องความมั่นคงด้านไอทีและไพรเวซีด้วยสถาปัตยกรรมเอ็นเตอร์ไพรส์
- จัดเตรียมกลไกการระบุและจัดทำเอกสารด้านความมั่นคงและความต้องการด้านไพรเวซี
- สนับสนุนการรวมความมั่นคงและไพรเวซีที่เกิดขึ้นในแต่ละกิจกรรมขององค์กร

ในเอกสารนี้ได้นำเสนอ 8 องค์ประกอบของหลักปฏิบัติเกี่ยวกับสารสนเทศที่เป็นธรรม (Fair Information Practice Principles-FIPPs) ดังในตารางที่ 2.3



ตารางที่ 2.3 หลักการปฏิบัติเกี่ยวกับสารสนเทศที่เป็นธรรม [6]

หลักการ	คำอธิบาย
1.ความโปร่งใส	มีการประกาศให้ทราบถึงการจัดเก็บ การใช้งาน เผยแพร่และการเก็บรักษาของข้อมูลที่ใช้ในการระบุตัวตน
2.การมีส่วนร่วมของบุคคลและการขดเซย	เกี่ยวข้องกับข้อมูลบุคคลที่ใช้ในการระบุตัวตน และการแสวงหาผลประโยชน์จะต้องได้รับการยินยอมการเก็บ การใช้งาน การเผยแพร่ และการเก็บรักษา โดยจัดเตรียมกลไกการเข้าถึงที่เหมาะสม การแก้ไข และการขดเซยโดยค่าเสียหาย
3.การระบุวัตถุประสงค์	ต้องได้รับอนุญาตในการจัดเก็บข้อมูลที่ใช้ในการระบุตัวตนซึ่งต้องบอกรวัตถุประสงค์ในการจัดเก็บและการนำเอาข้อมูลไปใช้งาน
4.การลดการเก็บข้อมูล และการเก็บรักษา	การเก็บรวบรวมข้อมูลที่ใช้ในการระบุตัวตนจะต้องระบุ วัตถุประสงค์ในการเก็บ โดยการเก็บรักษาข้อมูลจะเก็บรักษาไว้เท่าที่จำเป็นตามที่วัตถุประสงค์กำหนด
5.การจัดจัดการใช้งานข้อมูล	การแบ่งปันข้อมูลและการจัดเก็บข้อมูลจะต้องเป็นไปตามวัตถุประสงค์ที่กำหนด
6.คุณภาพข้อมูลและความสมบูรณ์	สร้างข้อมูลที่มีความถูกต้องและสมบูรณ์ตรงตามวัตถุประสงค์ที่ได้แจ้งให้สาธารณะทราบ
7.ความมั่นคง	มีปกป้องข้อมูลทุกช่องทางทางการสื่อสาร มีความมั่นคงทางกายภาพที่ช่วยลดความเสี่ยงที่จะเกิดขึ้น
8. ความรับผิดชอบและการตรวจสอบ	ควรมีรับผิดชอบต่อการปฏิบัติตามความต้องการด้านการป้องกันไพรเวซี นโยบายที่กำหนดและการตรวจสอบการดำเนินงานข้อมูลมีความสอดคล้องกับการควบคุมด้านไพรเวซี

สรุปเอกสารนี้มีวัตถุประสงค์เพื่อใช้เป็นทรัพยากรสำหรับองค์กรที่พยายามทำความเข้าใจว่าทำอย่างไรถึงจะบูรณาการเรื่องของความมั่นคงและไพรเวซีให้เกิดขึ้นในองค์กร ถึงแม้ว่าในเอกสารนี้จะแนะนำขั้นตอนแรกจนถึงขั้นตอนสุดท้ายแต่การนำไปเป็นแนวทางปฏิบัติสามารถเลือกทำในหัวข้อใดที่สนใจก็ได้ เอกสารนี้เหมาะสำหรับผู้ที่ความรู้หลากหลายสาขาซึ่งไม่จำเป็นเฉพาะผู้ที่มีหน้าที่รับผิดชอบดูแลเรื่องความมั่นคงหรือด้านไพรเวซี

2.2 งานวิจัยที่เกี่ยวข้อง

ในส่วนนี้กล่าวถึงงานวิจัยที่ได้ศึกษาเพื่อใช้เป็นแนวทางในการทำงานวิจัยประกอบไปด้วย

2.2.1 การควบคุมการเข้าถึงตามบทบาท

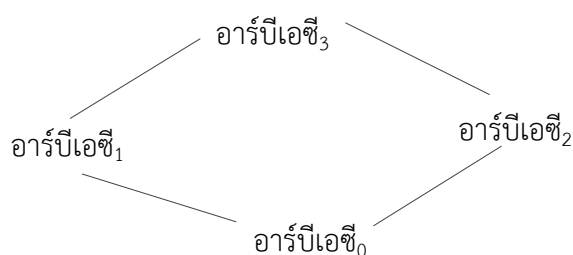
การควบคุมการเข้าถึงตามบทบาทหรืออาร์บีเอซี (Role Based Access Control: RBAC) [10] เกิดจากความต้องการเนื่องจากระบบคอมพิวเตอร์ประกอบด้วยแอปพลิเคชันที่ให้บริการสำหรับผู้ใช้งานหลากหลายกลุ่มจึงเกิดการตระหนักถึงความมั่นคงของข้อมูล โดยที่ผู้ดูแลระบบและผู้พัฒนาซอฟต์แวร์จะมีการควบคุมการเข้าถึงที่แตกต่างกัน เพื่อมั่นใจว่ามีเพียงผู้ที่ได้รับมอบหมายสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลและทรัพยากรที่ให้บริการ สำหรับอาร์บีเอซีได้เสนอคำศัพท์สำคัญและเนื้อหาที่ใช้ดังต่อไปนี้

- การเข้าถึง (Access) เป็นการระบุประเภทการโต้ตอบระหว่างผู้กระทำ (Subject) และสิ่งที่ จะกระทำ (Object) ซึ่งผลลัพธ์ที่ได้คือลำดับการไหลของข้อมูลจากที่หนึ่งไปสู่อีกที่หนึ่ง
- การควบคุมการเข้าถึง (Access Control) กระบวนการของการจำกัดการเข้าถึงทรัพยากร ของระบบมีเพียงผู้ที่ได้รับมอบหมายสิทธิเท่านั้นสามารถเข้าถึงทรัพยากรและบริการได้
- บทบาทผู้บริหาร (Administrative Role) คือบทบาทที่มีสิทธิในการปรับปรุงกลุ่มผู้ใช้งาน บทบาท สิทธิ และการมอบหมายสิทธิ
- ข้อจำกัด (Constraint) คือ ความสัมพันธ์หรือจำนวนของบทบาท
- กลุ่ม (Groups) คือ กลุ่มของผู้ใช้งาน
- สิทธิ (Permission) คือ รายละเอียดที่บอกว่าได้รับอนุญาตให้กระทำสิ่งไหนได้บ้าง
- บทบาท (Role) คือ ตำแหน่งงานในองค์กรซึ่งบอกถึงภาระความรับผิดชอบ
- เซสชัน (Session) คือ การแมป (Mapping) ระหว่างผู้ใช้งานและบทบาท
- ผู้ใช้งาน (User) คือ บุคคลใดๆ ซึ่งปฏิสัมพันธ์กับคอมพิวเตอร์โดยตรง

แบบจำลองอาร์บีเอซีประกอบด้วยส่วนที่สำคัญต่อไปนี้คือ

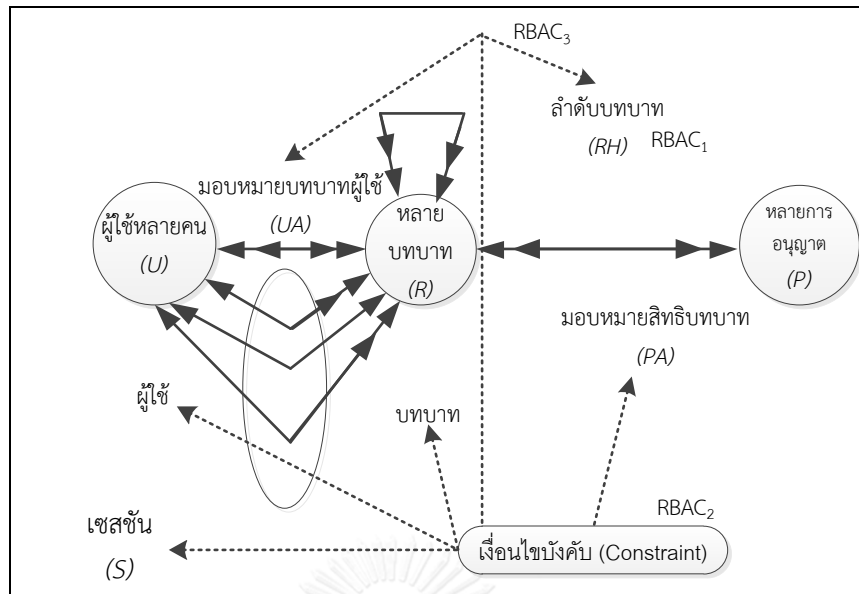
- ผู้ใช้และบทบาท (Users and Roles)
- สิทธิ (Permission) ในอาร์บีเอซีคือ การอนุญาตให้เข้าถึงระบบ คำว่า “การอนุญาต (Authorization)” “สิทธิในการเข้าถึง (Access Right)” “สิทธิพิเศษ (Privilege)” คำเหล่านี้เป็นคำที่แสดงถึงสิทธิในการใช้งานออบเจกต์ (Object) คือดาต้าออบเจกต์ หรือออบเจกต์ของทรัพยากรที่อยู่ในระบบคอมพิวเตอร์ซึ่งสิทธิการใช้งานสามารถใช้ได้กับหนึ่งออบเจกต์หรือมากกว่านั้น และกำหนดได้ว่าอ่านได้อย่างเดียวหรือทั้งอ่านและเขียน ในอาร์บีเอซีผู้ใช้งานมีได้หลายบทบาท ในทางกลับกันบทบาทก็สามารถถูกใช้งานได้หลายผู้ใช้งาน ในหนึ่งบทบาทอาจมีได้หลายสิทธิการใช้งาน และสิทธิการใช้งานหนึ่งสิทธิก็อาจจะถูกมอบหมายให้กับหลายบทบาท
- เซสชัน (Session) เซสชันจะถูกสร้างขึ้นในระหว่างการใช้งาน เซสชันทำการแยกจากผู้ใช้งานตามบทบาทที่ได้รับ ผู้ใช้งานหนึ่งคนมีหลายบทบาท ผู้ใช้งานก็สามารถมีหลายเซสชันได้

การควบคุมการเข้าถึงตามบทบาทมีหลายรูปแบบในการใช้งานดังปรากฏในรูปที่ 2.1 คือรูปแบบอาร์บีเอซี₀ คือรูปแบบที่เป็นฐานรากของอาร์บีเอซี รูปแบบอาร์บีเอซี₁ และรูปแบบอาร์บีเอซี₂ โดยสองรูปแบบหลัง เป็นการต่อยอดจากรูปแบบอาร์บีเอซีที่ 1 โดยรวมเอารูปแบบอาร์บีเอซี₀ เข้าไปด้วย โดยมีความแตกต่างตรงที่รูปแบบอาร์บีเอซี₁ ได้เพิ่มความสามารถด้านการลำดับของบทบาท ขณะที่รูปแบบอาร์บีเอซี₂ ได้เพิ่มความสามารถด้านการมอบหมายสิทธิและรูปแบบของอาร์บีเอซี₃ คือการรวมความสามารถทุกรูปแบบของอาร์บีเอซีเข้าด้วยกัน



รูปที่ 2.3 กลุ่มของรูปแบบอาร์บีเอซี [10]

ในรูปที่ 2.2 แสดงให้เห็นว่ากรณีที่เป็นรูปแบบอาร์บีเอซี₀ จะประกอบด้วยผู้ใช้งาน บทบาท สิทธิและเซสชัน ยกเว้นความสามารถด้านการลำดับบทบาทและการมอบหมายสิทธิ โดยอาร์บีเอซีได้กำหนดนิยามดังต่อไปนี้



รูปที่ 2.4 แบบจำลองอาร์บีเอซี [10]

นิยามที่ 1 แบบจำลองอาร์บีเอซี₀ มีส่วนประกอบดังนี้

- U, R, P และ S (ผู้ใช้, บทบาท, สิทธิและเซสชัน)
- $PA \subseteq P \times R$ การมอบหลายหมายสิทธิ ให้กับบทบาท
- $UA \subseteq U \times R$ การมอบหมายหลายผู้ใช้ ให้กับบทบาท
- ผู้ใช้: $s \rightarrow U$ ฟังก์ชันที่แมปแต่ละเซสชัน S_i ให้กับผู้ใช้งานเพียงหนึ่งคน
- บทบาท: $s \rightarrow 2^R$ ฟังก์ชันที่แมปแต่ละเซสชัน S_i ให้กับกลุ่มของบทบาท $roles(S_i) \subseteq \{r \mid (user(S_i), r) \in UA\}$ และเซสชัน S_i สิทธิคือ $U_r \in roles(S_i) \{p \mid (p, r) \in PA$

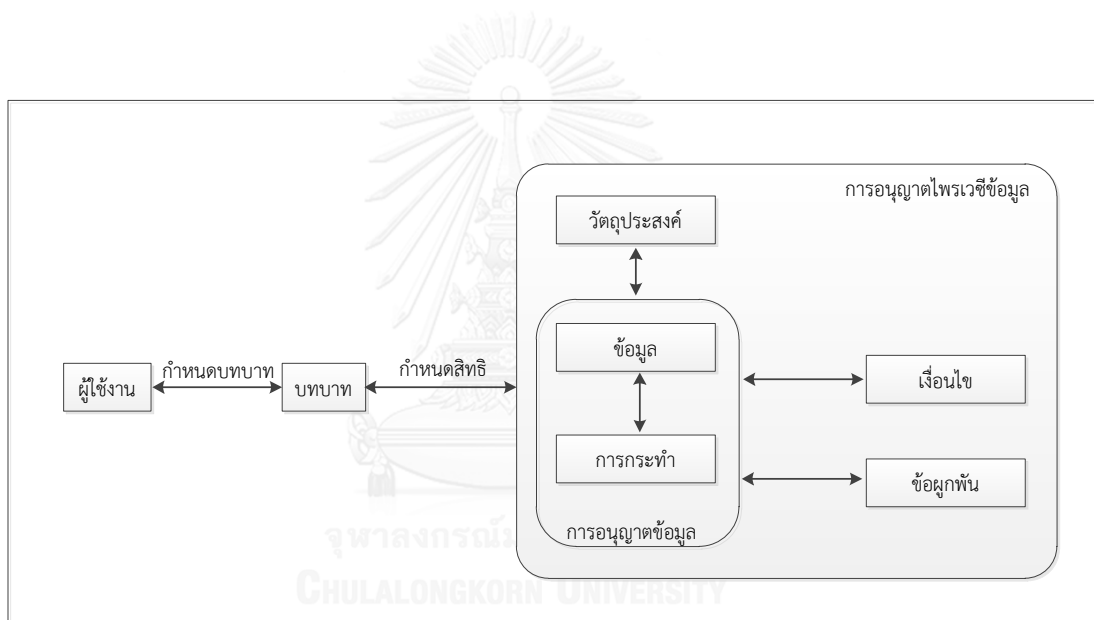
นิยามที่ 2 แบบจำลองอาร์บีเอซี₁ ประกอบด้วยส่วนประกอบดังนี้

- U, R, P, S, PA, UA (ผู้ใช้, บทบาท, สิทธิ, เซสชัน, การมอบหมายสิทธิ, การมอบหมายผู้ใช้)
- $RH \subseteq R \times R$ คือเป็นส่วนหนึ่งของลำดับสิทธิให้กับบทบาท ซึ่งอาจจะเขียนได้ว่า \geq ;
- บทบาท: $s \rightarrow 2^R$ เพิ่มเติมจากนิยามที่ 1 คือ $roles(S_i) \subseteq \{r \mid (Er' \geq r) [user(s), r' \in UA]$

สรุปสิ่งที่งานวิจัยการควบคุมการเข้าถึงตามบทบาทนำเสนอคือ แนวคิดต้นแบบที่นำเสนอการใช้งานใดๆ ต้องมีการกำหนดบทบาทและสิทธิ ผ่านการมอบหมายให้กับผู้ใช้งานที่เกี่ยวข้องซึ่งงานวิจัยนี้ได้ถูกนำไปต่อยอดแนวความคิดและพัฒนาเรื่องการควบคุมการเข้าถึงตามบทบาทในด้านอื่นเช่น ด้านโทรเวชของข้อมูล ด้านการรักษาความมั่นคง เป็นต้น

2.2.2 การควบคุมการเข้าถึงตามบทบาทด้านความเป็นส่วนตัว

งานวิจัยนี้ได้กล่าวถึงการควบคุมการเข้าถึงตามบทบาทด้านความเป็นส่วนตัว (Privacy-aware Role Based Access Control: P-RBAC) [11] ซึ่งต่อไปในงานวิจัยนี้จะเรียกว่า “พ็อบบีเอซี” คืองานวิจัยที่ต่อยอดมาจากงานวิจัยการควบคุมการเข้าถึงตามบทบาท [10] วัตถุประสงค์ของงานวิจัยพ็อบบีเอซีเพื่อสนับสนุนให้เกิดการตระหนักถึงความเป็นส่วนตัวโดยการควบคุมการเข้าถึงตามบทบาท การใช้นโยบายความเป็นส่วนตัว (Privacy Policies) ผ่านการมอบหมายสิทธิ (Permission Assignments: PA) ซึ่งสิทธิที่กล่าวถึงในงานวิจัยนี้จะแตกต่างจากงานวิจัยเดิม [10] ได้กล่าวไว้เพราะได้เพิ่มส่วนประกอบที่ใช้แทนความสัมพันธ์ของความเป็นส่วนตัว (Privacy) แนวคิดของแบบจำลองการเข้าถึงตามบทบาทปรากฏดังรูปที่ 2.3 ซึ่งส่วนประกอบในแต่ละส่วนที่อยู่ในแบบจำลองอธิบายได้ดังต่อไปนี้คือ



รูปที่ 2.5 แนวความคิดของแบบจำลอง พ็อบบีเอซี [11]

- ผู้ใช้งานคือ บุคคลที่ใช้งานระบบ
- บทบาทคือ หน้าที่การทำงานหรือชื่อตำแหน่งในองค์กร
- ข้อมูลคือ สารสนเทศใดๆ หรือเมตาดาต้าที่สามารถใช้ระบุตัวตนได้
- การกระทำคือ การปฏิบัติงานระหว่างผู้ใช้งานกับข้อมูล
- วัตถุประสงค์คือ ขอบเขตของการกระทำกับข้อมูล
- ข้อมูลผูกพันคือ สิ่งจะต้องดำเนินการหลังจากการกระทำลำดับล่าสุด

- เงื่อนไขคือ สิ่งที่ต้องดำเนินการให้ก่อนแล้วเสร็จก่อนที่จะเริ่มทำงานในขั้นตอนอื่น

งานวิจัยอาร์บีเอซีได้กล่าวถึงนโยบายไพรเวซีว่าควรจะเป็นสิ่งเดียวกับนโยบายที่ใช้ควบคุมการเข้าถึงเพราะต่างก็มีวัตถุประสงค์เดียวกันคือ การจำกัดการเข้าถึงทรัพยากรและในการกำหนดนโยบายไม่ควรกำหนดขึ้นมาให้เพื่อเกิดความสับสนแต่จะต้องกำหนดให้สอดคล้องกัน

นิยามที่ 1 ของแบบจำลองพ็ออาร์บีเอซีประกอบด้วยส่วนประกอบดังต่อไปนี้

- เซตของ U คือเซตของผู้ใช้ เซตของ R คือเซตของบทบาท เซตของ D คือเซตของข้อมูล เซตของ P_u คือเซตของวัตถุประสงค์ เซต A คือเซตของการกระทำ เซตของ O คือเซตของข้อมูลพื้น และภาษาเงื่อนไข (LC_0)
- เซตของ การอนุญาตใช้ข้อมูล (Data Permission) $DP = \{(a,d) \mid a \in A, d \in D\}$
- เซตของ Privacy-sensitive Data Permission $PDP = \{(dp,pu,c,o) \mid dp \in DP, pu \in P_u, c \text{ เป็นนิพจน์ของ } LC_0, o \in P(O)\}$ $P(O)$ คือพาวเวอร์เซตของ O
- การมอบหมายสิทธิให้กับผู้ใช้ $UA \subseteq U \times R$, เป็นการแมปผู้ใช้งานเข้ากับบทบาทโดยมีความสัมพันธ์แบบกลุ่มต่อกลุ่ม

พื้นฐานของภาษาเงื่อนไขในพ็ออาร์บีเอซีได้รวมเอาภาษาที่ง่ายต่อการทำความเข้าใจใช้แสดงเงื่อนไข และเงื่อนไขที่แสดงจะใช้ตัวแปรบริบท (Context Variables) เช่นตัวแปรที่ใช้เก็บความเกี่ยวข้องของสารสนเทศด้านไพรเวซี

นิยามที่ 2 แสดงโดยภาษาเงื่อนไข LC_0 ให้ X เป็นเซตของตัวแปรบริบท แต่ละตัวแปร $x \in X$ มีโดเมนจำกัดของค่าที่เป็นไปได้ หรือ D_x ; ในทุกๆ โดเมนจะมีค่าเป็นคู่ๆ โดยมีตัวดำเนินการคือ $=$ และ \neq หรือ ac ถูกนิยามว่า X มีรูปแบบ $(x \text{ opr } v)$ โดยที่ $x \in X, v \in D_x, \text{opr} \in \{=, \neq\}$ เงื่อนไขของ LC_0 (Over X) ได้นิยามไว้ดังต่อไปนี้

- ac คือ เงื่อนไขของ LC_0
- ให้ c_i และ c_j เป็นเงื่อนไขของ LC_0 ; แล้ว $c_i \wedge c_j$ เป็นเงื่อนไขของ LC_0
- ตัวอย่างทั่วไปของการใช้งานตัวแปรบริบทมีดังต่อไปนี้
- การรับการยินยอมจากเจ้าของ (OwnerConsent), โดเมน={ยอม,ไม่ยอม};
- การได้รับการยินยอมจากผู้ปกครอง (ParentalConsent), โดเมน={ยอม,ไม่ยอม}; ใช้แทนการได้ยินยอมจากผู้ปกครองในกรณีที่เด็กมีอายุต่ำกว่า 13
- อายุ (OwnerAge), โดเมน={ต่ำกว่า 13, วัยรุ่น, ผู้ใหญ่}; ใช้แทนข้อมูลเป็นช่วงของอายุ

- เวลาปัจจุบัน (CurrentTime), โดเมน={9.00-17.00,17.00-13.00,13.00-9.00}; ใช้แทนช่วงเวลาที่แตกต่างกัน

งานวิจัยได้อธิบายโดยผ่านตัวอย่างของสิทธิด้านความเป็นส่วนตัว (Privacy Permission) ซึ่งจะแสดงด้วยภาษาเงื่อนไข LC₀ โดยยกตัวอย่างจาก www.toys.org ซึ่งเป็นเว็บไซต์ขายของเล่นเด็ก

- บทบาท = {ผู้เป็นส่วนส่งสินค้า, นักการตลาด, ผู้เป็นส่วนธุรกิจ},
- การกระทำ = {อ่าน},
- ข้อมูล = {ข้อมูลการสั่งซื้อสินค้า, ที่อยู่ไปรษณีย์, อีเมล},
- วัตถุประสงค์ = {โปรโมชั่น, ออกบิล, ส่งสินค้า, วิจัย},
- ตัวแปรบริบท = {ข้อมูลผู้ใช้งาน, การรับการยินยอมจากเจ้าของ, การได้รับการยินยอมจากผู้ปกครอง, อายุ }

ต่อไปนี้เป็น การแสดงตัวอย่างนโยบายด้านความเป็นส่วนตัว

1. ผู้เป็นส่วนส่งสินค้าสามารถเข้าถึงข้อมูลที่อยู่ลูกค้าเพื่อวัตถุประสงค์ในการสั่งซื้อสินค้า
2. นักการตลาดสามารถเข้าถึงข้อมูลลูกค้าได้เพื่อดูอีเมลเพื่อวัตถุประสงค์ในการโปรโมชั่นถ้าลูกค้าอนุญาต
3. ผู้เป็นส่วนธุรกิจที่ทำธุรกิจด้วยกันสามารถเข้าถึงข้อมูลการสั่งซื้อสินค้าของลูกค้าเพื่อการวิจัย; อย่างไรก็ตามลูกค้าจะได้รับการแจ้งให้ทราบทางอีเมลที่ได้รับระบุไว้

สามารถเปลี่ยนเป็นนิพจน์ตามหลักการของพีอาร์บีเอซี ได้ดังนี้

PA1: (ผู้เป็นส่วนส่งสินค้า, (อ่าน,ที่อยู่ไปรษณีย์),ส่งสินค้า, N/A, ว่าง)

PA2:(นักการตลาด,(อ่าน,อีเมล), โปรโมต, การรับการยินยอมจากเจ้าของ=ยินยอม, ว่าง)

PA3:(ผู้เป็นส่วนธุรกิจ, ((อ่าน,ข้อมูลการสั่งซื้อสินค้า),วิจัย, N/A, แจ้งเตือน(ทางอีเมล)))

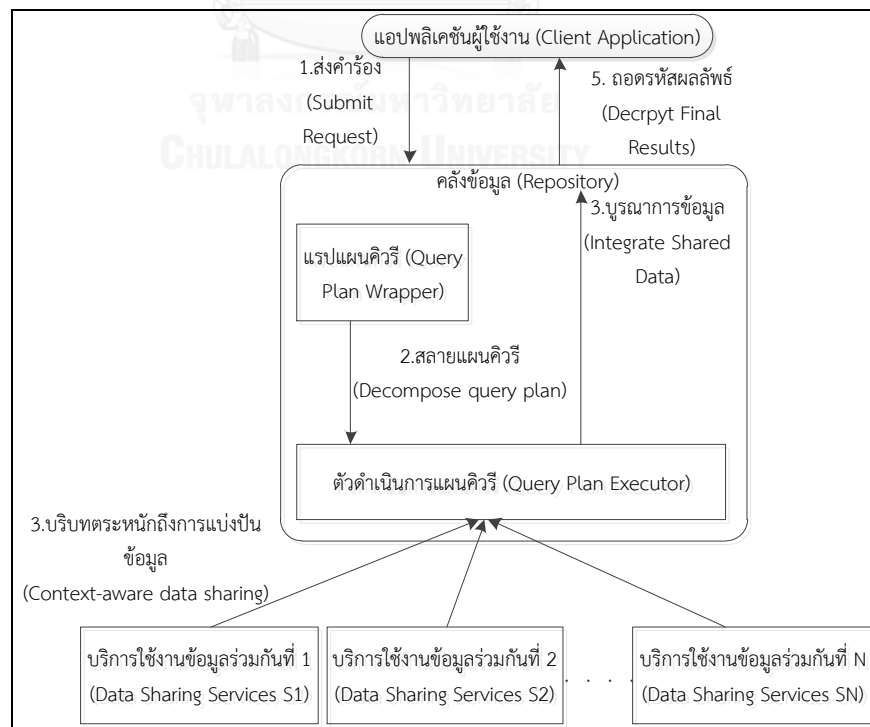
สรุปสิ่งที่งานวิจัยพีอาร์บีเอซีนำเสนอคือ แบบจำลองการเปลี่ยนจากนโยบายความเป็นส่วนตัวให้สามารถกำหนดเป็นสิทธิหรือกำหนดข้อจำกัดของแต่ละบทบาทสำหรับการใช้งาน

2.2.3 การรักษาความเป็นส่วนตัวของคลังข้อมูลสำหรับบูรณาการข้อมูลผ่านบริการใช้ข้อมูลร่วมกัน

งานวิจัยการรักษาความเป็นส่วนตัวของคลังข้อมูลสำหรับบูรณาการข้อมูลผ่านบริการใช้ข้อมูลร่วมกัน (A Privacy Preserving Repository for Data Integration across Data Sharing Services) [12] เป็นงานวิจัยเพื่อให้เป็นไปตามความต้องการของผู้ใช้งานด้านการบูรณาการข้อมูลที่ใช้งานร่วมกัน ประโยชน์ของงานวิจัยที่คาดว่าจะได้รับคือ

1. บริการที่ใช้งานข้อมูลร่วมกัน สามารถอัปเดตและควบคุมการเข้าถึงข้อมูล และใช้งานข้อมูลที่แบ่งปันในคลังข้อมูล
2. ข้อมูลที่แบ่งปัน เป็นข้อมูลที่แบ่งปันโดยใช้หลักการการแบ่งปันเฉพาะข้อมูลที่จำเป็น (Need-to-share)
3. คลังข้อมูล สามารถจำกัดการเก็บรวบรวมข้อมูลจากบริการใช้งานข้อมูลร่วมกันและบูรณาการเพื่อให้เกิดความเหมาะสมกับความต้องการของผู้ใช้

สถาปัตยกรรมและข้อสมมุติฐาน ในงานวิจัยนี้มีสมมุติฐานว่าคลังข้อมูลคือ เป็นศูนย์กลางการเก็บรวบรวมข้อมูล โดยในรูปที่ 2.6 อธิบายได้ว่า แอปพลิเคชันผู้ใช้งานส่งคำร้องไปยังคลังข้อมูล คลังข้อมูลจะดำเนินการวางแผนคิวรี คลังข้อมูลดำเนินการค้นหาข้อมูลโดยผ่านกระบวนการที่ตระหนักถึงการแบ่งปัน จากนั้นคืนผลลัพธ์คำร้องให้กับผู้ใช้งาน



รูปที่ 2.6 ภาพรวมงานวิจัยการรักษาความเป็นส่วนตัวของคลังข้อมูล [12]

ดังปรากฏในรูปที่ 2.6 คลังข้อมูลมี 2 องค์ประกอบหลักคือ ตัวดำเนินการแรบแพนคิวรี (Query Plan Wrapper) ซึ่งทำหน้าที่ในการวิเคราะห์ บำรุงการความต้องการและสร้างคิวรีที่แรบ เพื่อส่งให้กับตัวดำเนินการแผนคิวรี (Query Plan Executor) ซึ่งในการรักษาความเป็นส่วนตัวของคลังข้อมูล สำหรับบำรุงการข้อมูลผ่านบริการใช้ข้อมูลร่วมกันได้กำหนดนิยามคือ

นิยามที่ 1 (Query Plan) แผนคิวรีคือ บางส่วนของลำดับกลุ่มของคิวรี $\{ p_1, p_2, \dots, p_m \}$ ซึ่งมี 2 คุณสมบัติคือ

- ในแต่ละ p_i สามารถถูกประเมินหลังจากที่ทุก p_j ก่อนหน้าทุกคิวรีถูกประเมินแล้ว
- แต่ละ p_i สามารถใช้ข้อมูลได้โดยตรงจากข้อมูลที่ใช้งานร่วมกัน

นิยามที่ 2 (Privacy Preserving Repository) สำหรับแผนคิวรี หรือ $P = \{ p_1, p_2, \dots, p_m \}$ และคลังข้อมูลคือ REP

งานวิจัยนี้นำเสนอการพัฒนาคลังข้อมูลเพื่ออำนวยความสะดวกในการบูรณาการใช้งานข้อมูลร่วมกัน โดยการรักษาความเป็นส่วนตัวของคลังข้อมูล REP โดยมีขั้นตอนดังนี้

ขั้นตอนที่ 1: ผู้ใช้งานส่งคีย์สาธารณะ pk และความต้องการเกี่ยวกับการใช้งานข้อมูลมาที่คลังข้อมูล REP

ขั้นตอนที่ 2: แรบแพนคิวรีของ REP ดำเนินการวิเคราะห์ความต้องการของผู้ใช้และเปลี่ยนความต้องการนั้นให้เป็นกราฟแผนคิวรี G แล้วแยก G ให้เป็นกลุ่มของกราฟย่อย $\{ G_1, G_2, \dots, G_m \}$ แล้วส่งกราฟย่อยไปให้กับตัวดำเนินการตามแผนคิวรี

ขั้นตอนที่ 3: ตัวดำเนินการตามแผนคิวรี รับผิดชอบดูแลบริการการใช้ข้อมูลร่วมกัน S_i โดยที่จะส่ง G_i ให้กับ S_i เพื่อดำเนินการต่อ

ขั้นตอนที่ 4: ตัวดำเนินการตามแผนคิวรีดำเนินการตาม *Integrate Algorithm* โดยให้ผลลัพธ์คือ *FinalRes* ซึ่งเป็นผลลัพธ์สุดท้ายและดำเนินการเข้ารหัสผลลัพธ์กับ pk ของผู้ใช้งาน

ขั้นตอนที่ 5: REP ส่งคือผลลัพธ์ที่เข้ารหัสให้กับผู้ใช้งาน ผู้ใช้งานสามารถใช้ข้อมูลได้โดยการใช้คีย์ส่วนตัว sk ของผู้ใช้งานถอดรหัสคำร้องที่ส่งกลับมาจากคลังข้อมูล

สรุปงานวิจัยนี้เสนอแนวคิดเพื่อให้การสื่อสารระหว่างแอปพลิเคชันของผู้ใช้งานกับคลังข้อมูลที่มีการใช้งานข้อมูลร่วมกัน เพื่อให้เกิดความมั่นคงโดยการแรบแพนคิวรีที่ส่งออกไปยังคลังข้อมูลพร้อมคีย์สาธารณะของผู้ใช้ ผลลัพธ์ที่ได้รับคืนจากคลังข้อมูลจะถูกเข้ารหัสโดยคีย์สาธารณะของผู้ใช้งาน เพื่อให้ผู้ใช้งานถอดรหัสข้อมูลโดยใช้คีย์ส่วนตัวผู้ใช้งาน เพื่อให้เกิดความมั่นคงในการใช้งานคลังข้อมูล

บทที่ 3 การสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซี

ในบทนี้จะกล่าวถึงการสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง โดยมีขั้นตอนคือ ศึกษากระบวนการปัจจุบันของหน่วยงานกรณีศึกษาในงานวิจัย การทำงานวิจัย การสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซี การวิเคราะห์ออกแบบเครื่องมือสนับสนุน การสกัด เอนทิตีนโยบาย สรุปผลการประยุกต์แนวปฏิบัติพีบีดีพีไอเข้ากับคลังสารสนเทศกลาง โดยมีรายละเอียดดังต่อไปนี้

3.1 การศึกษาระบบงานปัจจุบัน

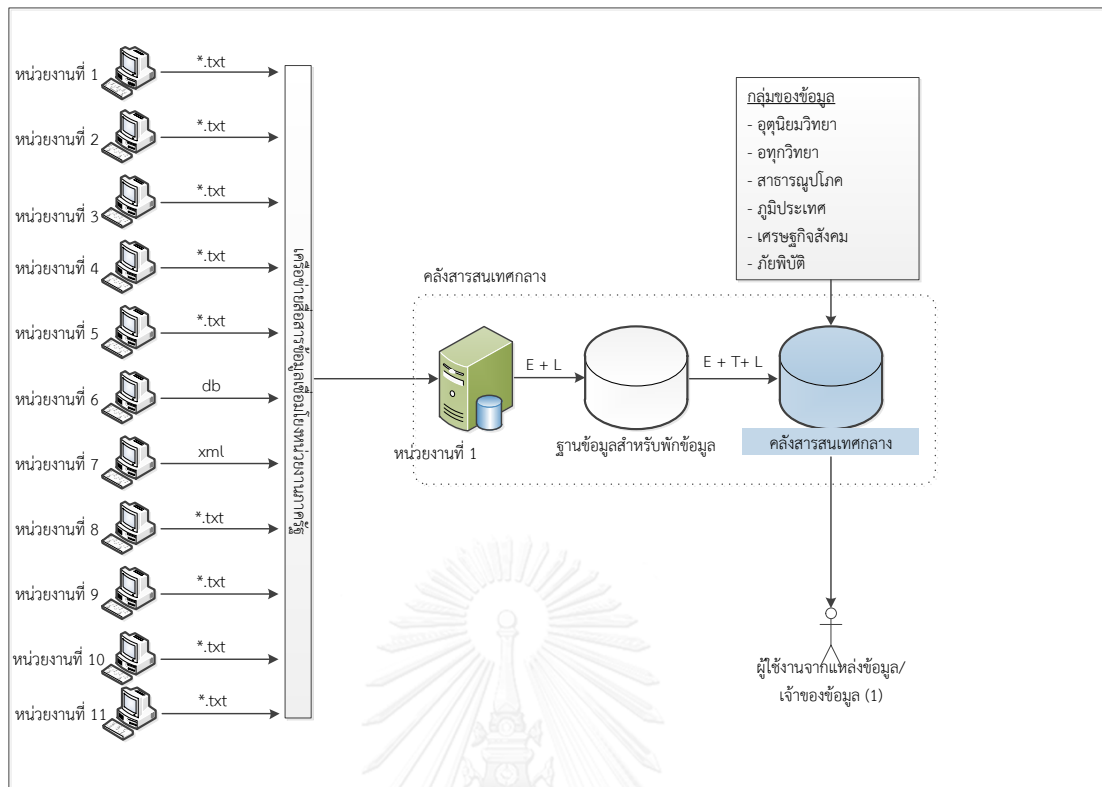
จากการศึกษาระบบคลังสารสนเทศกลางที่ใช้งานอยู่ในปัจจุบัน มีกระบวนการได้มาของข้อมูลคือ การเชื่อมโยงข้อมูลจากแต่ละแหล่งข้อมูล ขั้นตอนการเชื่อมโยงข้อมูลในคลังสารสนเทศกลางมีรายละเอียดดังนี้

3.1.1 กระบวนการรวบรวมและการเชื่อมโยงข้อมูลในคลังสารสนเทศกลาง

กระบวนการรวบรวมข้อมูลแต่ละหน่วยงานเพื่อเชื่อมโยงข้อมูล เริ่มจากคลังสารสนเทศกลาง ส่งแบบฟอร์มขอความร่วมมือเชื่อมโยงข้อมูลไปยังแต่ละแหล่งของข้อมูลที่เกี่ยวข้องกับการบริหารจัดการทรัพยากรน้ำเมื่อแหล่งข้อมูลตอบรับการเชื่อมโยง พร้อมกับส่งรายการรายละเอียดข้อมูลที่ต้องการเชื่อมโยงกับคลังสารสนเทศกลางเพื่อให้คลังสารสนเทศกลางดำเนินการเชื่อมโยงต่อไป

3.1.2 กระบวนการเชื่อมโยงนำเข้าข้อมูลในคลังสารสนเทศกลาง

ในหัวข้อนี้จะกล่าวถึงกระบวนการเชื่อมโยงข้อมูลในคลังสารสนเทศกลาง กระบวนการเชื่อมโยงข้อมูลกับหน่วยงานต่างๆ จะทำผ่านเครือข่ายหน่วยงานภาครัฐ (GIN) ข้อมูลที่ทำการเชื่อมโยงมีอยู่ 2 รูปแบบคือ ข้อมูลรูปแบบอพลวัต (Static Data) เป็นข้อมูลที่ใช้สำหรับการอ้างอิงเช่น ข้อมูลพื้นฐานต่างๆ ตำแหน่งที่ตั้งของเขื่อน ขนาดความจุ ปริมาตรกักเก็บน้ำ หรืออำเภอ ตำบล จังหวัดที่เป็นที่ตั้งของเครื่องวัดระดับปริมาณน้ำฝน เป็นต้น ข้อมูลแบบพลวัต (Dynamic Data) เป็นข้อมูลที่เกิดขึ้นอยู่ตลอดเวลา เช่น ระดับน้ำในแม่น้ำ ระดับน้ำในเขื่อน ปริมาณน้ำฝน อุณหภูมิ ความชื้นสัมพัทธ์ ความเข้มแสง ความเร็วลม ทิศทางลม เป็นต้น ซึ่งกระบวนการเชื่อมโยงข้อมูล กระบวนการเชื่อมโยงนำเข้าข้อมูลโดยแสดงในรูปที่ 3.1



รูปที่ 3.1 ภาพรวมการเชื่อมโยงข้อมูลสำหรับคลังสารสนเทศกลางของหน่วยงานการศึกษา

กระบวนการเชื่อมโยงข้อมูลดังที่ปรากฏอยู่ในรูป 3.1 แสดงกระบวนการเชื่อมโยงนำเข้าข้อมูลแบบพลวัต ข้อมูลที่เชื่อมโยงระหว่างแหล่งข้อมูลจนมาถึงการจัดเก็บในฐานข้อมูลสำหรับพักข้อมูล

3.1.3 กระบวนการแปลงข้อมูลให้อยู่ในรูปแบบเดียวกันเพื่อพร้อมใช้งาน

กระบวนการแปลงข้อมูลเป็นกระบวนการที่เกิดขึ้นระหว่างฐานข้อมูลสำหรับพักข้อมูลและฐานข้อมูลคลังสารสนเทศกลาง โดยในปัจจุบันคลังสารสนเทศกลางใช้เครื่องมืออัตโนมัติที่สามารถแปลงข้อมูลจากฐานข้อมูลสำหรับพักข้อมูลก่อนที่จะเก็บข้อมูลที่ผ่านการแปลงให้อยู่ในรูปแบบเดียวกันในเก็บไว้ในคลังสารสนเทศกลาง

3.1.4 การให้บริการข้อมูล

การให้บริการข้อมูลสำหรับคลังสารสนเทศกลางในปัจจุบัน แหล่งข้อมูลที่เชื่อมโยงข้อมูลกับคลังสารสนเทศกลางต้องลงทะเบียนใช้งานเพื่อให้ทราบว่ามาจากแหล่งข้อมูลหรือหน่วยงานใด เมื่อทำการลงทะเบียนแล้วเสร็จหน่วยงานหรือเจ้าของข้อมูลสามารถเข้าถึงข้อมูลที่อยู่ในคลังสารสนเทศกลางเพื่อใช้งานดังปรากฏอยู่ในรูปที่ 3.1 (1)

3.1.5 สรุปปัญหาจากการศึกษาระบบงานคลังสารสนเทศกลางปัจจุบัน

สรุปจากการศึกษาระบบคลังสารสนเทศกลางในปัจจุบันพบว่า มีสิ่งที่จะต้องพิจารณา ดังต่อไปนี้

1. การเข้าถึงข้อมูลที่เกี่ยวข้องอยู่ในคลังสารสนเทศกลางไม่มีการกำหนดนโยบายการใช้งานข้อมูลอย่างชัดเจน
2. ไม่มีการกำหนดบทบาทของผู้ใช้งานในคลังสารสนเทศกลาง
3. ไม่มีการกำหนดขอบเขตข้อจำกัดการใช้งานหรือเข้าถึงข้อมูลในคลังสารสนเทศกลาง
4. การนำข้อมูลที่อยู่ในคลังสารสนเทศกลางที่ผู้ใช้งานไม่มีสิทธิ ไปใช้งานโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

จากปัญหาที่ได้กล่าวข้างต้นหน่วยงานกรณีศึกษาจึงจำเป็นต้องดำเนินการเพื่อกำหนดนโยบายการใช้งานคลังสารสนเทศกลาง เพื่อใช้ในการกำหนดสิทธิให้กับผู้ใช้งานให้เข้าถึงข้อมูล จัดการข้อมูลเป็นไปตามวัตถุประสงค์ขององค์กรที่กำหนด

ดังนั้นจากประเด็นปัญหาดังกล่าวผู้วิจัยได้นำเสนอขั้นตอนการสร้างนโยบายการใช้งานสำหรับคลังสารสนเทศกลางโดยการประยุกต์ใช้แนวปฏิบัติพีบีดีพีไอเอ และการนำนโยบายการใช้งานดังกล่าวเป็นข้อมูลนำเข้าเพื่อออกแบบและสร้างเครื่องมือสนับสนุน เพื่อให้การใช้งานข้อมูลในคลังสารสนเทศกลางเป็นไปตามนโยบายที่กำหนดและเพื่อเป็นการแก้ไขปัญหาดังที่กล่าวมา

3.2 ขั้นตอนการทำงานวิจัย

หัวข้อขั้นตอนการทำงานวิจัยนำเสนอแนวคิดการสร้างนโยบายการใช้งานคลังสารสนเทศกลางและขั้นตอนการพัฒนาแอปพลิเคชันสำหรับคลังสารสนเทศกลางหรือเครื่องมือสนับสนุน

จากการวิเคราะห์แนวปฏิบัติกรอบงานพีบีดีพีไอเอเพื่อประยุกต์ใช้กับคลังสารสนเทศกลางสำหรับขั้นตอนหรือกระบวนการก่อนจะดำเนินการสร้างนโยบายการใช้งานคลังสารสนเทศกลาง องค์กรจะต้องพิจารณาและคำนึงถึงโครงสร้างขององค์กรเพื่อให้เกิดการสนับสนุนการสร้างนโยบายที่ตระหนักถึงไพรเวซี ในกรณีศึกษาที่ผู้ทำงานวิจัยได้วิเคราะห์แนวปฏิบัติพีบีดีพีไอเอและได้จัดทำโครงสร้างองค์กรของคลังสารสนเทศกลางเพื่อให้เกิดการตระหนักถึงไพรเวซีในคลังสารสนเทศกลาง ซึ่งสามารถนำโครงสร้างองค์กรนี้ไปปรับใช้ให้เหมาะสมกับคลังสารสนเทศด้านอื่นหรือลักษณะงานที่คล้ายคลึงกัน รายละเอียดของโครงสร้างองค์กรดังปรากฏในรูปที่ 3.2



รูปที่ 3.2 โครงสร้างองค์กรและภาระหน้าที่ของกรณีศึกษาคลังสารสนเทศกลาง

1. คณะผู้บริหารคลังสารสนเทศกลาง

- กำหนด/เลือกมาตรฐานระดับสากลด้านโทรเวชและความมั่นคง คณะผู้บริหารของคลังสารสนเทศกลางเป็นผู้ทำหน้าที่ในการพิจารณาและผลักดันนำเอามาตรฐานที่เหมาะสมด้านโทรเวชและความมั่นคงในระดับสากลมาใช้กับคลังสารสนเทศกลาง พร้อมทั้งกำหนดกรอบนโยบายกฎระเบียบการดำเนินงานสำหรับคลังสารสนเทศกลาง

2. คณะผู้บริหารคลังสารสนเทศกลาง

- กำหนด/เลือกมาตรฐานระดับสากลด้านโทรเวชและความมั่นคง คณะผู้บริหารของคลังสารสนเทศกลางเป็นผู้ทำหน้าที่ในการพิจารณาและผลักดันให้เกิดการนำเอามาตรฐานที่เหมาะสมด้านโทรเวชและความมั่นคงในระดับสากลมาใช้กับคลังสารสนเทศกลาง พร้อมทั้งกำหนดกรอบนโยบาย กฎระเบียบสำหรับการดำเนินงานในคลังสารสนเทศกลาง

3. ฝ่ายนโยบายไอทีและความมั่นคง

- กำหนดผู้ทำหน้าที่ด้านไอทีและความมั่นคง แผนกนโยบายไอทีและความมั่นคงทำหน้าที่กำหนดผู้รับผิดชอบด้านไอทีและความมั่นคงเพื่อให้ดำเนินกิจกรรมบำรุงรักษา ปกป้องข้อมูลและอื่นๆ ที่เกี่ยวข้องกับไอทีและความมั่นคงภายในคลังสารสนเทศกลาง
- ประเมินผลกระทบและความเสี่ยงที่อาจเกิดขึ้น แผนกนโยบายไอทีและความมั่นคงดำเนินการประเมินผลกระทบที่อาจเกิดขึ้น ในกรณีที่เกิดความบกพร่องด้านไอทีและความมั่นคง ทั้งนี้การประเมินเพื่อให้เกิดข้อสรุปและป้องกันก่อนที่จะเกิดเหตุการณ์นั้น
- จัดทำกฎระเบียบ กระบวนการใช้งานข้อมูล แผนกนโยบายไอทีและความมั่นคงเป็นผู้กำหนดกฎระเบียบการใช้งานข้อมูลที่อยู่ในคลังสารสนเทศกลาง กระบวนการระหว่างผู้ใช้งานกับคลังสารสนเทศกลางรวมถึงข้อจำกัดในการใช้งาน จัดทำเอกสารเผยแพร่ให้ผู้เกี่ยวข้องได้รับทราบ
- กำหนดระเบียบการเก็บรักษา/ทำลายข้อมูลและคำชี้แจง แผนกนโยบายไอทีและความมั่นคงเป็นผู้พิจารณากำหนดกฎระเบียบสำหรับการเก็บรักษา ทำลายข้อมูลพร้อมทั้งจัดทำเอกสารชี้แจงรายละเอียดเหตุการณ์การเก็บรักษา การทำลาย
- กำหนดช่วงเวลาเพื่อทวนสอบกฎระเบียบนโยบาย แผนกนโยบายไอทีและความมั่นคงควรมีการกำหนดช่วงเวลาเพื่อทวนสอบกฎระเบียบด้านไอทีและความมั่นคงที่ใช้อยู่เพื่อปรับปรุงให้สอดคล้องกับสถานการณ์ และเทคโนโลยีที่เปลี่ยนแปลง
- กำหนดรายการความต้องการด้านไอทีและความมั่นคง แผนกนโยบายไอทีและความมั่นคงเป็นผู้ดำเนินการจัดทำรายการความต้องการด้านไอทีและความมั่นคง โดยรายการความต้องการที่ได้จะนำไปสู่การพัฒนาเครื่องมือสับเพื่อใช้ในคลังสารสนเทศกลางดำเนินการพัฒนาโดยแผนกวิจัยและพัฒนา

4. ฝ่ายวิจัยและพัฒนา

- ดำเนินการออกแบบและพัฒนาเครื่องมือสนับสนุนการทำงานด้านไอทีและความมั่นคง แผนกวิจัยและพัฒนาดำเนินการออกแบบพัฒนาเครื่องมือสนับสนุนเพื่อใช้ในคลังสารสนเทศกลาง สำหรับในงานวิจัยนี้ได้ดำเนินการในส่วนนี้ โดยได้ทำการวิเคราะห์แนวปฏิบัติที่ดีพีไอเอ (ตาราง ง.1) มาเป็นแผนภาพคลาส (ภาคผนวก ง รูปที่ ง.40-ง.46) และนำมาพัฒนาเป็นเครื่องมือสนับสนุนสำหรับคลังสารสนเทศ รายละเอียดในการพัฒนาออกแบบและเครื่องมือสนับสนุนจะกล่าวโดยละเอียดในบทที่ 4

5. ฝ่ายตรวจสอบ

- ตรวจสอบการปฏิบัติตามนโยบายไพรเวซีและความมั่นคง กระบวนการที่กำหนด ฝ่ายตรวจสอบดำเนินการตรวจสอบการปฏิบัติงานของคลังสารสนเทศกลางว่าเป็นไปตามนโยบายไพรเวซีและความมั่นคงรวมถึงกระบวนการที่ได้กำหนดขึ้น
- กำหนดช่วงเวลาเพื่อให้หน่วยงานภายนอกประเมินตรวจสอบ ฝ่ายตรวจสอบคลังสารสนเทศกลางกำหนดวันเวลาเพื่อให้หน่วยงานภายนอกคลังสารสนเทศกลางดำเนินการตรวจสอบการปฏิบัติการนโยบายที่กำหนดใช้
- กำหนดเกณฑ์ชี้วัดประโยชน์ที่ได้รับและวัตถุประสงค์การดำเนินงาน ฝ่ายตรวจสอบเป็นผู้กำหนดเกณฑ์ชี้วัดและดำเนินการตรวจสอบประเมินการดำเนินงานของคลังสารสนเทศกลางเพื่อให้การดำเนินงานเป็นไปตามวัตถุประสงค์และได้ประโยชน์ตามที่คาดหวัง

6. ฝ่ายสื่อสารองค์กร

- เปิดเผยข้อมูลด้านไพรเวซีและความมั่นคง กระบวนการดำเนินธุรกิจ เพื่อให้เกิดความโปร่งใสในการดำเนินงาน ผู้เกี่ยวข้องสามารถเข้าถึงเอกสารด้านไพรเวซีและความมั่นคงของคลังสารสนเทศกลางเพื่อทราบถึงวัตถุประสงค์การดำเนินงาน การเก็บ การใช้งานและการเปิดเผยข้อมูล
- จัดอบรมหลักสูตรเพื่อให้เกิดการตระหนักถึงไพรเวซีและความมั่นคง เพื่อให้ผู้ที่เกี่ยวข้องได้รับการอบรมเพื่อให้เข้าใจถึงบทบาทหน้าที่สิทธิตลอดจนหลักการ วิธีการและแนวปฏิบัติขององค์กร
- เปิดเผยเอกสารด้านสถาปัตยกรรมด้านไพรเวซีและความมั่นคง เพื่อให้ผู้ที่เกี่ยวข้องได้รับทราบสถาปัตยกรรมไพรเวซีและความมั่นคงของคลังสารสนเทศกลางเพื่อให้เกิดความโปร่งใส
- เปิดเผยรายงานการตรวจสอบด้านไพรเวซีและความมั่นคง ฝ่ายสื่อสารองค์กรต้องเปิดเผยเอกสารที่ได้จากฝ่ายตรวจสอบ ผลการประเมินต่างๆ ที่เกิดขึ้นเพื่อให้ผู้เกี่ยวข้องได้รับทราบ

7. ผู้ใช้งานข้อมูล

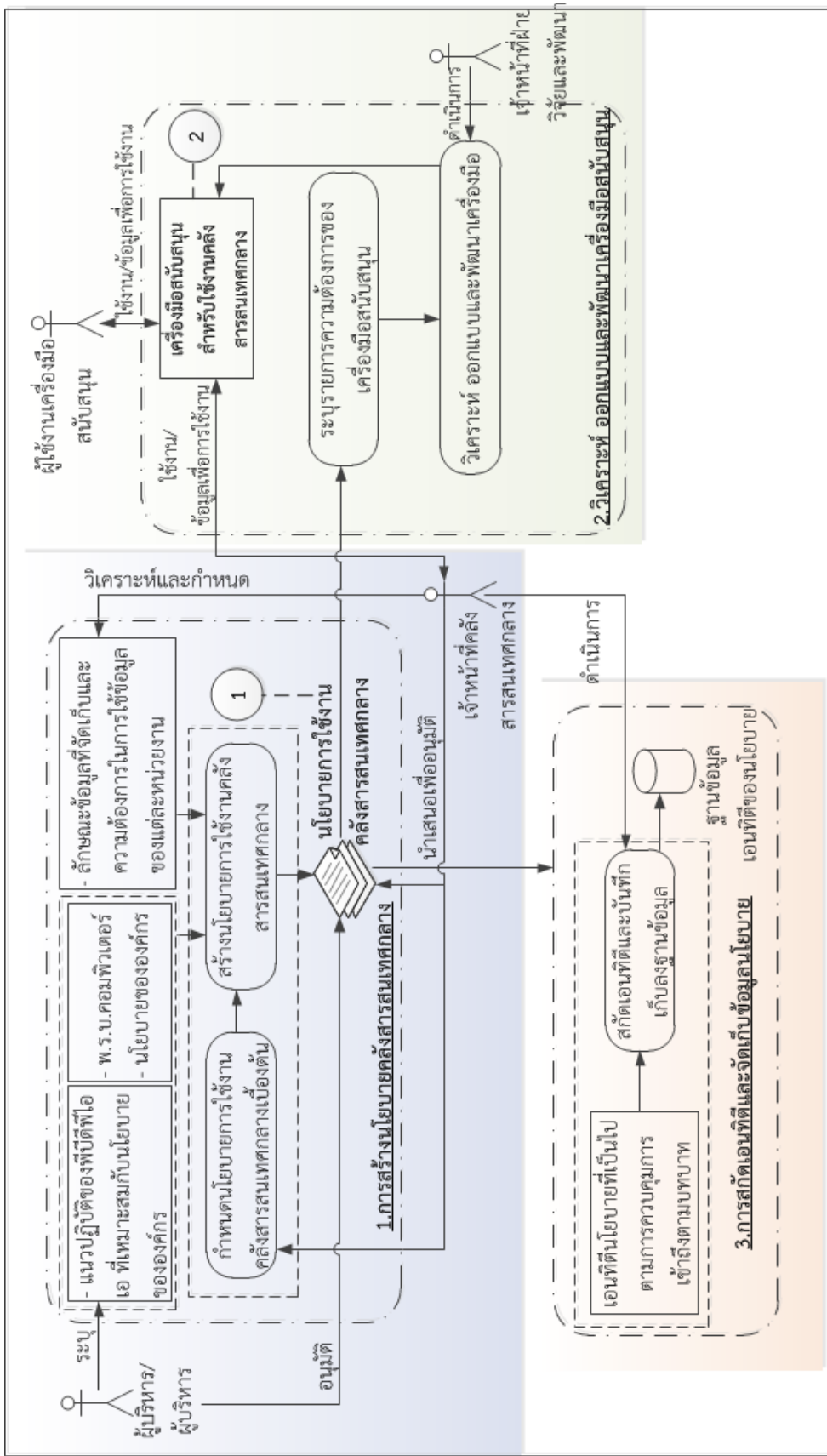
- เข้าถึงเอกสาร/รายงานขององค์กร ผู้ใช้งานหรือผู้เกี่ยวข้องสามารถเข้าถึงเอกสารรายงานของคลังสารสนเทศกลางได้
- ใช้งานเครื่องมือตามนโยบายที่กำหนด ผู้ใช้งานหรือผู้เกี่ยวข้องสามารถใช้งานเครื่องมือสนับสนุนที่ฝ่ายวิจัยและพัฒนาออกแบบและพัฒนา โดยการใช้งานเป็นไปตามนโยบายการใช้งานคลังสารสนเทศกลาง

แนวคิดการสร้างและการนำเอานโยบายการใช้งานคลังสารสนเทศกลางไปใช้งานดังปรากฏในรูปที่ 3.3 แสดงให้เห็นถึงกระบวนการสำคัญประกอบด้วย 3 ขั้นตอนคือ ขั้นตอนสร้างนโยบายคลังสารสนเทศกลาง ขั้นตอนการวิเคราะห์ ออกแบบและพัฒนาเครื่องมือสนับสนุน ขั้นตอนการสกัดเอนทิตีและจัดเก็บข้อมูลนโยบายการใช้งาน มีรายละเอียดดังต่อไปนี้

1) ขั้นตอนการสร้างนโยบายคลังสารสนเทศกลางคือ ขั้นตอนเพื่อให้ได้มาซึ่งนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี โดยมีข้อมูลนำเข้าหลายรายการเช่น แนวปฏิบัติของพีบีดีพีไอเอ พ.ร.บ.คอมพิวเตอร์ และนโยบายขององค์กร เป็นต้น

2) ขั้นตอนวิเคราะห์ ออกแบบและพัฒนาเครื่องมือสนับสนุนคือ ขั้นตอนถัดจากขั้นตอนการสร้างนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี โดยนโยบายดังกล่าวจะถูกใช้เป็นข้อมูลนำเข้าเพื่อวิเคราะห์ระบุรายการความต้องการ ออกแบบและพัฒนาเครื่องมือสนับสนุนต่อไป

3) ขั้นตอนการสกัดเอนทิตีและจัดเก็บข้อมูลนโยบายการใช้งานคือ ขั้นตอนหลังจากที่พัฒนาเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางแล้วเสร็จ เครื่องมือสนับสนุนดังกล่าวจะถูกใช้ในการสกัดเอนทิตีของนโยบายการใช้งานคลังสารสนเทศกลางซึ่งประกอบด้วยข้อมูลที่สำคัญ เช่น บทบาทผู้ใช้งาน ข้อมูล การกระทำ วัตถุประสงค์ เงื่อนไขและข้อผูกพัน เป็นต้น และจัดเก็บในฐานข้อมูลเพื่อใช้ในการกำหนดสิทธิการใช้งานข้อมูลในคลังสารสนเทศต่อไป

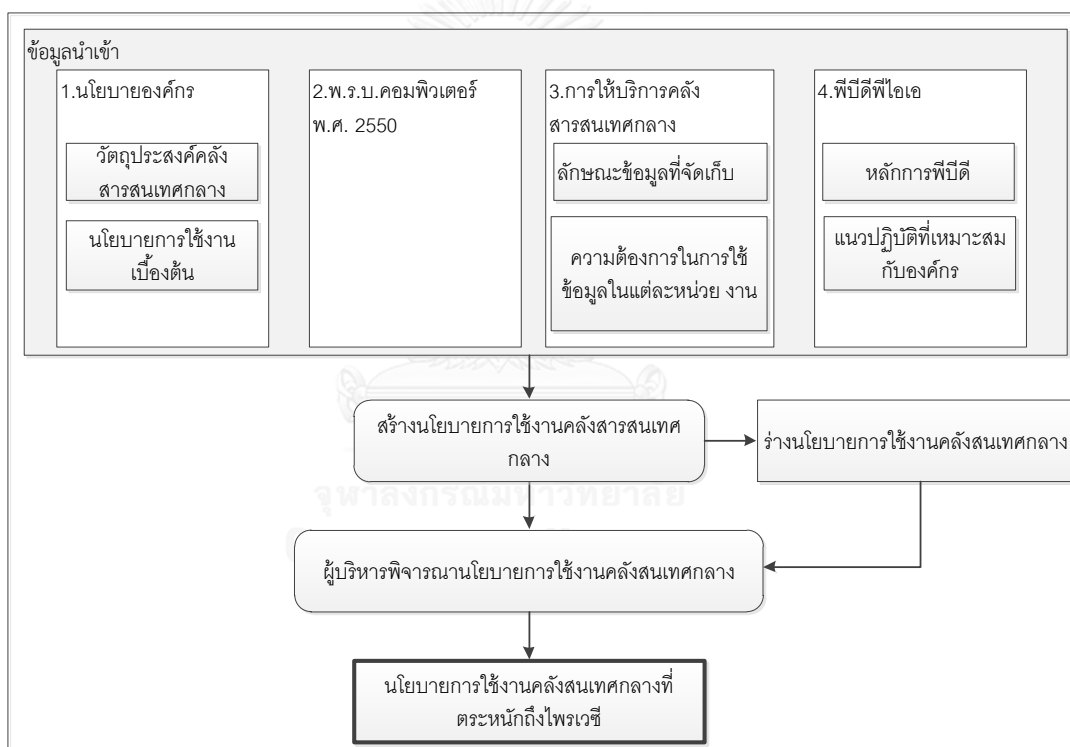


รูปที่ 3.3 แนวคิดการสร้างและการนำนโยบายการใช้งานคลังสารสนเทศกลางไปใช้งาน

3.3 การสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง

วัตถุประสงค์การสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง เพื่อให้เกิดการใช้งานข้อมูลที่อยู่ในคลังสารสนเทศกลางเป็นไปตามบทบาท และวัตถุประสงค์ในการเก็บรวบรวม โดยผลลัพธ์ที่ได้คือ นโยบายจะใช้เป็นข้อมูลนำเข้าเพื่อใช้ในการพิจารณาสร้างรายการความต้องการของเครื่องมือสนับสนุนต่อไป

ข้อมูลนำเข้าที่ใช้ในการสร้างนโยบายการใช้งาน ขั้นตอนการสร้างนโยบายอธิบายถึงกระบวนการขั้นตอนผู้ที่มีส่วนเกี่ยวข้องในการสร้างนโยบาย และข้อมูลนำออกคือ นโยบายการใช้งานคลังสารสนเทศกลางซึ่งผลลัพธ์เพื่อนำไปใช้งานต่อไป ภาพรวมของการสร้างนโยบายการใช้งานปรากฏอยู่ในรูปที่ 3.4 มีรายละเอียดดังนี้



รูปที่ 3.4 ภาพรวมการสร้างนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี

3.3.1 ข้อมูลนำเข้า

ข้อมูลนำเข้ากล่าวถึงรายละเอียดของรายการที่ต้องพิจารณาเพื่อใช้ในการสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลางโดยประกอบด้วย 4 ส่วน คือ นโยบายองค์กร

พ.ร.บ.คอมพิวเตอร์ การใช้บริการคลังสารสนเทศกลางและพีซีดีพีไอเอ ดังปรากฏดังรูปที่ 3.4 มีรายละเอียดดังนี้

1) นโยบายองค์กร การสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง จำเป็นต้องพิจารณาถึงความสอดคล้องกับนโยบายขององค์กร วัตถุประสงค์ของคลังสารสนเทศกลางซึ่งรวมไปถึงเป้าหมายและวิสัยทัศน์ขององค์กรด้วย อีกทั้งจำเป็นต้องพิจารณาถึงนโยบายการใช้งานเบื้องต้นที่ถูกกำหนดขึ้นเจ้าหน้าที่คลังสารสนเทศกลาง ซึ่งนโยบายการใช้งานเบื้องต้นยังไม่ได้มีการพิจารณาตระหนักถึงไพรเวซี

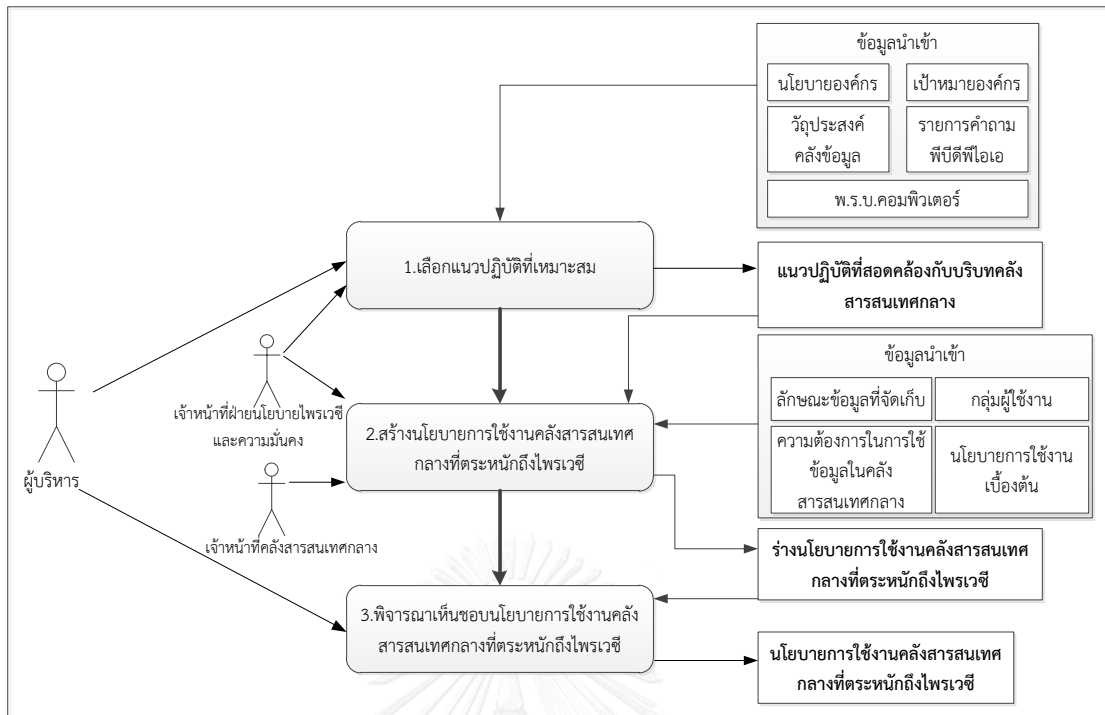
2) พ.ร.บ.คอมพิวเตอร์ เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และเพื่อให้เกิดระเบียบในการปฏิบัติการ การดำเนินงาน การกำหนดหน้าที่ภายในองค์กรให้เกิดความชัดเจนและถูกต้องในแนวทางเดียวกันด้านไอที และเพื่อเป็นการสร้างมาตรฐานให้กับองค์กรจึงใช้ พ.ร.บ.คอมพิวเตอร์เป็นข้อมูลนำเข้าในการสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง

3) การให้บริการคลังสารสนเทศกลาง เป็นข้อมูลนำเข้าเพื่อใช้วิเคราะห์สร้างนโยบายการใช้งานซึ่งประกอบด้วย ลักษณะข้อมูลที่จัดเก็บในคลังสารสนเทศกลาง เช่น ช่วงเวลาความถี่ของข้อมูล ประเภทข้อมูลที่เชื่อมโยงในแต่ละแหล่ง ลักษณะการจัดเก็บข้อมูลของจากแหล่งข้อมูล เป็นต้น และยังคงพิจารณาถึงความต้องการใช้งานข้อมูลที่อยู่ในคลังสารสนเทศกลาง เพื่อจัดเตรียมรูปแบบการให้บริการข้อมูลที่ตรงกับความต้องการ

4) พีซีดีพีไอเอเป็นสิ่งสำคัญที่จะต้องพิจารณาเพื่อให้คลังสารสนเทศกลางได้ตระหนักถึงไพรเวซีและความมั่นคง แนวปฏิบัติแต่ละข้อในพีซีดีพีไอเอจะถูกเลือกโดยผู้บริหารโดยพิจารณาให้เข้ากับบริบทคลังสารสนเทศกลาง (รายละเอียดเพิ่มเติมแนวปฏิบัติที่พิจารณาประยุกต์ใช้กับคลังสารสนเทศกลางแสดงอยู่ในภาคผนวก ง ตารางที่ ง.2) โดยในแต่ละแนวปฏิบัติของพีซีดีพีไอเอสอดคล้องหลักการของพีซีดี

3.3.2 ขั้นตอนการสร้างนโยบายการใช้งานคลังสารสนเทศกลาง

ขั้นตอนการสร้างนโยบายการใช้งานคลังสารสนเทศกลางกล่าวถึงกิจกรรมที่ทำในแต่ละขั้นตอนเช่น การเลือกแนวปฏิบัติที่เหมาะสม การสร้างนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี การพิจารณาเห็นชอบนโยบายการใช้งานคลังสารสนเทศกลาง ดังปรากฏอยู่ในรูปที่ 3.5 มีรายละเอียดดังนี้



รูปที่ 3.5 กิจกรรมการสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซี

1) ขั้นตอนการเลือกแนวปฏิบัติที่เหมาะสม

วัตถุประสงค์ของขั้นตอนนี้คือ การเลือกแนวปฏิบัติที่เหมาะสมสำหรับคลังสารสนเทศกลาง จากรายการคำถามพีบีดีพีไอเอ (ตาราง ง.1) โดยพิจารณาถึงนโยบายองค์กร เป้าหมายองค์กร วัตถุประสงค์การดำเนินงานของคลังสารสนเทศกลาง พ.ร.บ.คอมพิวเตอร์ โดยกระบวนการพิจารณาเลือกแนวปฏิบัติที่เหมาะสมกับคลังสารสนเทศกลางนั้นต้องสอดคล้องกับมาตรฐานด้านไพรเวซีตามที่ผู้บริหารคลังสารสนเทศกลางได้กำหนดเป็นแนวทาง เพื่อให้ฝ่ายนโยบายไพรเวซีและความมั่นคงพิจารณาเลือกแนวปฏิบัติที่สอดคล้องกับคลังสารสนเทศกลาง

ส่วนข้อมูลนำออกของขั้นตอนนี้คือ แนวปฏิบัติพีบีดีพีไอเอที่เหมาะสมกับคลังสารสนเทศกลาง แนวปฏิบัติที่เหมาะสมที่ผ่านการพิจารณาเลือกคำถามในแต่ละหลักการรายละเอียดเพิ่มเติมปรากฏอยู่ในตารางที่ ง.2 ภาคผนวก ง ในตารางที่ 3.1 แสดงตัวอย่างของแนวปฏิบัติพีบีดีพีไอเอที่ผ่านการเลือกในแต่ละหลักการของพีบีดี เพื่อนำมาใช้ในการพิจารณาสร้างนโยบายการใช้งานคลังสารสนเทศกลางต่อไป

ตารางที่ 3.1 ตัวอย่างแนวปฏิบัติที่สอดคล้องกับบริบทคลังสารสนเทศกลาง

หลักการปฏิบัติ	แนวปฏิบัติปฏิบัติที่เลือก	เหตุผลที่เลือก	ประโยชน์ที่ได้รับ
1) การป้องกันและคาดการณ์ก่อนที่จะเกิดกรรกราด้านโทรเวช	a) มีบุคคลได้รับมอบหมายให้ทำหน้าที่รับผิดชอบในการพัฒนา บำรุงรักษา และดำเนินการเรื่องสารสนเทศด้านโทรเวชขององค์กร และดำเนินการปกป้องข้อมูลหรือไม่? s) ได้มีการดำเนินการอบรมเพื่อให้เกิดการตระหนักถึงเรื่องความมั่นคงและโทรเวช?	เพื่อให้คลังสารสนเทศกลาง ดำเนินการกำหนดผู้ที่ทำหน้าที่รับผิดชอบด้านการบำรุงรักษา ปกป้องข้อมูลและดูแลสารสนเทศด้านโทรเวชขององค์กร	ช่วยให้คลังสารสนเทศกลางมีเจ้าหน้าที่ดูแลรับผิดชอบด้านการบำรุงรักษา ปกป้องข้อมูลขององค์กรอย่างชัดเจน
2) โทรเวชจะได้รับบริการป้องกันตั้งแต่เริ่มต้นใช้งาน แม้ไม่มีบริการกำหนดโดยผู้ใช้งาน	k) ได้มีการนำหลักการการเข้าถึงตามบทบาทมาใช้งานโดยอยู่บนฐาน ‘จำเป็นต้องรู้’ และ ‘สิทธิพื้นฐาน’ ?	เพื่อให้ผู้เกี่ยวข้องที่คลังสารสนเทศกลางได้ทราบถึงขั้นตอนการทำงาน และเข้าใจถึงบทบาทผู้ใช้งานในคลังสารสนเทศกลาง	ช่วยให้ผู้ใช้งานมีความเข้าใจในการใช้งานเครื่องมือรวมถึงบทบาทที่ได้รับ
3) โทรเวชที่ติดตั้งอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินงานกิจกรรมในองค์กร	k.10) ต้องมีการบังคับให้มีการตั้งรหัสผ่านที่ยากต่อการเดา รวมไปถึงมีการกำหนดขนาดความยาวอย่างน้อยเท่าไร ?	เพื่อสร้างความมั่นใจให้กับผู้เกี่ยวข้องที่คลังสารสนเทศกลางว่ารหัสผ่านที่ผู้ใช้กำหนดขึ้นใช้งานให้แยกต่อการคาดเดา	ช่วยสร้างความมั่นใจและช่วยให้ผู้ใช้งานวิธีสร้างรหัสผ่านที่เข้มแข็ง

ตารางที่ 3.4 ตัวอย่างแนวปฏิบัติที่สอดคล้องกับบริบทคลังสารสนเทศกลาง (ต่อ)

หลักการพิบัติ	แนวปฏิบัติที่เลือก	เหตุผลที่เลือก	ประโยชน์ที่ได้รับ
4) ให้ความสำคัญกับกฎระเบียบและวัตถุประสงค์โดยพิจารณาทั้งเรื่องประสิทธิภาพมั่นคง	b) ได้มีการกำหนดโครงสร้างและกลไกเมื่อหน่วยงานภายนอกต้องการเข้าถึงข้อมูล อาจจะต้องนำเข้าสู่ที่ประชุมหารือ เพื่อให้มั่นใจได้ว่าไม่มีการแย่งชิงหน้าที่ของไพรเวตออกจากความมั่นคง ?	เพื่อสร้างความมั่นใจและความน่าเชื่อถือให้กับผู้ที่เกี่ยวข้องคลังสารสนเทศกลาง	ช่วยให้สร้างภาพลักษณ์สำหรับคลังสารสนเทศกลางที่มีทั้งความมั่นคงและไพรเวตซีในการใช้งาน
5) ไพรเวตซีได้ถูกฝังอยู่ระบบตั้งแต่เริ่มกิจกรรมจนถึงสิ้นสุดกิจกรรมของข้อมูล	k.1) มีการกำหนดช่วงเวลาของกลุ่มข้อมูลที่เก็บรักษา ?	เพื่อแสดงให้เห็นกับผู้ที่เกี่ยวข้องกับคลังสารสนเทศกลาง ได้รับทราบช่วงเวลาของการจัดเก็บ ทำลาย ข้อมูลด้านไพรเวตซี	ช่วยให้เจ้าของข้อมูลทราบว่าข้อมูลจะไม่ถูกเก็บรักษาเพื่อใช้ประโยชน์อย่างอื่น
6) ความโปร่งใสในการดำเนินกิจกรรมด้านไพรเวตซีภายในองค์กรตามนโยบายที่ได้กำหนด	a) ได้มีการกำหนดข้อมูลที่ใช้ในการติดต่อสื่อสารของบุคคลในองค์กรทำหน้าที่รับผิดชอบด้านไพรเวตซีและความมั่นคง และเปิดเผยข้อมูลเหล่านี้ให้รับรู้ทั่วองค์กร ?	เพื่ออำนวยความสะดวกแก่ผู้เกี่ยวข้อง กับคลังสารสนเทศกลาง	ช่วยเพิ่มช่องทางติดต่อสื่อสารให้กับผู้ใช้งาน
7) ผู้เกี่ยวข้องด้านไพรเวตซีจะต้องสนับสนุนเพื่อที่ไพรเวตซีเกิดประโยชน์สูงสุดต่อผู้ใช้งาน	b) ทุกนโยบาย ขั้นตอนปฏิบัติและสารสนเทศเขียนอยู่ภาษาที่เข้าใจง่ายและผู้ใช้งานสามารถเข้าถึงได้โดยง่ายและเข้าถึงได้ทุกเมื่อ ?	เพื่อสร้างความโปร่งใสในการปฏิบัติงาน และการดำเนินงานของผู้เกี่ยวข้องคลังสารสนเทศกลาง	ช่วยให้เกิดความโปร่งใสในด้านการดำเนินงานในคลังสารสนเทศกลาง

2) ขั้นตอนการสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง

วัตถุประสงค์ของขั้นตอนนี้ คือเพื่อร่างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง ในขั้นตอนนี้เจ้าหน้าที่คลังสารสนเทศกลางและเจ้าหน้าที่จากฝ่ายนโยบายไพรเวซีและความมั่นคงจะทำหน้าที่กำหนดร่างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลางโดยพิจารณาข้อมูลนำเข้าดังนี้

- 1) แนวปฏิบัติที่ดีที่ไอเอทีที่สอดคล้องกับบริบทคลังสารสนเทศที่ผ่านการเลือก
- 2) ลักษณะข้อมูลที่จัดเก็บ ดังแสดงตัวอย่างข้อมูลที่จัดเก็บในตารางที่ 3.2
- 3) ความต้องการในการใช้ข้อมูลในคลังสารสนเทศกลางคือ แหล่งข้อมูลที่เชื่อมโยงข้อมูลให้กับคลังสารสนเทศกลางจะมีความต้องการใช้ข้อมูลที่แตกต่างกันเช่น แหล่งข้อมูลที่มีข้อมูลปริมาณน้ำในเขื่อน อาจจะมีความต้องการใช้ข้อมูลด้านปริมาณน้ำฝนเพื่อคำนวณปริมาณน้ำกักเก็บในเขื่อน เป็นต้น
- 4) นโยบายการใช้งานเบื้องต้นคือ นโยบายการใช้งานคลังสารสนเทศกลางเบื้องต้นที่ถูกกำหนดขึ้นโดยเจ้าหน้าที่คลังสารสนเทศกลางเป็นผู้กำหนดขึ้นเองยังไม่ได้มีการพิจารณาตระหนักถึงไพรเวซี ตัวอย่างของนโยบายการใช้งานเบื้องต้นแสดงอยู่ในตารางที่ 3.3
- 5) กลุ่มผู้ใช้งาน คือกลุ่มของผู้ใช้งานในคลังสารสนเทศกลางประกอบด้วย 2 กลุ่มผู้ใช้งานคือกลุ่มผู้ใช้งานที่เกี่ยวข้องกับการเชื่อมโยงข้อมูลและกลุ่มผู้ใช้งานทั่วไป รายละเอียดดังแสดงในตาราง 3.4

ตารางที่ 3.2 ตัวอย่างลักษณะข้อมูลที่จัดเก็บในคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

ชื่อข้อมูล	ช่วงเวลาความถี่ของข้อมูล	เวลาในการเชื่อมโยงข้อมูล
1. ปริมาณฝนรายชั่วโมง	10 นาที	ทุก 10 นาที
2. ปริมาณฝน 24 ชั่วโมง	1 ชั่วโมง	ทุกชั่วโมง
3. ปริมาณฝนรายวัน	-	-
4. ปริมาณน้ำในเขื่อน	1 วัน	ทุกวัน

ตารางที่ 3.3 ตัวอย่างนโยบายการใช้งานคลังสารสนเทศกลางเบื้องต้นของหน่วยงานกรณีศึกษา

1. นักวิจัยสามารถเรียกดูข้อมูลได้ต้องลงทะเบียนและเข้าสู่ระบบ สามารถเรียกดูข้อมูลระดับน้ำ ข้อมูลปริมาณน้ำ เชื้ออน ความเข้มแสง ความชื้น ความกดอากาศ อุณหภูมิ ระดับน้ำทะเล
2. เจ้าหน้าที่ของแต่ละหน่วยงานที่ให้ข้อมูลกับคลังสารสนเทศกลางสามารถเรียกดูข้อมูลได้ โดยต้องเข้าสู่ระบบ
3. ผู้ใช้งานคลังสารสนเทศกลาง จะได้รับสิทธิตามบทบาทหน้าที่รับผิดชอบ
4. ผู้ใช้งานคลังสารสนเทศต้องไม่เผยแพร่ข้อมูลที่อยู่ในคลังสารสนเทศกลางที่เป็นการหาประโยชน์ส่วนตัว ตามข้อบังคับการใช้งานคลังสารสนเทศกลาง
5. ผู้ใช้งานคลังสารสนเทศกลางจะต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ตารางที่ 3.4 ตัวอย่างกลุ่มผู้ใช้งานในคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

กลุ่มผู้ใช้งาน	บทบาท	หน้าที่ความรับผิดชอบ
เจ้าหน้าที่คลังสารสนเทศกลาง	เจ้าหน้าที่คลังสารสนเทศกลาง	บริหารจัดการกลุ่มผู้ใช้งาน มอบหมายสิทธิการใช้งาน การเข้าถึงข้อมูลในคลังสารสนเทศกลาง
กลุ่มผู้ใช้งานที่เกี่ยวข้องกับการเชื่อมโยงข้อมูล	นักวิจัย	สามารถนำข้อมูลออกมาใช้เพื่อวัตถุประสงค์สำหรับงานวิจัย
	นักพัฒนาระบบ	สามารถนำข้อมูลมาใช้งานเพื่อพัฒนาระบบ
	ผู้ดูแลฐานข้อมูล	สามารถเข้าถึงข้อมูลเพื่อตรวจสอบให้ข้อมูลพร้อมใช้งาน
	ตัวแทนหน่วยงาน	สามารถเข้าถึงข้อมูลและนำไปเอาไปใช้งานตามสิทธิที่ได้
กลุ่มผู้ใช้งานข้อมูล	ผู้บริหารระดับสูง	สามารถเข้าถึงข้อมูลผ่านการประมวลผลผ่านรายงานที่ระบบจัดเตรียมไว้
	นักวิชาการ	สามารถเข้าถึงข้อมูลบางประเภทที่สามารถใช้ประโยชน์เพื่องานด้านวิชาการ
	นักข่าว ประชาชนทั่วไป	สามารถเข้าถึงข้อมูลโดยทั่วไปที่ระบบจัดเตรียมไว้

ผลลัพธ์จากขั้นตอนนี้คือร่างนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี แสดงในตารางที่ 3.5 โดยมีรายละเอียดที่แสดงให้เห็นว่านโยบายการใช้งานแต่ละข้อนั้นสอดคล้องกับ หลักการและแนวปฏิบัติพีดีพีไอเอข้อไหน

ตารางที่ 3.5 ตัวอย่างร่างนโยบายการใช้งานคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

1.ร่างนโยบายคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี ตามแนวปฏิบัติที่เหมาะสม	มาจากหลักการพีดีพีไอเอและแนวปฏิบัติพีดีพีไอเอใน ตาราง ภาคผนวก ง.2 ข้อไหน
1.1) องค์กรจะต้องกำหนดผู้รับผิดชอบในการบำรุงรักษา จัดการเกี่ยวกับไพรเวซีของข้อมูล และไพรเวซีของผู้ใช้งาน ในคลังสารสนเทศกลางโดยประกาศให้รับทราบโดยทั่วกัน	หลักการพีดีพีไอเอข้อที่ 1 แนวปฏิบัติพีดีพีไอเอข้อ a
1.2) องค์กรจะต้องสร้างหลักสูตรอบรมการใช้งานข้อมูลใน คลังสารสนเทศกลางให้กับผู้ใช้งาน เพื่อความลดปัญหา ระหว่างการใช้งาน	หลักการพีดีพีไอเอข้อที่ 1 แนวปฏิบัติพีดีพีไอเอข้อ s
1.3) องค์กรจะต้องมีกลไกในการตรวจสอบตัวตนและสิทธิ ในการกระทำกับข้อมูลตามบทบาทของผู้ใช้งานที่ได้รับใน คลังสารสนเทศกลาง เพื่อป้องกันการละเมิดบทบาทหน้าที่ ของผู้ใช้งาน	หลักการพีดีพีไอเอข้อที่ 2 แนวปฏิบัติพีดีพีไอเอข้อ k
1.4) องค์กรจะต้องมีตัวช่วย หรือเครื่องมือแนะนำการตั้ง รหัสผ่านที่ยากต่อการคาดเดาให้กับผู้ใช้งาน โดยรหัสผ่าน จะต้องมีความปลอดภัยที่ดี เพื่อความปลอดภัยในการใช้งาน	หลักการพีดีพีไอเอข้อที่ 3 แนวปฏิบัติพีดีพีไอเอข้อ k.10
1.5) องค์กรจะต้องมีกลไกในการตรวจสอบความมั่นคง ไพรเวซีของข้อมูล และไพรเวซีของผู้ใช้งานในคลัง สารสนเทศกลาง เพื่อสร้างความมั่นใจในการใช้งาน	หลักการพีดีพีไอเอข้อที่ 4 แนวปฏิบัติพีดีพีไอเอข้อ b
1.6) องค์กรจะต้องมีการจัดทำตารางที่ระบุถึงการเก็บ การ รักษา หรือการทำลายข้อมูลที่อยู่ในคลังสารสนเทศกลาง ให้กับผู้ใช้งาน เพื่อความโปร่งใสและรับทราบโดยทั่วกัน	หลักการพีดีพีไอเอข้อที่ 5 แนวปฏิบัติพีดีพีไอเอข้อ k.1
1.7) องค์กรจะต้องกำหนดผู้รับผิดชอบด้านนโยบายไพรเวซี ของข้อมูลและความมั่นคงในคลังสารสนเทศกลางและ ประกาศช่องทางสื่อสารให้รับทราบโดยทั่วกัน	หลักการพีดีพีไอเอข้อที่ 6 แนวปฏิบัติพีดีพีไอเอข้อ a
1.8) องค์กรจะต้องจัดทำนโยบายการใช้งาน โดยใช้ภาษาที่ ง่ายต่อการทำความเข้าใจ เข้าถึงได้สะดวกให้กับผู้ใช้งาน และบุคคลทั่วไปรับทราบโดยทั่วกัน	หลักการพีดีพีไอเอข้อที่ 7 แนวปฏิบัติพีดีพีไอเอข้อ b

ตารางที่ 3.5 ตัวอย่างร่างนโยบายการใช้งานคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา (ต่อ)

2.ร่างนโยบายคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี พิจารณาจากนโยบายการใช้งานเบื้องต้น	มาจากหลักการพีบีดีและแนวปฏิบัติพีดีพีไอเอใน ตาราง ภาคผนวก ง.2 ข้อไหน
2.1) ผู้ใช้งานคลังสารสนเทศกลางจะต้องทำการลงทะเบียนและเข้าสู่ระบบก่อนการใช้งาน และเมื่อออกจากระบบระบบจะบันทึกประวัติการใช้งาน	หลักการพีบีดีที่ 2 แนวปฏิบัติพีดีพีไอเอข้อ g
2.2) ผู้ใช้งานที่ได้รับสิทธินักวิจัยสามารถเรียกดูข้อมูลระดับน้ำ ข้อมูลปริมาณน้ำเขื่อน ความเข้มแสง ความชื้น ความกดอากาศ อุณหภูมิ ระดับน้ำทะเล โดยมีวัตถุประสงค์เพื่อ งานวิจัยข้อมูลเท่านั้น และเมื่อต้องการเผยแพร่ข้อมูลต้อง ได้รับความยินยอมจากเจ้าของข้อมูล	หลักการพีบีดีที่ 2 แนวปฏิบัติพีดีพีไอเอข้อ b,c
2.3) ผู้ใช้งานที่ได้รับสิทธิเจ้าหน้าที่ประจำหน่วยงาน สามารถเรียกดูข้อมูลได้ เมื่อต้องการเปิดเผยข้อมูล ส่งต่อข้อมูล ต้องได้รับการยินยอมจากหน่วยงานเจ้าของข้อมูลก่อน โดยระบุวัตถุประสงค์เพื่อใช้ข้อมูล	หลักการพีบีดีที่ 7 แนวปฏิบัติพีดีพีไอเอข้อ a.1-3,l
2.4) ผู้ใช้งานคลังสารสนเทศกลาง จะได้รับสิทธิตามบทบาทหน้าที่ และความผิชอบ	หลักการพีบีดีที่ 3 แนวปฏิบัติพีดีพีไอเอข้อ k.8-10
2.5) ผู้ใช้งานคลังสารสนเทศต้องไม่เผยแพร่ข้อมูลที่อยู่ในคลังสารสนเทศกลาง เพื่อเป็นการหาประโยชน์เชิงพาณิชย์ ตามข้อบังคับการใช้งานคลังสารสนเทศกลาง	หลักการพีบีดีที่ 1 แนวปฏิบัติพีดีพีไอเอข้อ g
2.6) ผู้ใช้งานคลังสารสนเทศกลางจะต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	หลักการพีบีดีที่ 1 แนวปฏิบัติพีดีพีไอเอข้อ z

3) ขั้นตอนพิจารณาเห็นชอบนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี

ขั้นตอนพิจารณาเห็นชอบนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซีมีกิจกรรมดังนี้ เจ้าหน้าที่ฝ่ายไพรเวซีและความมั่นคงนำเสนอร่างนโยบายการใช้งานเสนอต่อผู้บริหารเพื่อพิจารณา ในกรณีที่ผู้บริหารมีมติให้ปรับแก้ไขร่างนโยบายการใช้งานคลังสารสนเทศกลางเจ้าหน้าที่ฝ่ายนโยบายไพรเวซีและความมั่นคงและเจ้าหน้าที่คลังสารสนเทศกลางต้องดำเนินการพิจารณาปรับแก้ตามความเห็นของผู้บริหาร และดำเนินการนำเสนอร่างนโยบายการใช้งานคลัง

สารสนเทศกลางต่อผู้บริหารอีกครั้ง เพื่อให้ผู้บริหารพิจารณาเห็นชอบนโยบายการใช้งาน ผลลัพธ์ของขั้นตอนนี้คือได้นโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลางที่ผ่านการพิจารณาเห็นชอบโดยผู้บริหาร ตัวอย่างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลางที่ผ่านการเห็นชอบจากผู้บริหารแสดงอยู่ในหัวข้อ 3.3.4 ในตารางที่ 3.6

3.3.3 ข้อมูลนำออก

ขั้นตอนนี้แสดงให้เห็นถึงผลลัพธ์สุดท้ายของการสร้างนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซีที่ผ่านการเห็นชอบของผู้บริหารแสดงในตารางที่ 3.6 ได้แสดงตัวอย่างนโยบายการใช้งานโดยแบ่งออกเป็น 2 ส่วนคือนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซีโดยพิจารณาจากแนวปฏิบัติที่เหมาะสม (ข้อ 1) และนโยบายการใช้งานคลังสารสนเทศที่ตระหนักถึงไพรเวซีโดยพิจารณาจากนโยบายการใช้งานเบื้องต้น (ข้อ 2)

ตารางที่ 3.6 ตัวอย่างนโยบายการใช้งานคลังสารสนเทศกลางของหน่วยงานหน่วยงานกรณีศึกษา

1.นโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซีตามแนวปฏิบัติที่เหมาะสม
1.1) องค์กรจะต้องกำหนดผู้รับผิดชอบในการบำรุงรักษา จัดการเกี่ยวกับไพรเวซีของข้อมูล และไพรเวซีของผู้ใช้งานในคลังสารสนเทศกลางโดยประกาศให้รับทราบโดยทั่วกัน
1.2) องค์กรจะต้องสร้างหลักสูตรอบรมการใช้งานข้อมูลในคลังสารสนเทศกลางให้กับผู้ใช้งาน เพื่อความลดปัญหา ระหว่างการใช้งาน
1.3) องค์กรจะต้องมีกลไกในการตรวจสอบตัวตนและสิทธิในการกระทำกับข้อมูลตามบทบาทของผู้ใช้งานที่ได้รับในคลังสารสนเทศกลาง เพื่อป้องกันการละเมิดบทบาทหน้าที่ของผู้ใช้งาน
1.4) องค์กรจะต้องมีตัวช่วย หรือเครื่องมือแนะนำการตั้งรหัสผ่านที่ยากต่อการคาดเดาให้กับผู้ใช้งาน โดยรหัสผ่านจะต้องมีคุณสมบัติที่ดี เพื่อความปลอดภัยในการใช้งาน
1.5) องค์กรจะต้องมีกลไกในการตรวจสอบความมั่นคง ไพรเวซีของข้อมูล และไพรเวซีของผู้ใช้งานในคลังสารสนเทศกลาง เพื่อสร้างความมั่นใจในการใช้งาน
1.6) องค์กรจะต้องมีการจัดทำตารางที่ระบุถึงการเก็บ การรักษา หรือการทำลายข้อมูลที่อยู่ในคลังสารสนเทศกลางให้กับผู้ใช้งาน เพื่อความโปร่งใสและรับทราบโดยทั่วกัน
1.7) องค์กรจะต้องกำหนดผู้รับผิดชอบด้านนโยบายไพรเวซีของข้อมูลและความมั่นคงในคลังสารสนเทศกลางและประกาศช่องทางการสื่อสารให้รับทราบโดยทั่วกัน
1.8) องค์กรจะต้องจัดทำนโยบายการใช้งาน โดยใช้ภาษาที่ง่ายต่อการทำความเข้าใจง่าย เข้าถึงได้สะดวกให้กับผู้ใช้งานและบุคคลทั่วไปรับทราบโดยทั่วกัน

ตารางที่ 3.6 ตัวอย่างนโยบายการใช้งานคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา (ต่อ)

2.นโยบายคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี พิจารณาจากนโยบายการใช้งานเบื้องต้น
2.1) ผู้ใช้งานคลังสารสนเทศกลางจะต้องทำการลงทะเบียน และเข้าสู่ระบบก่อนการใช้งาน และเมื่อออกจากระบบ ระบบจะบันทึกประวัติการใช้งาน
2.2) ผู้ใช้งานที่ได้รับสิทธินักวิจัยเข้าสู่ระบบสามารถเรียกดูข้อมูลระดับน้ำ ข้อมูลปริมาณน้ำเขื่อน ความเข้มแสง ความชื้น ความกดอากาศ อุณหภูมิ ระดับน้ำทะเล โดยมีวัตถุประสงค์เพื่องานวิจัยข้อมูลเท่านั้น และเมื่อต้องการเผยแพร่ข้อมูลต้องได้รับความยินยอมจากเจ้าของข้อมูล และเมื่อออกจากระบบ ระบบจะบันทึกประวัติการใช้งาน
2.3) ผู้ใช้งานที่ได้รับสิทธิเจ้าหน้าที่ประจำหน่วยงานเข้าสู่ระบบ สามารถเรียกดูข้อมูลปริมาณน้ำฝนได้ เมื่อต้องการเปิดเผยข้อมูล ส่งต่อข้อมูล ต้องได้รับการยินยอมจากหน่วยงานเจ้าของข้อมูลก่อน โดยระบุวัตถุประสงค์เพื่อใช้ข้อมูล และเมื่อออกจากระบบ ระบบจะบันทึกประวัติการใช้งาน
2.4) ผู้ใช้งานคลังสารสนเทศกลาง จะได้รับสิทธิตามบทบาทหน้าที่ และความผิตชอบ
2.5) ผู้ใช้งานคลังสารสนเทศต้องไม่เผยแพร่ข้อมูลที่อยู่ในคลังสารสนเทศกลาง เพื่อเป็นการหาประโยชน์เชิงพาณิชย์ ตามข้อบังคับการใช้งานคลังสารสนเทศกลาง
2.6) ผู้ใช้งานคลังสารสนเทศกลางจะต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

3.4 วิเคราะห์ออกแบบและพัฒนาเครื่องมือสนับสนุน

จากรูปที่ 3.3 ขั้นตอนที่ 2 คือการวิเคราะห์ออกแบบเครื่องมือสนับสนุน โดยใช้นโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซีจากหัวข้อที่ 3.3.4 เป็นส่วนหนึ่งของข้อมูลนำเข้า สำหรับสร้างเป็นรายการความต้องการของเครื่องมือสนับสนุน การวิเคราะห์และออกแบบเครื่องมือสนับสนุนจะกล่าวโดยละเอียดในบทที่ 4 ตารางที่ 3.7 แสดงให้เห็นถึงความสอดคล้องของฟังก์ชันงานของเครื่องมือสนับสนุนกับนโยบายการใช้งานคลังสารสนเทศกลางและแนวปฏิบัติที่ดีพีไอเอ

ตารางที่ 3.7 ฟังก์ชันงานเครื่องมือสนับสนุนและนโยบายการใช้งานคลังสารสนเทศกลาง

ฟังก์ชันงานเครื่องมือสนับสนุน	สอดคล้องกับนโยบายการใช้งานในตารางที่ 3.6	สอดคล้องกับแนวปฏิบัติพีบีดีพีไอเอ ตาราง ง.2
<p>ความสามารถด้านการสนับสนุนการจัดการนโยบาย</p> <ol style="list-style-type: none"> 1. เพิ่ม/บันทึก/ค้นหา/แก้ไข/นโยบายการใช้งาน 2. ยกเลิก/ระงับใช้นโยบายการใช้งาน 3. สกัดเอาทิตินโยบายการใช้งาน 4. เพิ่ม/บันทึก/แก้ไข/กำหนด ข้อมูลผู้รับผิดชอบนโยบายการใช้งาน 	<p>ข้อ 1.1, ข้อ 1.8</p>	<p>หลักการพีบีดีที่ 7</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ b</p> <p>หลักการพีบีดีที่ 1</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ a</p>
<p>ความสามารถด้านการกำหนดค่าพื้นฐานการใช้งานข้อมูลคือ</p> <ol style="list-style-type: none"> 1. เพิ่ม/บันทึก/แก้ไข/กำหนด/ลบ รายการไพรเวซีข้อมูลค่าเริ่มต้น 2. เรียกดูข้อมูลในคลังสารสนเทศกลาง 	<p>ข้อ 1.5</p>	<p>หลักการพีบีดีที่ 4</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ b</p>
<p>ความสามารถด้านการเรียกดูข้อมูลเข้าใช้งานระบบคือ</p> <ol style="list-style-type: none"> 1. บันทึก/ค้นหารายการเข้าใช้ระบบ 2. ออกรายงานการเข้าใช้ระบบ แบบรายวันหรือกำหนดช่วงระยะเวลา 	<p>ข้อ 2.6</p>	<p>หลักการพีบีดีที่ 1</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ z</p>

ตารางที่ 3.7 ฟังก์ชันงานเครื่องมือสนับสนุนและนโยบายการใช้งานคลังสารสนเทศกลาง (ต่อ)

ฟังก์ชันงานเครื่องมือสนับสนุน	สอดคล้องกับนโยบายการใช้งานในตารางที่ 3.6	สอดคล้องกับแนวปฏิบัติพีบีดีพีไอเอ ตาราง ง.2
<p>ความสามารถด้านการระบุตัวตนคือ</p> <ol style="list-style-type: none"> 1. บันทึกการลงทะเบียน/ตรวจสอบการเข้าสู่ระบบ เพื่อใช้งานเครื่องมือสนับสนุน 2. แก้ไขข้อมูลส่วนตัวผู้ใช้งาน 3. กู้รหัสผ่าน/แก้ไขรหัสผ่าน ผู้ใช้งาน 	ข้อ 1.3	<p>หลักการพีบีดีที่ 2</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ k</p>
<p>ความสามารถด้านการแนะนำรหัสผ่านคือ</p> <ol style="list-style-type: none"> 1. แสดงตัวอย่างรหัสผ่านให้ผู้ใช้งาน 2. แสดงคำแนะนำในการสร้างรหัสผ่านที่เข้มแข็ง 	ข้อ 1.4	<p>หลักการพีบีดีที่ 3</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ k.10</p>
<p>ความสามารถด้านการสนับสนุนการอบรมด้านไพรเวซีคือ</p> <ol style="list-style-type: none"> 1. เพิ่ม/บันทึก/แก้ไข/ลบ หลักสูตรการอบรม 2. กำหนดกลุ่มเป้าหมายของหลักสูตรการอบรม 3. บันทึกการเข้ารับหลักสูตรการอบรม 4. ออกรายงานหลักสูตรการอบรม 	ข้อ 1.2	<p>หลักการพีบีดีที่ 1</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ s</p>
<p>ความสามารถด้านการบริหารการเปิดเผยข้อมูล</p> <ol style="list-style-type: none"> 1. บันทึก/ตรวจสอบสถานะการพิจารณา/แสดงรายการ/ค้นหา คำร้องการขอใช้ข้อมูล 2. แสดงรายงานคำขอใช้ข้อมูลที่ผ่านการพิจารณา 	ข้อ 2.2 , ข้อ 2.3	<p>หลักการพีบีดีที่ 2</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ b,c</p> <p>หลักการพีบีดีที่ 7</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ a.1-3,l</p>

ตารางที่ 3.7 ฟังก์ชันงานเครื่องมือสนับสนุนและนโยบายการใช้งานคลังสารสนเทศกลาง (ต่อ)

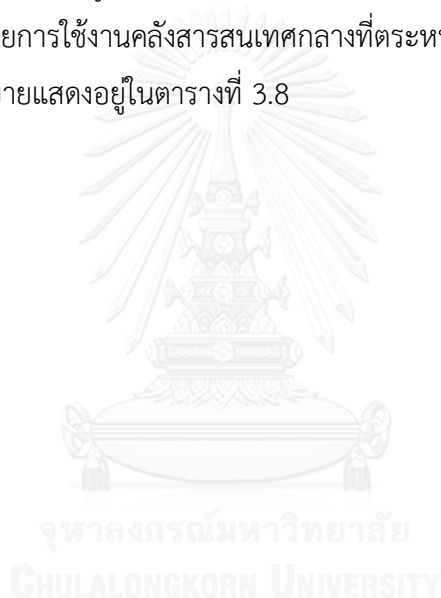
ฟังก์ชันงานเครื่องมือสนับสนุน	สอดคล้องกับนโยบายการใช้งานในตารางที่ 3.6	สอดคล้องกับแนวปฏิบัติพีบีดีพีไอเอ ตาราง ง.2
<p>ความสามารถด้านการบริหารการส่งต่อข้อมูลคือ</p> <ol style="list-style-type: none"> บันทึก/อนุมัติ/ตรวจสอบสถานะการพิจารณา/แสดงรายการ/ค้นหา คำร้องการขอต่อข้อมูล แสดงรายการที่ผ่านการพิจารณาส่งต่อข้อมูล 	ข้อ 2.2 , ข้อ 2.3	<p>หลักการพีบีดีที่ 2</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ b,c</p> <p>หลักการพีบีดีที่ 7</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ a.1-3,l</p>
<p>ความสามารถด้านการควบคุมสิทธิและบทบาทคือ</p> <ol style="list-style-type: none"> เพิ่ม/บันทึก/แก้ไข/ลบ สิทธิและบทบาท บันทึกมอบหมาย/แก้ไขการมอบหมาย/สามารถตรวจสอบ สิทธิและบทบาท 	ข้อ 1.3	<p>หลักการพีบีดีที่ 2</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ k</p>
<p>ความสามารถด้านการสร้างตารางรายการสนับสนุนเพื่อการเก็บรักษาและทำลายข้อมูลมีคือ</p> <ol style="list-style-type: none"> เพิ่ม/บันทึก/แก้ไข/ลบ รายการเก็บรักษาและทำลายข้อมูล แสดงรายงานการเก็บรักษาและทำลายข้อมูล 	ข้อ 1.7	<p>หลักการพีบีดีที่ 6</p> <p>แนวปฏิบัติพีบีดีพีไอเอข้อ a</p>

3.5 การสกัดเอนทิตีและจัดเก็บนโยบาย

จากรูปที่ 3.3 ขั้นตอนที่ 3 คือการสกัดนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี เจ้าหน้าที่คลังสารสนเทศกลางพิจารณานโยบายการใช้งานคลังสารสนเทศกลางที่ผ่านการเห็นชอบจากผู้บริหาร โดยใช้เครื่องมือสนับสนุนที่พัฒนาในการสกัดเอนทิตีนโยบายการใช้งานคลังสารสนเทศกลาง ในการสกัดนโยบายการใช้งานนั้นเจ้าหน้าที่คลังสารสนเทศกลางจะต้องพิจารณาว่านโยบายการให้มีเอนทิตีงานวิจัยนี้ได้ใช้เอนทิตี [9] เหล่านี้คือ

- บทบาทคือ หน้าที่การทำงานหรือชื่อตำแหน่งในองค์กร
- ข้อมูลคือ สารสนเทศใดๆ หรือเมตาดาต้าที่สามารถใช้ระบุตัวตนได้
- การกระทำคือ การปฏิบัติงานระหว่างผู้ใช้งานกับข้อมูล
- วัตถุประสงค์คือ ขอบเขตของการกระทำกับข้อมูล
- ข้อผูกพันคือ สิ่งที่ต้องดำเนินการหลังจากการกระทำลำดับล่าสุด
- เงื่อนไขคือ สิ่งที่ต้องดำเนินการให้ก่อนแล้วเสร็จก่อนที่จะเริ่มทำงานในขั้นตอนอื่น

หลังจากที่นโยบายการใช้งานคลังสารสนเทศกลางได้ถูกสกัดและจัดเก็บในฐานข้อมูล ข้อมูลดังกล่าว จะถูกนำไปใช้ในการกำหนดให้กับผู้ใช้งานคลังสารสนเทศกลางตามบทบาทที่ระบุในนโยบาย ตัวอย่างผลลัพธ์เอนทิตีของนโยบายการใช้งานคลังสารสนเทศกลางที่ระหนกถึงไพรเวซีในตาราง 3.6 ข้อ 2 ที่ผ่านการสกัดเอนทิตีนโยบายแสดงอยู่ในตารางที่ 3.8



ตารางที่ 3.8 ตัวอย่างการสกัดเอาเนื้อหาต้นนโยบายการใช้งานคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

นโยบายข้อ	บทบาท	ข้อมูล	วัตถุประสงค์	การกระทำ	เงื่อนไข	ข้อผูกพัน
2.1	ผู้ใช้งาน	-	ลงทะเบียน	-	-	ระบบบันทึกประวัติการใช้งาน
2.2	นักวิจัย	ระดับน้ำ	เพื่อการวิจัย, เผยแพร่ข้อมูล	เรียกดู	ได้รับความยินยอมจากเจ้าของข้อมูล	ระบบบันทึกประวัติการใช้งาน
	นักวิจัย	ข้อมูลในเซ็นเซอร์	เพื่อการวิจัย, เผยแพร่ข้อมูล	เรียกดู	ได้รับความยินยอมจากเจ้าของข้อมูล	ระบบบันทึกประวัติการใช้งาน
	นักวิจัย	ความเข้มแสง	เพื่อการวิจัย, เผยแพร่ข้อมูล	เรียกดู	ได้รับความยินยอมจากเจ้าของข้อมูล	ระบบบันทึกประวัติการใช้งาน
	นักวิจัย	ความกดอากาศ	เพื่อการวิจัย, เผยแพร่ข้อมูล	เรียกดู	ได้รับความยินยอมจากเจ้าของข้อมูล	ระบบบันทึกประวัติการใช้งาน
2.3	เจ้าหน้าที่ประจำหน่วยงาน	ปริมาณน้ำฝน	ใช้ข้อมูล, เปิดเผยแพร่ข้อมูล	เรียกดู	ได้รับความยินยอมจากเจ้าของข้อมูล	ระบบบันทึกประวัติการใช้งาน

3.6 สรุปผลการประยุกต์แนวปฏิบัติพีบีพีไอเข้ากับคลังสารสนเทศกลาง

ในหัวข้อจะกล่าวถึงผลของการวิเคราะห์รายการแนวปฏิบัติของพีบีพีไอเอที่นำมาประยุกต์ใช้กับคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา เพื่อใช้ในการสร้างนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซีแสดงในตารางสรุปที่ 3.9

จากตารางที่ ๓.2 มีรายการแนวปฏิบัติทั้งหมด 123 แนวปฏิบัติประกอบด้วย

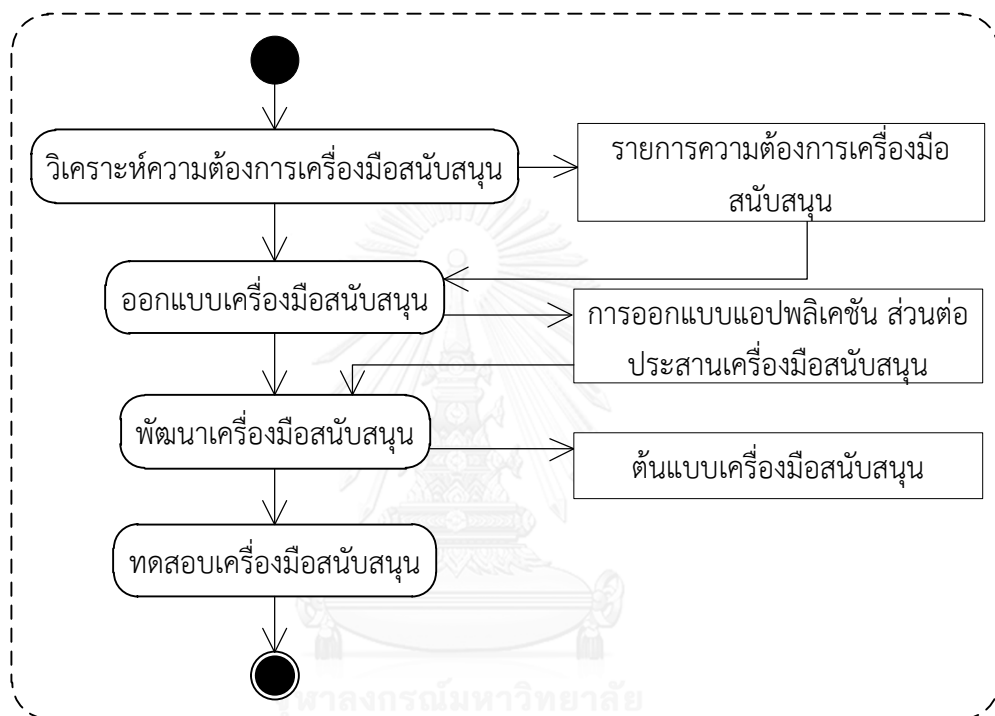
1. แนวปฏิบัติที่มีผลการพิจารณา ✘ ไม่นำมาประยุกต์ใช้ในองค์กร 47 แนวปฏิบัติ (38.21%)
2. แนวปฏิบัติที่มีผลการพิจารณา ✔ นำมาประยุกต์ใช้ในองค์กร 65 แนวปฏิบัติ (52.84%)
3. แนวปฏิบัติที่มีผลการพิจารณา ⊙ อยู่ระหว่างพิจารณา 11 แนวปฏิบัติ (8.94%)

ตารางที่ 3.9 สรุปการรายการแนวปฏิบัติที่นำประยุกต์ใช้กับคลังสารสนเทศกลางจากตาราง ๓.2

หลักการพีบีพี	แนวปฏิบัติพีบีพีไอเอ		คิดเป็นร้อยละของ แนวปฏิบัติในแต่ละ หลักการ	คิดเป็นร้อยละ ของแนวปฏิบัติ ทั้งหมด
	แนวปฏิบัติทั้งหมด	แนวปฏิบัติที่เลือก		
หลักการที่ 1	28	16	57.14%	13%
หลักการที่ 2	12	7	58.33%	5.69%
หลักการที่ 3	26	9	34.61%	7.31%
หลักการที่ 4	10	7	70%	5.69%
หลักการที่ 5	19	7	36.84%	5.69%
หลักการที่ 6	10	5	50%	4.06%
หลักการที่ 7	18	14	77.77%	11.38%
	รวม 123	รวม 65		52.84%

บทที่ 4 การวิเคราะห์ออกแบบและพัฒนาเครื่องมือสนับสนุน

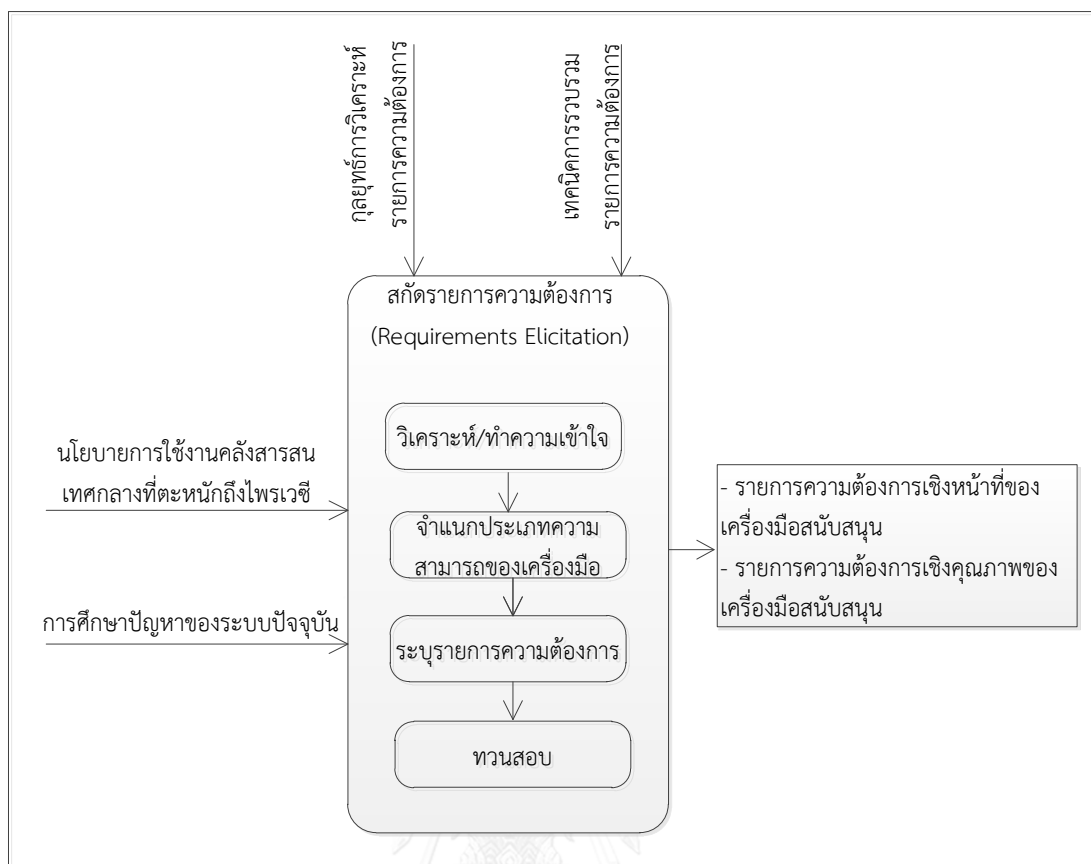
ในบทนี้จะกล่าวถึงการวิเคราะห์ความต้องการ การออกแบบและพัฒนาเครื่องมือสนับสนุน และการทดสอบเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางโดยมีขั้นตอนปรากฏในรูปที่ 4.1



รูปที่ 4.1 ขั้นตอนวิเคราะห์ออกแบบและพัฒนาเครื่องมือสนับสนุน

4.1 การวิเคราะห์ความต้องการของเครื่องมือสนับสนุน

การวิเคราะห์ความต้องการของแอปพลิเคชันที่ตระหนักถึงไปเวเซีหรือเครื่องมือสนับสนุนมีวัตถุประสงค์เพื่อแสดงขั้นตอนวิธีการวิเคราะห์ข้อมูลนำเข้า เพื่อกำหนดเป็นรายการความต้องการของเครื่องมือสนับสนุนดังปรากฏอยู่ในรูปที่ 4.2 ผลลัพธ์ที่ได้ในขั้นตอนนี้คือรายการความต้องการเชิงหน้าที่และความต้องการเชิงคุณภาพของเครื่องมือสนับสนุน



รูปที่ 4.2 การวิเคราะห์รายการความต้องการของเครื่องมือสนับสนุน

รายละเอียดขั้นตอนการสักรายการความต้องการของเครื่องมือสนับสนุนจะต้องพิจารณาถึงข้อมูลนำเข้าดังต่อไปนี้คือ

1) ข้อมูลนำเข้า

- กลยุทธ์ในการวิเคราะห์รายการความต้องการ (Requirements Analysis Strategy) กลยุทธ์ในการวิเคราะห์รายการความต้องการที่ใช้ในงานวิจัยนี้คือ กระบวนการทางธุรกิจแบบอัตโนมัติ (Business Process Automation) โดยใช้เทคนิคการวิเคราะห์ปัญหา (Problem Analysis) จากการสอบถามจากผู้ที่เกี่ยวข้องเพื่อใช้เป็นข้อมูลในการระบุปัญหาของคลังสารสนเทศกลางจากระบบปัจจุบัน (As-is system) เพื่อนำมาพัฒนาแก้ไขให้ตรงตามความต้องการในเครื่องมือสนับสนุนที่กำลังพัฒนาต่อไป (To-be system)

- เทคนิคการรวบรวมรายการความต้องการ (Requirements Gathering Technique) เทคนิคที่ใช้ในการรวบรวมรายการความต้องการคือ การออกแบบแอปพลิเคชันแบบมีส่วนร่วม (Joint Application Design: JAD) เพื่อให้ได้รายการความต้องการของเครื่องมือสนับสนุน จึงต้องรวบรวม

ความต้องการจากกลุ่มคณะทำงานที่เกี่ยวข้องกับคลังสารสนเทศกลางเช่น หัวหน้ากลุ่มงาน เจ้าหน้าที่คลังสารสนเทศกลาง หัวหน้ากลุ่มงานพัฒนา หัวหน้ากลุ่มงานระบบเครือข่าย เป็นต้น เนื่องจากเป็นกลุ่มผู้ใช้งานที่เกี่ยวข้องกับคลังสารสนเทศกลางโดยตรง เพื่อสรุปรายการความต้องการร่วมกัน

- นโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงเป็นไปรษณีย์ เป็นเอกสารที่จำเป็นที่ใช้ในการวิเคราะห์รายการความต้องการเครื่องมือสนับสนุน เพื่อทราบถึงขอบเขตการใช้งานข้อมูล สิทธิและบทบาทการใช้งานข้อมูล กระบวนการเปิดเผยหรือร้องขอข้อมูล ที่ระบุในนโยบายการใช้งานคลังสารสนเทศกลางตามที่ได้กล่าวไว้ในบทที่ 3

- การศึกษาปัญหาของระบบปัจจุบัน (As-is System) คือ การศึกษากระบวนการทำงานของคลังสารสนเทศกลางเช่น การรวบรวมข้อมูล การเชื่อมโยงข้อมูล การแปลงข้อมูล ผู้ใช้งานที่เกี่ยวข้องการใช้บริการข้อมูลของคลังสารสนเทศกลาง นิยาม มาตรฐานที่นำมาประยุกต์ใช้ เป็นต้น เพื่อทราบถึงปัญหาของคลังสารสนเทศกลางได้กล่าวไว้ในบทที่ 3

2) ขั้นตอนการสกัดรายการความต้องการ ประกอบด้วยกิจกรรมดังต่อไปนี้

- วิเคราะห์/ทำความเข้าใจคือ การศึกษานโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไปรษณีย์และระบบการทำงานปัจจุบันของคลังสารสนเทศกลาง

- จำแนกความสามารถของเครื่องมือสนับสนุนคือ การจัดกลุ่มประเภทความสามารถของเครื่องมือสนับสนุนเช่น ความสามารถด้านบริหารจัดการข้อมูล ความสามารถด้านการจัดการกลุ่มผู้ใช้งาน เป็นต้น

- ระบุรายการความต้องการคือ การระบุรายการความต้องการของเครื่องมือสนับสนุน ประกอบด้วยรายการความเชิงระบบของเครื่องมือสนับสนุนและรายการความต้องการเชิงคุณภาพของเครื่องมือสนับสนุน

- ทวนสอบคือ การทวนสอบรายการความต้องการของเครื่องมือสนับสนุนว่ามีความถูกต้องครบถ้วนตามความต้องการ

3) ข้อมูลนำออก

- รายการความต้องการเชิงหน้าที่ของเครื่องมือสนับสนุน (Functional Requirements:FR) คือ รายการหน้าที่ความสามารถของเครื่องมือสนับสนุน รายการความต้องการเชิงหน้าที่ของเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางของหน่วยงานกรณีศึกษาแสดงในตารางที่ 4.1

- รายการความต้องการเชิงคุณภาพของเครื่องมือสนับสนุน (Non-Functional Requirements:NFR) คือ รายการความต้องการของเครื่องมือสนับสนุนเชิงคุณภาพโดยส่งผลทำให้เครื่องมือสนับสนุนมีคุณภาพดีขึ้น แสดงอยู่ตารางที่ 4.2

4.1.1 รายการความต้องการเชิงหน้าที่ของเครื่องมือสนับสนุน

ตัวอย่างรายการความต้องการเชิงหน้าที่ (Functional Requirements) ของเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงานกรณีศึกษาในตารางที่ 4.1 แสดงกลุ่มความสามารถของเครื่องมือสนับสนุน รายการความต้องการทั้งหมดสามารถดูเพิ่มเติมได้ที่ภาคผนวก ก ตารางที่ ก.2

ตารางที่ 4.1 ตัวอย่างรายการความต้องการเชิงหน้าที่ของเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

หมายเลขความต้องการ	กลุ่มความสามารถ	คำอธิบาย
FRG1	การจัดการนโยบาย	บริหารจัดการด้านนโยบายการใช้งาน
FRG2	การกำหนดค่าพื้นฐานการใช้งานข้อมูล	บริหารจัดการด้านไอพีแอดเดรสข้อมูลเริ่มต้น
FRG3	ข้อมูลเข้าใช้งานระบบ	บริหารจัดการด้านข้อมูลการเข้าใช้งานระบบ
FRG4	การระบุตัวตน	บริหารจัดการด้านการระบุตัวตน
FRG5	การแนะนำรหัสผ่าน	บริหารจัดการด้านการแนะนำรหัสผ่าน
FRG6	การอบรมด้านไอพีแอดเดรส	บริหารจัดการด้านหลักสูตรการอบรม
FRG7	การเปิดเผยข้อมูล	บริหารจัดการด้านคำร้องขอใช้ข้อมูล
FRG8	การส่งต่อข้อมูล	บริหารจัดการด้านคำร้องขอส่งต่อข้อมูล
FRG9	การควบคุมสิทธิและบทบาท	บริหารจัดการด้านสิทธิและบทบาท
FRG10	การเก็บรักษาและทำลายข้อมูล	บริหารจัดการด้านรายการเก็บรักษาและทำลายข้อมูล

4.1.2 รายการความต้องการเชิงคุณภาพของเครื่องมือสนับสนุน

ตัวอย่างรายการความต้องการเชิงคุณภาพ (Non-functional Requirements) ของเครื่องมือสนับสนุนแสดงดังตารางที่ 4.2

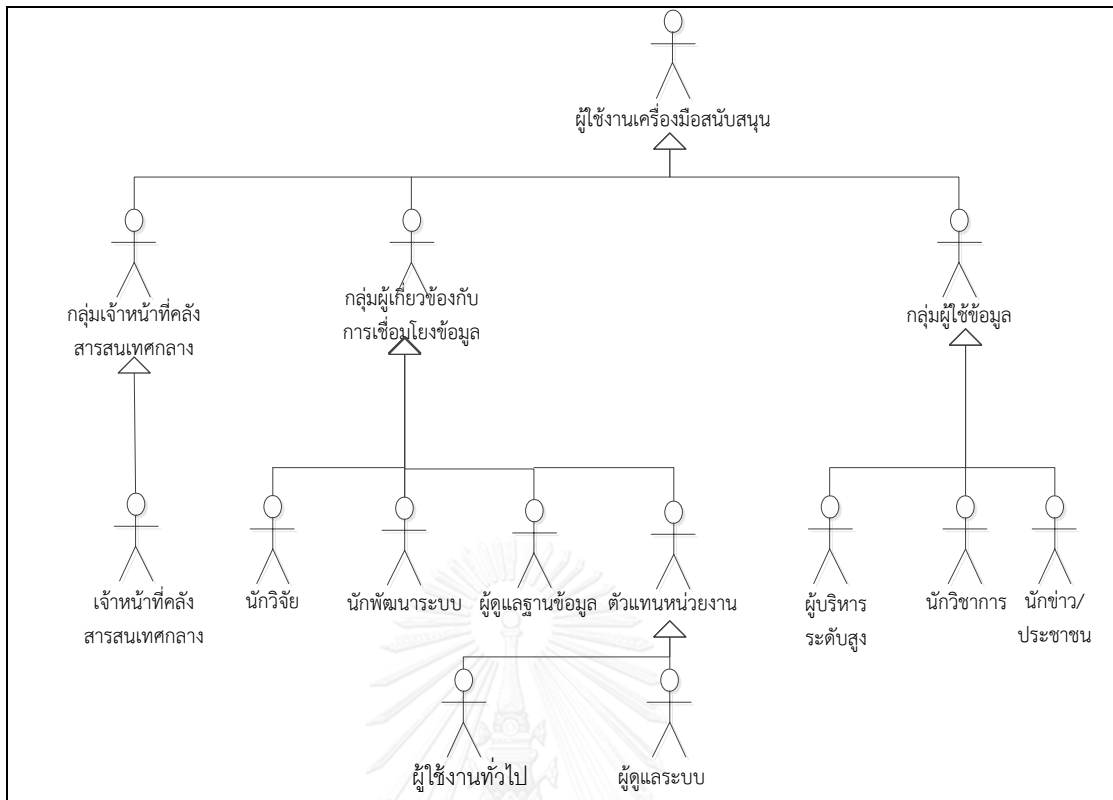
ตารางที่ 4.2 รายการความต้องการเชิงคุณภาพของเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

หมายเลขความต้องการ	ประเภทความต้องการ	รายการความต้องการ
NFR1	Usability	เครื่องมือสนับสนุนการใช้งานคลังสารสนเทศกลางมีการออกแบบให้ง่ายต่อการใช้งานคือ มีส่วนต่อประสานแสดงให้ผู้ใช้ทราบสถานะการใช้งานปัจจุบัน เรียบง่าย ไม่ซับซ้อน มีความสม่ำเสมอของส่วนต่อประสาน มีรูปแบบส่วนต่อประสานทิศทางเดียวกัน
NFR2	Security	เครื่องมือสนับสนุนมีการกำหนดดิสทริบิวชันและบทบาทการใช้งาน ตรวจสอบการเข้าใช้งาน ตามข้อกำหนดเครื่องมือสนับสนุน
NFR3	Portability	เครื่องมือสนับสนุนมีรูปแบบการนำไปติดตั้งที่ไม่ซับซ้อน สามารถใช้งานได้ง่ายผ่านทางเว็บเบราว์เซอร์เช่น กูเกิลโครม, มอซิลลา ไฟร์ฟอกซ์, อินเทอร์เน็ตเอกซ์พลอเรอร์ เป็นต้น
NFR4	Maintainability	รหัสต้นฉบับ (Source Code) ของเครื่องมือสนับสนุนมีการเขียนหมายเหตุ อธิบายโค้ดในแต่ละส่วน เพื่อให้ง่ายต่อการบำรุงรักษา
NFR5	Accuracy	แบบฟอร์มสำหรับให้ผู้ใช้กรอกข้อมูลสามารถตรวจสอบการกรอกข้อมูล มีการทำงานที่ถูกต้อง จุดเชื่อมโยงจะต้องเชื่อมโยงไปหน้าที่มีอยู่จริง

4.2 การออกแบบและพัฒนาเครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลาง

4.2.1 การกำหนดดิสทริบิวชันเครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลาง

เครื่องมือสนับสนุนการใช้งานคลังสารสนเทศกลางได้มีการกำหนดบทบาทหน้าที่และสิทธิในการใช้งาน เพื่อให้สอดคล้องกับข้อมูลและการให้บริการคลังสารสนเทศกลางปรากฏในรูปที่ 4.3



รูปที่ 4.3 บทบาทผู้ใช้งานเครื่องมือสนับสนุนการใช้งานคลังสารสนเทศกลาง

จากรูปที่ 4.3 แสดงให้เห็นกลุ่ม บทบาทและสิทธิผู้ใช้งานเครื่องมือสนับสนุนสำหรับคลังสารสนเทศที่แตกต่างกันออกไปดังแสดงรายละเอียดในตารางที่ 4.3

ตารางที่ 4.3 กลุ่มผู้ใช้งาน บทบาท สิทธิของผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลาง

กลุ่มผู้ใช้งาน	บทบาท	คำอธิบาย
เจ้าหน้าที่คลังสารสนเทศกลาง	เจ้าหน้าที่คลังสารสนเทศกลาง	บริหารจัดการกลุ่มผู้ใช้งาน มอบหมายสิทธิการใช้งาน การเข้าถึงข้อมูลในคลังสารสนเทศกลาง
กลุ่มผู้เกี่ยวข้องกับการเชื่อมโยงข้อมูล	นักวิจัย	ใช้งานข้อมูลเพื่อวัตถุประสงค์สำหรับงานวิจัย
	นักพัฒนาระบบ	ใช้งานข้อมูลเพื่อการพัฒนาาระบบ
	ผู้ดูแลฐานข้อมูล	ใช้งานข้อมูลเพื่อตรวจสอบข้อมูล ให้พร้อมใช้งาน

ตารางที่ 4.3 กลุ่มผู้ใช้งาน บทบาท สิทธิของผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลาง (ต่อ)

กลุ่มผู้เกี่ยวกับการเชื่อมโยงข้อมูล	ตัวแทนหน่วยงาน	ตัวแทนหน่วยงาน แบ่งผู้ใช้งานออกเป็น 2 ประเภทคือ “ผู้ใช้งานทั่วไป” สามารถเข้าใช้งานได้ตามที่นโยบายการใช้งานที่กำหนด “ผู้ดูแลระบบ” สามารถเปลี่ยนแปลงค่าโพรเวซีข้อมูลของหน่วยงานได้ ซึ่งในหนึ่งหน่วยงานจะมีเพียงบุคคลเดียวเท่านั้นที่ได้รับสิทธินี้
กลุ่มผู้ใช้ข้อมูล	ผู้บริหารระดับสูง	ใช้งานข้อมูลที่ผ่านการประมวล ดูรายงานที่ระบบจัดเตรียมไว้
	นักวิชาการ	ใช้งานข้อมูลบางประเภทตามที่กำหนด เพื่อใช้ในงานวิชาการ
	นักข่าว/ประชาชน	ใช้งานข้อมูลทั่วไปที่คลังสารสนเทศกลางจัดเตรียมไว้

4.2.2 การออกแบบฟังก์ชันงานเครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลาง

การออกแบบเครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลางแบ่งออกเป็น 5 ส่วนย่อย ตามลักษณะกลุ่มของรายการความต้องการเชิงหน้าที่ของคลังสารสนเทศกลางคือ

1) ส่วนการจัดการนโยบาย (Policy Management) ทำหน้าที่บริหารจัดการนโยบายการใช้งานของคลังสารสนเทศกลางเช่น การเพิ่ม การบันทึก และเผยแพร่นโยบายการใช้งานคลังสารสนเทศกลาง เป็นต้น

2) ส่วนการจัดการโพรเวซี (Privacy Management) ทำหน้าที่บริหารจัดการโพรเวซีข้อมูลในคลังสารสนเทศกลางเช่น การกำหนดค่าโพรเวซีเริ่มต้นให้กับข้อมูล การกำหนดโพรเวซีเริ่มต้นให้กับผู้ใช้งานในคลังสารสนเทศกลาง เป็นต้น

3) ส่วนการจัดการข้อมูลการใช้งานระบบ (Log Management) ทำหน้าที่ในการบริหารจัดการข้อมูลการเข้าใช้งานของผู้ใช้งานเครื่องมือสนับสนุน

4) ส่วนจัดการการระบุตัวตน (Authentication Management) ทำหน้าที่จัดการในการบริหารจัดการด้านความมั่นคงและสิทธิ การตรวจสอบการเข้าใช้งานเครื่องมือสนับสนุน

5) ส่วนการแนะนำรหัสผ่าน (Password Suggestion) ทำหน้าที่แสดงตัวอย่างรหัสผ่านที่เข้มแข็ง แนะนำการสร้างรหัสผ่านที่มีคุณสมบัติที่ดีให้กับผู้ใช้งาน รวมไปถึงการทดสอบความเข้มแข็งของรหัสผ่าน เป็นต้น

6) ส่วนการบริหารจัดการหลักสูตรอบรม (Training Management) ทำหน้าที่บริหารจัดการหลักสูตรอบรมด้านไอที เช่น การเพิ่มหลักสูตรอบรม การบันทึกหลักสูตรอบรม การออกรายงาน การเข้ารับการอบรม เป็นต้น

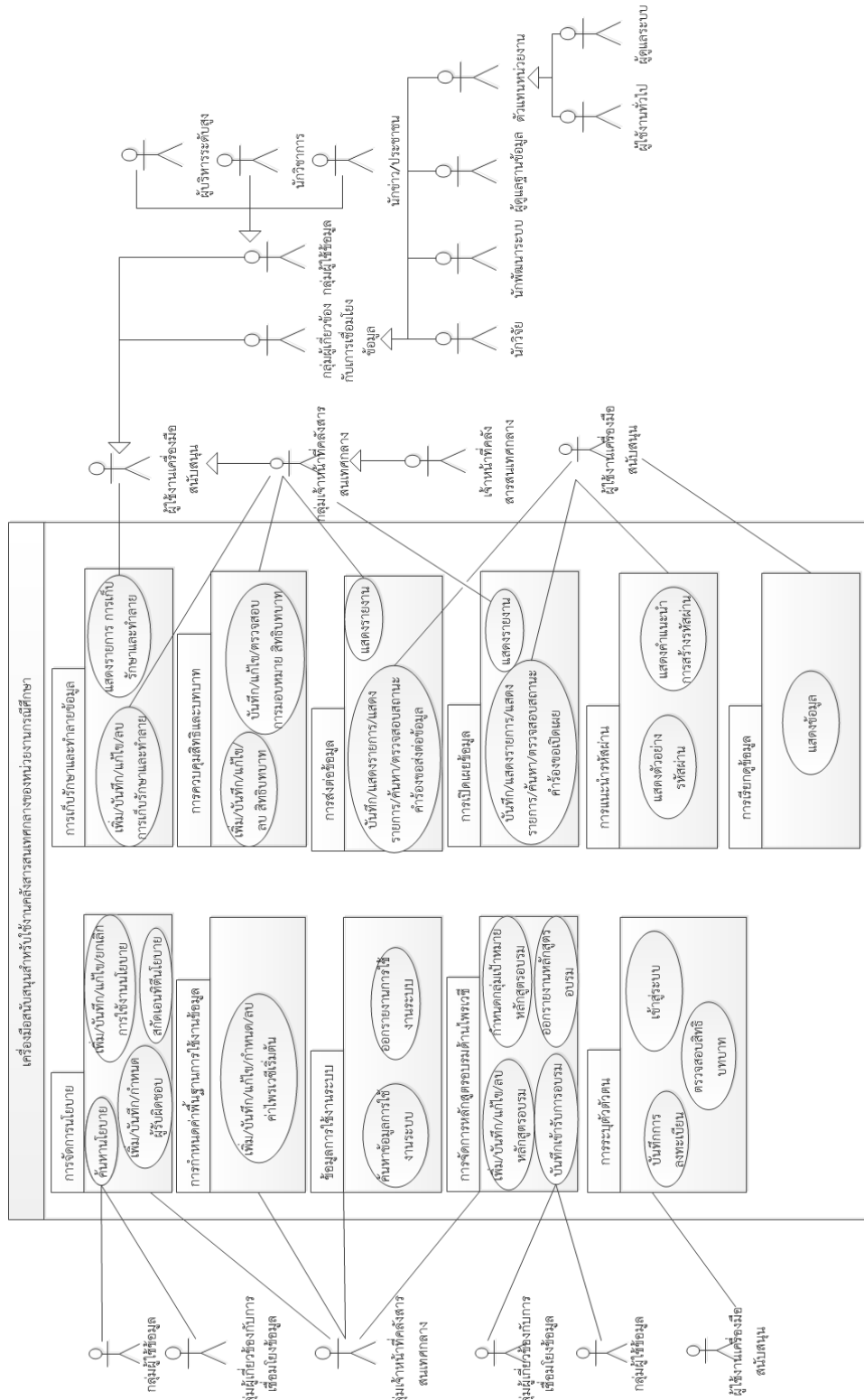
7) ส่วนการบริหารจัดการ การเปิดเผยข้อมูล (Consent Management) ทำหน้าที่บริหารจัดการด้านคำร้องขอเพื่อขอการยินยอมจากเจ้าของข้อมูลเพื่อเปิดเผยข้อมูล

8) ส่วนการบริหารจัดการ การส่งต่อข้อมูล (Transfer Data Management) ทำหน้าที่บริหารจัดการคำร้องขอเพื่อส่งต่อข้อมูล เช่น การส่งคำร้องเพื่อขอส่งต่อข้อมูล เรียกดูสถานะคำร้องขอส่งต่อข้อมูล เป็นต้น

9) ส่วนการควบคุมสิทธิและบทบาท (Role based Management) ทำหน้าที่บริหารจัดการด้านการสิทธิและบทบาทของผู้ใช้งาน เช่น การเพิ่มบทบาท การบันทึกบทบาท การมอบหมายบทบาทให้กับผู้ใช้งาน เป็นต้น รวมถึงการจัดการสก็อตที่นโยบายสารสนเทศกลาง

10) การเก็บรักษาและทำลายข้อมูล (Data Retention) ทำหน้าที่บริหารจัดการด้านการเก็บรักษาและทำลายข้อมูล เช่น การกำหนดระยะเวลาในการเก็บรักษาข้อมูล การกำหนดระยะเวลาการทำลายข้อมูลในคลังสารสนเทศกลาง แสดงระยะเวลาการเก็บรักษาและทำลายข้อมูลให้ผู้ใช้งานทราบ เป็นต้น

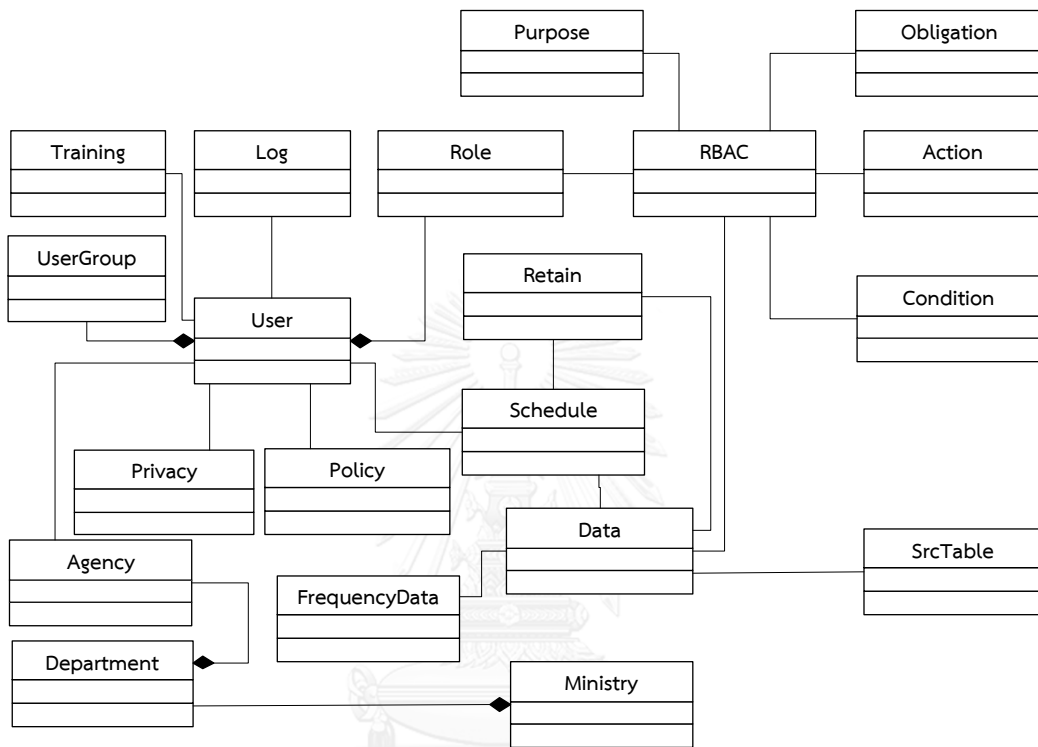
ความสามารถของเครื่องมือสนับสนุนคลังสารสนเทศกลางแสดงในรูปแบบแผนภาพยูสเคสปรากฏดังรูปที่ 4.4 และตัวอย่างคำอธิบายยูสเคสปรากฏอยู่ในภาคผนวก จ.



รูปที่ 4.4 แผนภาพรายละเอียดของเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลาง

4.2.3 การออกแบบเชิงโครงสร้างของเครื่องมือสนับสนุนโดยใช้แผนภาพคลาส

การออกแบบเชิงโครงสร้างเครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลาง เพื่อแสดงความสัมพันธ์ขององค์ประกอบของเครื่องมือสนับสนุน ปรากฏดังรูปที่ 4.5 และคำอธิบายแผนภาพคลาสแสดงอยู่ในตารางที่ 4.4



รูปที่ 4.5 แผนภาพคลาสของเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลาง

ตารางที่ 4.4 คำอธิบายแผนภาพคลาสเครื่องมือสนับสนุนจากรูปที่ 4.5

ชื่อคลาส	คำอธิบาย
User	คลาสที่เกี่ยวข้องกับผู้ใช้งานเครื่องมือสนับสนุน
UserGroup	คลาสที่เกี่ยวข้องกับกลุ่มผู้ใช้งานในคลังสารสนเทศกลาง
Training	คลาสที่เกี่ยวข้องกับการจัดการหลักสูตรการอบรม
Log	คลาสที่เกี่ยวข้องกับการเก็บบันทึกการใช้งานเครื่องมือสนับสนุน
RBAC	คลาสที่เกี่ยวข้องกับการจัดการการเข้าถึงตามบทบาท
Role	คลาสที่เกี่ยวข้องกับบทบาทผู้ใช้งาน
Purpose	คลาสที่เกี่ยวข้องกับวัตถุประสงค์ที่สกัดจากนโยบายการใช้งาน
Action	คลาสที่เกี่ยวข้องกับการกระทำที่สกัดจากนโยบายการใช้งาน
Data	คลาสที่เกี่ยวข้องกับข้อมูลที่สกัดจากนโยบายการใช้งาน
Obligation	คลาสที่เกี่ยวข้องกับเงื่อนไขที่ต้องกระทำก่อนที่สกัดจากนโยบายการใช้

	งาน
Condition	คลาสที่เกี่ยวข้องกับเงื่อนไขการใช้งานที่สกัดได้จากนโยบายการใช้งาน
Retain	คลาสที่เกี่ยวข้องกับการเก็บรักษาข้อมูลที่สกัดได้จากนโยบายการใช้งาน
Schedule	คลาสที่เกี่ยวข้องกับการจัดการตารางเวลาสำหรับบันทึกระยะเวลาการเก็บรักษาข้อมูล
Policy	คลาสเกี่ยวข้องกับการจัดการนโยบายใช้งานคลังสารสนเทศกลาง
Privacy	คลาสเกี่ยวข้องกับการจัดการความเป็นส่วนตัวของข้อมูลที่อยู่ในคลังสารสนเทศกลาง
FrequencyData	คลาสเกี่ยวข้องกับความถี่ของข้อมูลที่อยู่ในคลังสารสนเทศกลาง
SrcTable	คลาสเกี่ยวข้องกับการจัดเก็บข้อมูลในคลังสารสนเทศกลาง
Agency	คลาสเกี่ยวข้องกับหน่วยงานที่เกี่ยวข้องกับคลังสารสนเทศกลาง
Department	คลาสเกี่ยวข้องกับแผนกที่หน่วยงานสังกัด
Ministry	คลาสเกี่ยวข้องกับกระทรวง หน่วยงาน

4.2.4 สถาปัตยกรรมการออกแบบที่ใช้ในการพัฒนาเครื่องมือสนับสนุน

การพัฒนาเครื่องมือสนับสนุนคลังสารสนเทศกลาง ผู้วิจัยเลือกใช้สถาปัตยกรรมการออกแบบเอ็มวีซี (MVC Pattern) ในการออกแบบและพัฒนาเครื่องมือสนับสนุน สถาปัตยกรรมการออกแบบเอ็มวีซีแบ่งโครงสร้างออกเป็น 3 ส่วน คือ โมเดล (Model) วิว (View) และคอนโทรลเลอร์ (Controller) สำหรับรายละเอียดสถาปัตยกรรมการออกแบบเอ็มวีซีที่ใช้ในการพัฒนาเครื่องมือสนับสนุนแสดงอยู่ในตารางที่ 4.5 รายละเอียดสถาปัตยกรรมการออกแบบเอ็มวีซีที่นำมาประยุกต์ใช้กับเครื่องมือสนับสนุนคลังสารสนเทศกลางแสดงอยู่ในตารางที่ 4.6

ตารางที่ 4.5 รายละเอียดสถาปัตยกรรมการออกแบบเอ็มวีซี

แบบรูปเอ็มวีซี	คำอธิบาย
โมเดล (Model)	โมเดล ทำหน้าที่เป็นตัวแทนของข้อมูล ทั้งข้อมูลที่อยู่ในรูปแบบไฟล์หรือจัดเก็บในระบบฐานข้อมูล เมื่อข้อมูลนั้นถูกโหลดเข้ามาในแอปพลิเคชัน โมเดลอยู่ในรูปแบบของออบเจกต์ ตัวอย่างเช่น ออบเจกต์ของบทบาท ออบเจกต์ของผู้ใช้งาน เป็นต้น
วิว (View)	วิวทำหน้าที่ในการแสดงผล เช่น การแสดงแบบฟอร์มกรอกข้อมูล แสดงผลลัพธ์ของการค้นหา เป็นต้น ซึ่งวิวจะประกอบไปด้วยตรรกะการแสดงผล (Presentation Logic) ตัวอย่างเช่น การแสดงผลเรียงลำดับข้อมูลจากคลังสารสนเทศกลาง

ตารางที่ 4.5 รายละเอียดสถาปัตยกรรมการออกแบบเอ็มวีซี (ต่อ)

แบบรูปเอ็มวีซี	คำอธิบาย
คอนโทรลเลอร์ (Controller)	<p>คอนโทรลเลอร์คือ ออบเจกต์ทำหน้าที่รับคำสั่งเช่น คำสั่งค้นหา คำสั่งลบ ข้อมูล เป็นต้น เมื่อมีคำสั่งหรือคำร้อง (Request) มาจากผู้ใช้งาน คอนโทรลเลอร์จะทำหน้าที่เรียกใช้ออบเจกต์อื่นให้ทำงานแทน เช่น โมเดล ออบเจกต์ วิวออบเจกต์ เป็นต้น ให้ทำงานร่วมกัน ตัวอย่างของการทำงานของคอนโทรลเลอร์เช่น</p> <ol style="list-style-type: none"> 1. รับข้อมูลจากผู้ใช้งานจากการกรอกฟอร์ม 2. ทำการตรวจสอบ (Validation) ข้อมูลว่าครบถ้วน ถูกต้องก่อนจะนำไปประมวลผลต่อไป 3. เรียกใช้ โมเดลออบเจกต์เพื่อประมวลผลคำสั่งพร้อมข้อมูล 4. ส่งต่อผลลัพธ์จากการประมวลผลไปยังวิวออบเจกต์เพื่อแสดงผลให้ผู้ใช้งานต่อไป

ตารางที่ 4.6 ตัวอย่างรายละเอียดสถาปัตยกรรมเอ็มวีซีของเครื่องมือสนับสนุนคลังสารสนเทศกลาง

แบบรูปเอ็มวีซี	ชื่อคลาส	คำอธิบาย
โมเดล	PolicyModel	ออบเจกต์ของนโยบายการใช้งาน
	PrivacyModel	ออบเจกต์ของไพรเวซีซีผู้ใช้งานและไพรเวซีซีข้อมูล
	UserModel	ออบเจกต์ของผู้ใช้งานคลังสารสนเทศกลาง
	RoleModel	ออบเจกต์ของบทบาทผู้ใช้งาน
	DataModel	ออบเจกต์ของข้อมูลในคลังสารสนเทศกลาง
	ActionModel	ออบเจกต์การกระทำผู้ใช้งานเครื่องมือ
	ConditionModel	ออบเจกต์ของเงื่อนไขการใช้งานข้อมูล
	ObligationModel	ออบเจกต์ของภาระผูกพันการใช้งานข้อมูล
	PurposeModel	ออบเจกต์ของวัตถุประสงค์ใช้งานข้อมูล
	RetainModel	ออบเจกต์ของการเก็บรักษาข้อมูล
MinistryModel	ออบเจกต์ของข้อมูลกระทรวงเจ้าของข้อมูล	

ตารางที่ 4.6 ตัวอย่างรายละเอียดสถาปัตยกรรมเอ็มวีซีของเครื่องมือสนับสนุนคลังสารสนเทศกลาง
(ต่อ)

แบบรูปเอ็มวีซี	ชื่อคลาส	คำอธิบาย
โมเดล	LogModel	ออบเจกต์ของการเก็บข้อมูลการใช้งาน
	AgencyModel	ออบเจกต์ของหน่วยงานเจ้าของข้อมูล
	DepartmentModel	ออบเจกต์ของทบวงกรมของเจ้าของข้อมูล
	TrainingModel	ออบเจกต์ของหลักสูตรการอบรม
	UserGroupModel	ออบเจกต์ของกลุ่มผู้ใช้งาน
	ScheduleModel	ออบเจกต์ของตารางเวลาในการจัดเก็บรักษาข้อมูล
วิว	Policy	วิวของนโยบายการใช้งาน
	Privacy	วิวของไพรเวซีผู้ใช้งานและข้อมูล
	User	วิวของผู้ใช้งานคลังสารสนเทศกลาง
	Role	วิวของบทบาทผู้ใช้งาน
	Data	วิวของข้อมูลในคลังสารสนเทศกลาง
	Action	วิวของการกระทำ
	Condition	วิวของเงื่อนไขการใช้งานข้อมูล
	Obligation	วิวของภาระผูกพันการใช้งานข้อมูล
	Purpose	วิวของวัตถุประสงค์ใช้งานข้อมูล
	Retain	วิวของการเก็บรักษาข้อมูล
	Ministry	วิวของข้อมูลกระทรวงเจ้าของข้อมูล
	Log	วิวของการเก็บข้อมูลการใช้งาน
	Agency	วิวของหน่วยงานเจ้าของข้อมูล
	Department	วิวของทบวงกรมของเจ้าของข้อมูล
	Training	วิวของหลักสูตรการอบรม
	UserGroup	วิวของกลุ่มผู้ใช้งาน
Schedule	วิวของตารางเวลาในการจัดเก็บรักษาข้อมูล	

ตารางที่ 4.6 ตัวอย่างรายละเอียดสถาปัตยกรรมเอ็มวีซีของเครื่องมือสนับสนุนคลังสารสนเทศกลาง
(ต่อ)

แบบรูปเอ็มวีซี	ชื่อคลาส	คำอธิบาย
คอนโทรลเลอร์	PolicyController	คอนโทรลเลอร์ของนโยบายการใช้งาน
	PrivacyController	คอนโทรลเลอร์ของไพรเวซีผู้ใช้งานและข้อมูล
	UserController	คอนโทรลเลอร์ของผู้ใช้งานคลังสารสนเทศกลาง
	RoleController	คอนโทรลเลอร์ของบทบาทผู้ใช้งาน
	DataController	คอนโทรลเลอร์ของข้อมูลในคลังสารสนเทศกลาง
	ActionController	คอนโทรลเลอร์ของการกระทำ
	ConditionController	คอนโทรลเลอร์ของเงื่อนไขการใช้งานข้อมูล
	ObligationController	คอนโทรลเลอร์ของภาระผูกพันการใช้งานข้อมูล
	PurposeController	คอนโทรลเลอร์ของวัตถุประสงค์ใช้งานข้อมูล
	RetainController	คอนโทรลเลอร์ของการเก็บรักษาข้อมูล
	MinistryController	คอนโทรลเลอร์ของข้อมูลกระทรวงเจ้าของข้อมูล
	LogController	คอนโทรลเลอร์ของการเก็บข้อมูลการใช้งาน
	AgencyController	คอนโทรลเลอร์ของหน่วยงานเจ้าของข้อมูล
	DepartmentController	คอนโทรลเลอร์ของทบวงกรมของเจ้าของข้อมูล
	TrainingController	คอนโทรลเลอร์ของหลักสูตรการอบรม
	UserGroupController	คอนโทรลเลอร์ของกลุ่มผู้ใช้งาน
ScheduleController	คอนโทรลเลอร์ของตารางเวลาในการจัดเก็บรักษาข้อมูล	

4.2.5 เครื่องมือที่ใช้ในการออกแบบและพัฒนาเครื่องมือสนับสนุนคลังสารสนเทศกลาง

ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ในการพัฒนาเครื่องมือสนับสนุนคลังสารสนเทศกลางในงานวิจัยนี้มีรายละเอียดดังนี้

1) ด้านฮาร์ดแวร์

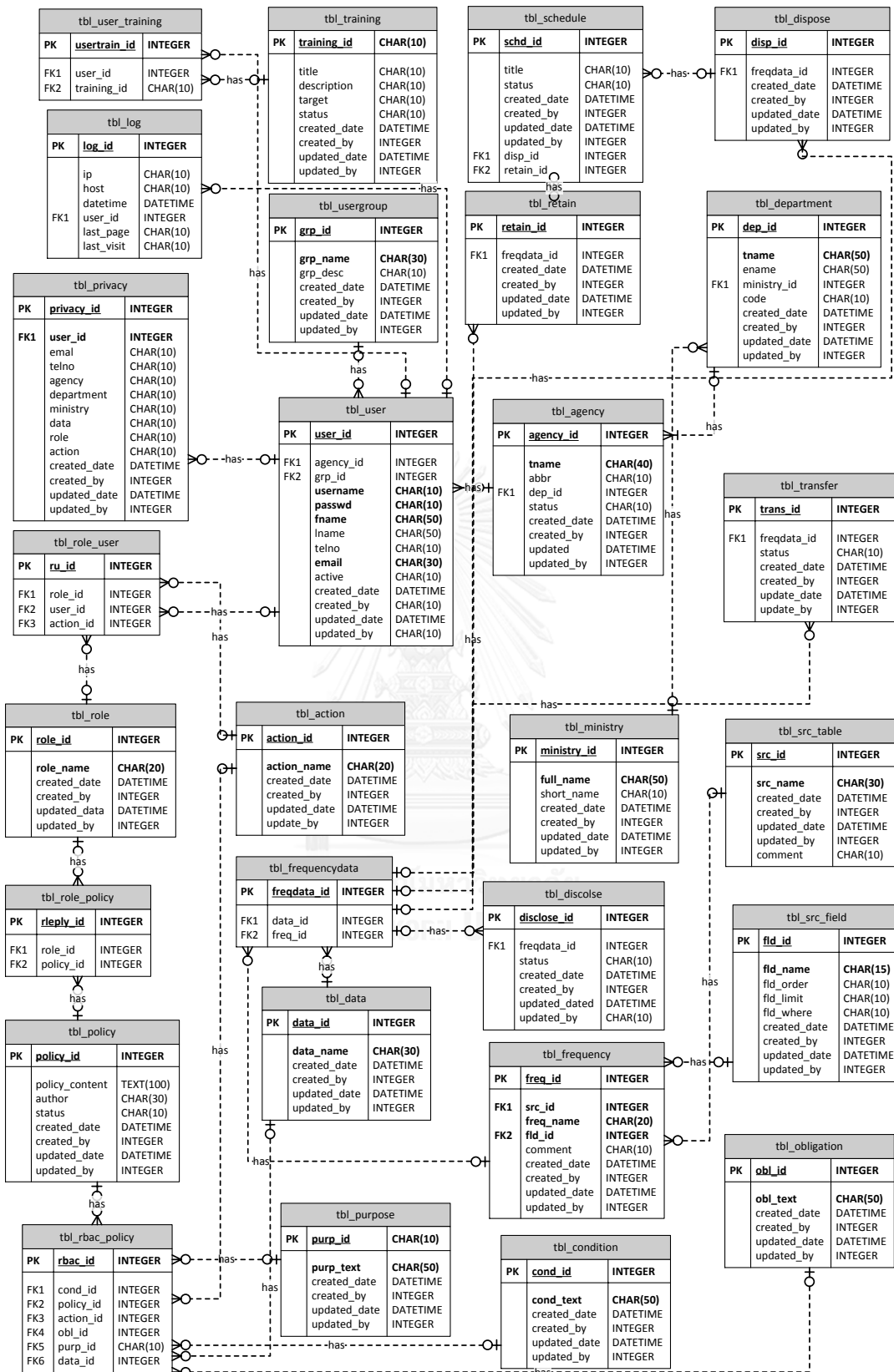
- เครื่องคอมพิวเตอร์ส่วนบุคคล Intel core 2 Duo ความเร็ว 2.4 กิกะเฮิรตซ์
- หน่วยความจำ (Memory) 8 กิกะไบต์
- จานบันทึกแบบแข็ง (Hard disk) ความจุ 512 กิกะไบต์

2) ด้านซอฟต์แวร์

- บรรณาธิการข้อความ (Sublime Text3 Text Editor)
- ลาราวเวลเฟรมเวิร์ค (Laravel) เป็นชุดเครื่องมือสำหรับพัฒนาเว็บแอปพลิเคชัน
- พีเอชพี (PHP) ภาษาคอมพิวเตอร์ในลักษณะเซิร์ฟเวอร์-ไซด์ สคริปต์
- อะแพชี เว็บเซิร์ฟเวอร์ (Apache Webserver) เครื่องมือทำหน้าที่ให้บริการเว็บเซิร์ฟเวอร์ผ่านโพรโทคอล เอชทีทีพี (HTTP)
- โปสท์เกรสคิวเอล (PostgreSQL) เครื่องมือบริหารจัดการฐานข้อมูล
- ลินุกซ์มินต์ (LinuxMint) ระบบปฏิบัติการ ใช้ในการพัฒนาระบบ
- กูเกิลโครม เว็บเบราว์เซอร์ ใช้เพื่อทดสอบการแสดงผลระบบ
- ไฟร์ฟอกซ์ เว็บเบราว์เซอร์ ใช้เพื่อทดสอบการแสดงผลระบบ

4.2.6 แบบจำลองข้อมูลในการอิมพลิเมนต์ของเครื่องมือสนับสนุนคลังสารสนเทศกลาง

การออกแบบ แบบจำลองข้อมูลของเครื่องมือสนับสนุนสำหรับการใช้งานคลังสารสนเทศกลาง เป็นแบบจำลองข้อมูลโครงสร้างฐานข้อมูลเชิงสัมพันธ์ (Relational database) แผนภาพแสดงความสัมพันธ์ระหว่างเอนทิตี (Entity relationship diagram) ปรากฏในรูปที่ 4.6



รูปที่ 4.6 ความสัมพันธ์ระหว่างเอนทิตีของเครื่องมือสนับสนุนคลังสารสนเทศกลาง

จากแผนภาพแสดงความสัมพันธ์ระหว่างเอนทิตีจากรูปที่ 4.6 ในตารางที่ 4.7 แสดงคำอธิบายตารางเอนทิตีของเครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลาง รายละเอียดคำอธิบายตารางเอนทิตีของเครื่องมือสนับสนุนทั้งหมดแสดงในภาคผนวก ข

ตารางที่ 4.7 ชื่อตารางและคำอธิบายในการอิมพลีเมนต์ระบบ

ลำดับ	ชื่อตาราง	คำอธิบาย
1	tbl_user_training	ตารางจัดเก็บข้อมูลการอบรมของผู้ใช้
2	tbl_log	ตารางจัดเก็บข้อมูลการเข้าใช้งานระบบของผู้ใช้งาน
3	tbl_privacy	ตารางจัดเก็บข้อมูลไพรเวซี
4	tbl_role_user	ตารางจัดเก็บข้อมูลบทบาทของผู้ใช้งาน
5	tbl_training	ตารางจัดเก็บข้อมูลรายละเอียดเกี่ยวกับการอบรม
6	tbl_usergroup	ตารางจัดเก็บข้อมูลรายละเอียดกลุ่มผู้ใช้งาน
7	tbl_user	ตารางจัดเก็บข้อมูลรายละเอียดผู้ใช้
8	tbl_agency	ตารางจัดเก็บข้อมูลรายละเอียดหน่วยงาน
9	tbl_retain	ตารางจัดเก็บข้อมูลรายละเอียดเกี่ยวกับการรักษาข้อมูล
10	tbl_schedule	ตารางจัดเก็บข้อมูลตารางเวลาเก็บรักษา/ทำลาย
11	tbl_dispose	ตารางจัดเก็บข้อมูลรายละเอียดทำลายข้อมูล
12	tbl_department	ตารางจัดเก็บข้อมูลรายละเอียดแผนก
13	tbl_transfer	ตารางจัดเก็บข้อมูลเกี่ยวกับการส่งต่อข้อมูล
14	tbl_role	ตารางจัดเก็บข้อมูลรายละเอียดบทบาท
15	tbl_role_policy	ตารางจัดเก็บข้อมูลรายละเอียดบทบาทจากนโยบาย
16	tbl_policy	ตารางจัดเก็บข้อมูลรายละเอียดนโยบายการใช้งาน
17	tbl_rbac_policy	ตารางจัดเก็บข้อมูลเอนทิตีของนโยบายการใช้งาน
18	tbl_purpose	ตารางจัดเก็บข้อมูลรายละเอียดวัตถุประสงค์การใช้งาน

ตารางที่ 4.7 ชื่อตารางและคำอธิบายในการอิมพลิเมนต์ระบบ (ต่อ)

ลำดับ	ชื่อตาราง	คำอธิบาย
19	tbl_data	ตารางจัดเก็บรายละเอียดข้อมูลที่ให้บริการ
20	tbl_frequencydata	ตารางจัดเก็บข้อมูลรายละเอียดช่วงเวลาของข้อมูล
21	tbl_action	ตารางจัดเก็บข้อมูลรายละเอียดของแต่ละการกระทำ
22	tbl_ministry	ตารางจัดเก็บข้อมูลรายละเอียดกระทรวง
23	tbl_disclose	ตารางจัดเก็บข้อมูลรายละเอียดการเปิดเผยข้อมูล
24	tbl_frequency	ตารางจัดเก็บข้อมูลรายละเอียดความถี่ข้อมูล
25	tbl_condition	ตารางจัดเก็บข้อมูลรายละเอียดของเงื่อนไขการใช้งาน
26	tbl_src_table	ตารางจัดเก็บข้อมูลชื่อตารางข้อมูลคลังสารสนเทศกลาง
27	tbl_src_field	ตารางจัดเก็บข้อมูลฟิลด์ของข้อมูลเพื่อใช้เรียกข้อมูล
28	tbl_obligation	ตารางจัดเก็บข้อมูลรายละเอียดข้อผูกพันการใช้งาน

4.2.7 การออกแบบฟังก์ชันงานและส่วนต่อประสานผู้ใช้งาน

เครื่องมือสนับสนุนคลังสารสนเทศกลาง งานวิจัยนี้ได้พัฒนาในรูปแบบเว็บแอปพลิเคชัน โดยมีบทบาทผู้ใช้งานที่เกี่ยวข้องกับเครื่องมือสนับสนุนดังแสดงในตารางที่ 4.8 และในตารางที่ 4.9 แสดงความสัมพันธ์ระหว่างผู้ใช้งานเครื่องมือสนับสนุนและฟังก์ชันงานของเครื่องมือสนับสนุน

ส่วนต่อประสานของเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางแบ่งออกเป็น 2 ส่วนประกอบด้วย

- 1.) ส่วนต่อประสานการจัดการหลังบ้าน สำหรับเจ้าหน้าที่คลังสารสนเทศกลาง
- 2.) ส่วนต่อประสานการใช้งาน สำหรับผู้ใช้งานเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลาง

ตารางที่ 4.9 ความสัมพันธ์ระหว่างผู้ใช้งานและฟังก์ชันงานของเครื่องมือสนับสนุน (ต่อ)

ฟังก์ชันงาน/เมนู	บทบาท								
	R1	R2	R3	R4	R5	R6	R7	R8	R9
14. เพิ่ม/บันทึก/แก้ไข/ลบ การเก็บรักษาและทำลายข้อมูล	✓	-	-	-	-	-	-	-	-
15. แสดงรายการ การเก็บรักษาและทำลายข้อมูล	✓	✓	✓	✓	✓	✓	✓	✓	✓
16. เพิ่ม/บันทึก/แก้ไข/ลบ สิทธิบทบาท	✓	-	-	-	-	-	-	-	-
17. บันทึก/แก้ไข/ตรวจสอบ การมอบหมายสิทธิบทบาท	✓	-	-	-	-	-	-	-	-
18. บันทึก/แสดงรายการ/ค้นหา/ตรวจสอบสถานะ คำร้องขอส่งต่อข้อมูล	✓	✓	✓	✓	✓	✓	✓	✓	-
19. แสดงรายงานคำร้องขอส่งต่อข้อมูล	✓	✓	✓	✓	✓	✓	✓	✓	-
20. บันทึก/แสดงรายการ/ค้นหา/ตรวจสอบสถานะ คำร้องขอเปิดเผยข้อมูล	✓	✓	✓	✓	✓	✓	✓	✓	-
21. แสดงรายงานคำร้องขอเปิดเผยข้อมูล	✓	✓	✓	✓	✓	✓	✓	✓	-
22. แสดงตัวอย่างรหัสผ่าน	✓	✓	✓	✓	✓	✓	✓	✓	✓
23. แสดงคำแนะนำการสร้างรหัสผ่าน	✓	✓	✓	✓	✓	✓	✓	✓	✓

1) ส่วนต่อประสานการจัดการหลังบ้าน

ส่วนต่อประสานของเครื่องมือสนับสนุนสำหรับจัดการหลังบ้านดำเนินการโดยเจ้าหน้าที่คลังสารสนเทศกลาง รายละเอียดส่วนตัวประสานแสดงอยู่ใน ตารางที่ ค.1 ภาคผนวก ค ตัวอย่างของส่วนต่อประสานสำหรับเจ้าหน้าที่คลังสารสนเทศกลางมีดังต่อไปนี้

- การสกัดเอนทิตีนโยบาย เมื่อเจ้าหน้าที่คลังสารสนเทศกลางดำเนินการกดปุ่มฟิวส์บีเอซีซึ่งปรากฏอยู่ในแต่ละรายการนโยบายการใช้งานคลังสารสนเทศกลาง ระบบจะนำเจ้าหน้าที่คลังสารสนเทศมายังหน้าสกัดเอนทิตีนโยบายการใช้งานคลังสารสนเทศกลาง ดังปรากฏในรูปที่ 4.7 เจ้าหน้าที่คลังสารสนเทศกลางพิจารณานโยบายการใช้งานที่กำลังดำเนินการสกัดเอนทิตีนั้น มีเอนทิตีอะไรบ้าง เมื่อทำการสกัดนโยบายการใช้เสร็จเจ้าหน้าที่คลังสารสนเทศกลางบันทึกจัดเก็บเอนทิตีเหล่านั้นเก็บไว้ในฐานข้อมูล

NHC ค้นหา นโยบายคลังฯ พอร์ทัลบีเอสอี ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักศูตรอบรม superadmin (กลุ่ม: SUPER ADMIN) การตั้งค่า

หน้าหลัก / นโยบายคลังฯ / แปลงนโยบายตามพอร์ทัลบีเอสอี / นโยบายคลังฯที่: 1

แผนผังอาร์บีเอสอี/นโยบายคลังฯ

นักวิจัยได้รับอนุญาตให้เรียกดูข้อมูล ปริมาณน้ำฝน โดยจะต้องเข้าสู่ระบบก่อนที่จะเรียกดูข้อมูลตามความถี่ของข้อมูลดังนี้

1. ข้อมูลปริมาณน้ำฝนราย 24 ชั่วโมง
2. ข้อมูลปริมาณน้ำฝนวันนี้
3. ข้อมูลปริมาณน้ำฝนวานนี้
4. ข้อมูลปริมาณน้ำฝนย้อนหลัง 3 วัน
5. ข้อมูลปริมาณน้ำฝนย้อนหลัง 7 วัน โดยมีวัตถุประสงค์เพื่องานวิจัยข้อมูลเท่านั้น และเมื่อต้องการดาวน์โหลดข้อมูลจะต้องได้รับความยินยอมจากเจ้าหน้าที่คลังข้อมูลแห่งชาติก่อนหลังจากออกจากระบบ ระบบจะทำการบันทึกประวัติการเรียกดูข้อมูลดังกล่าว

บทบาท	ข้อมูล	การกระทำ	วัตถุประสงค์	เงื่อนไข	ข้อมูลพื้นที่
นักวิจัย	ปริมาณน้ำฝนราย 24 ชั่วโมง	เรียกดูข้อมูล	เพื่องานวิจัย	ข้อมูลปัจจุบัน	เข้าสู่ระบบก่อน
	ปริมาณน้ำฝนวันนี้			ข้อมูลย้อนหลัง 3 วัน	บันทึกประวัติการใช้งานก่อนออกจากระบบ
	ปริมาณน้ำฝนวานนี้			ข้อมูลย้อนหลัง 7 วัน	

บทบาท:

ข้อมูล: นักวิจัย นักพัฒนาระบบ

การกระทำ: ผู้ดูแลฐานข้อมูล วัตถุประสงค์

วัตถุประสงค์: เจ้าหน้าที่ประจำหน่วยงาน เจ้าหน้าที่คลังข้อมูล

เงื่อนไข: บุคคลทั่วไป

ข้อมูลพื้นที่:

รูปที่ 4.7 ขั้นตอนการสกัดเอนทิตีนโยบายการใช้งานคลังสารสนเทศกลาง

- เมนูพอร์ทัลบีเอสอี เมื่อเจ้าหน้าที่คลังสารสนเทศกลางดำเนินการกดปุ่มพอร์ทัลบีเอสอีซึ่งจะประกอบด้วยเมนูย่อยตามเอนทิตีในงานวิจัย [11] ซึ่งในแต่ละเอนทิตีจะถูกใช้สำหรับการแยกเอนทิตีของนโยบายการใช้งานคลังสารสนเทศกลางเช่น ชื่อบทบาท ชื่อการกระทำ ชื่อข้อมูล ชื่อเงื่อนไข ชื่อข้อมูลพื้นที่และชื่อวัตถุประสงค์ เป็นต้น ดังปรากฏในรูปที่ 4.8

รหัส	ชื่อบทบาท	
1	นักวิจัย	แก้ไข ลบทิ้ง
2	นักพัฒนาระบบ	แก้ไข ลบทิ้ง
3	ผู้ดูแลฐานข้อมูล	แก้ไข ลบทิ้ง
4	เจ้าหน้าที่ประจำหน่วยงาน	แก้ไข ลบทิ้ง
5	เจ้าหน้าที่คลังข้อมูล	แก้ไข ลบทิ้ง
6	บุคคลทั่วไป	แก้ไข ลบทิ้ง

รูปที่ 4.8 การจัดเตรียมบทบาทผู้ใช้งานเครื่องมือสนับสนุน

- เมนูผู้ใช้งานและหน่วยงาน ประกอบด้วยเมนูย่อยคือ เมนูผู้ใช้งานในระบบ เป็นส่วนสำหรับบริหารจัดการผู้ใช้งานคลังสารสนเทศกลาง เจ้าหน้าที่คลังสารสนเทศกลางสามารถเปลี่ยนแปลงประเภทผู้ใช้งาน มอบหมายบทบาทให้กับผู้ใช้งาน ดังปรากฏในรูปที่ 4.9 เมนูผู้รับผิดชอบนโยบาย เป็นส่วนสำหรับให้เจ้าหน้าที่คลังสารสนเทศกลางบริหารจัดการผู้รับผิดชอบนโยบายการใช้งานคลังสารสนเทศกลาง ดังปรากฏในรูปที่ 4.10 เมนูหน่วยงาน มีหน้าที่สำหรับแสดงรายชื่อหน่วยงานเจ้าของทั้งหมดที่อยู่ในคลังสารสนเทศกลางดังปรากฏในรูปที่ 4.11

NHC ค้นหา นโยบายคลังฯ ทิวารีบีไอซี ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักสูตรอบรม เอกสาร superadmin (กลุ่ม: SUPER ADMIN)

หน้าหลัก / รายการผู้ใช้งาน / ผู้ใช้งานในระบบ

แผงผู้ใช้งานในระบบ

10 แถวต่อหน้า ค้นหา :

รหัส	ชื่อผู้ใช้	นามสกุล	บทบาท	วันที่ลงทะเบียน	ประเภทผู้ใช้	สถานะ	
1	user1	User1_test	นักวิจัย	2014-06-10	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
2	user2	User2	เจ้าหน้าที่ประจำหน่วยงาน	2014-06-10	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
3	user3	User3	นักวิจัย	2014-06-10	ทั่วไป	เปิดใช้งาน	แก้ไข
4	user4	User4	ผู้ดูแลฐานข้อมูล	2014-06-10	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
5	user5	user5	นักวิจัย	2014-10-13	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
6	user6	user6	นักวิจัย	2014-10-13	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
7	user7	user7	นักพัฒนาระบบ	2014-10-13	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข

แสดง 1 ถึง 7 จากทั้งหมด 7 แถว

ถอยหลัง 1 1 หน้า

รูปที่ 4.9 รายการผู้ใช้งานเครื่องมือสนับสนุนทั้งหมด

NHC ค้นหา นโยบายคลังฯ ทิวารีบีไอซี ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักสูตรอบรม เอกสาร superadmin (กลุ่ม: SUPER ADMIN)

รายการผู้ใช้งาน / ผู้รับผิดชอบนโยบาย / รายการผู้รับผิดชอบนโยบาย

แผงผู้ใช้งานในระบบ

10 แถวต่อหน้า ค้นหา :

เพิ่มผู้รับผิดชอบ

ลำดับ	ชื่อ	นามสกุล	ตำแหน่ง	เบอร์ติดต่อ	อีเมล	วันที่เพิ่ม	สถานะ	
1	user3	user3	หัวหน้ากลุ่มงานระบบคอมพิวเตอร์และระบบเครือข่าย	02 123 4567 ต่อ 003	user3@localhost	2014-07-08	ระงับใช้งาน	แก้ไข
2	user2	user2	หัวหน้ากลุ่มงานพัฒนาระบบงาน	02 123 4567 ต่อ 002	user2@localhost	2014-07-08	เปิดใช้งาน	แก้ไข
3	user1	user1	ผู้อำนวยการฝ่ายวิจัยและพัฒนา	02 123 4567 ต่อ 001	user1@localhost	2014-07-08	เปิดใช้งาน	แก้ไข

แสดง 1 ถึง 3 จากทั้งหมด 3 แถว

ถอยหลัง 1 1 หน้า

รูปที่ 4.10 รายชื่อผู้รับผิดชอบนโยบายการใช้งานคลังสารสนเทศกลาง

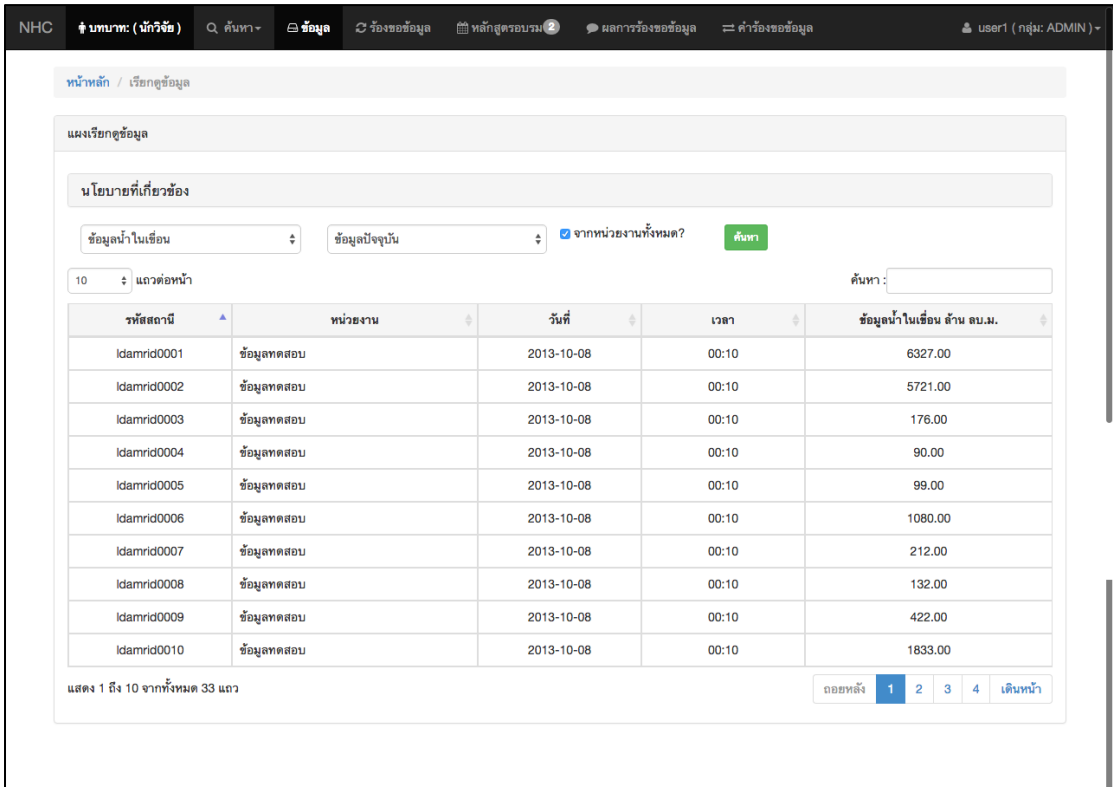
ลำดับ	รหัส	ชื่อหน่วยงาน	ชื่อย่อ	กระทรวง	ดำเนินการ
1	00006	หน่วยงานที่ 6	FFF	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
2	00002	หน่วยงานที่ 2	BBB	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
3	00008	หน่วยงานที่ 8	HHH	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
4	00009	หน่วยงานที่ 9	III	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
5	00012	หน่วยงานที่ 12	MMM	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
6	00001	หน่วยงานที่ 1	AAA	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
7	00003	หน่วยงานที่ 3	CCC	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
10	00005	หน่วยงานที่ 5	EEE	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
11	00011	หน่วยงานที่ 11	LLL	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
12	00007	หน่วยงานที่ 7	GGG	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง

รูปที่ 4.11 รายชื่อหน่วยงานเชื่อมโยงข้อมูลในคลังสารสนเทศกลาง

2) ส่วนต่อประสานการใช้งานสำหรับผู้ใช้งาน

ส่วนต่อประสานการใช้งานสำหรับผู้ใช้งานคลังสารสนเทศกลาง โดยผู้ที่ใช้งานจะต้องลงทะเบียนเพื่อใช้งานเครื่องมือสนับสนุน รายละเอียดสำหรับผู้ใช้งานคลังสารสนเทศกลางแสดงอยู่ในตาราง ค.2 ภาคผนวก ค ตัวอย่างส่วนต่อประสานสำหรับผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลางมีดังต่อไปนี้

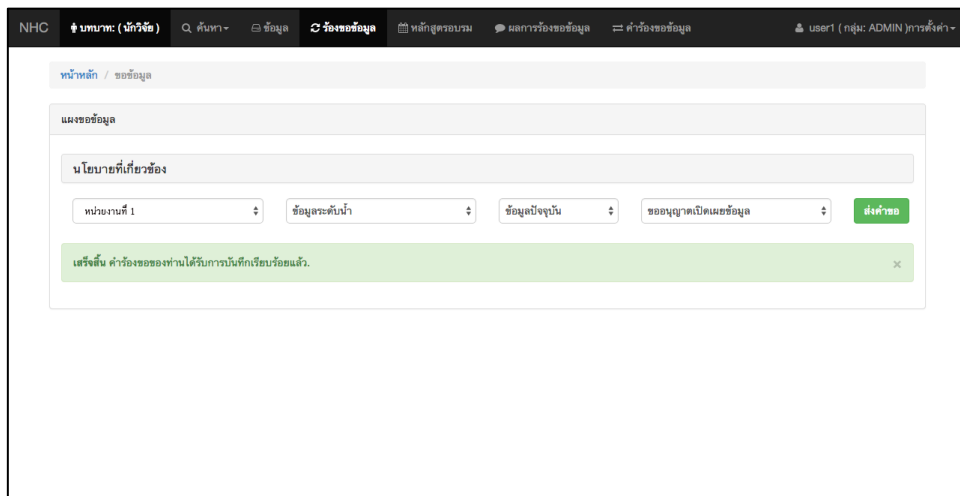
- เมนูข้อมูล คือการแสดงผลรายการข้อมูลให้กับผู้ใช้งาน การแสดงรายการข้อมูลนั้นเป็นไปตามบทบาทที่ผู้ใช้งานได้รับมอบหมายตัวอย่างเช่น นักวิจัย สามารถเรียกดูข้อมูลได้เฉพาะ ข้อมูลระดับน้ำ ปริมาณน้ำในเขื่อนและปริมาณน้ำฝนราย 24 ชั่วโมง เป็นต้น ระบบจะไม่แสดงข้อมูลให้ผู้ใช้งานนอกเหนือจากข้อมูลที่นโยบายได้กำหนดไว้ให้ผู้ใช้งาน ตัวอย่างของการเรียกดูข้อมูลปรากฏในรูปที่ 4.12



รหัสสถานี	หน่วยงาน	วันที่	เวลา	ข้อมูลนำในเขียน ล้าน ลบ.ม.
Idamrid0001	ข้อมูลทดสอบ	2013-10-08	00:10	6327.00
Idamrid0002	ข้อมูลทดสอบ	2013-10-08	00:10	5721.00
Idamrid0003	ข้อมูลทดสอบ	2013-10-08	00:10	176.00
Idamrid0004	ข้อมูลทดสอบ	2013-10-08	00:10	90.00
Idamrid0005	ข้อมูลทดสอบ	2013-10-08	00:10	99.00
Idamrid0006	ข้อมูลทดสอบ	2013-10-08	00:10	1080.00
Idamrid0007	ข้อมูลทดสอบ	2013-10-08	00:10	212.00
Idamrid0008	ข้อมูลทดสอบ	2013-10-08	00:10	132.00
Idamrid0009	ข้อมูลทดสอบ	2013-10-08	00:10	422.00
Idamrid0010	ข้อมูลทดสอบ	2013-10-08	00:10	1833.00

รูปที่ 4.12 การเรียกดูข้อมูลในคลังสารสนเทศกลางตามบทบาทนักวิจัย

- เมนูร้องขอข้อมูล ดำเนินการโดยผู้ใช้งาน ในกรณีที่ผู้ใช้งานจำเป็นต้องใช้ข้อมูลที่ผู้ใช้งานไม่มีสิทธิ ผู้ใช้งานจะดำเนินการกรอกคำร้องขอใช้ข้อมูล เพื่อส่งยังเจ้าของข้อมูลพิจารณาตามเหตุผลของคำร้องขอ หลังจากได้รับการอนุญาตจากเจ้าของข้อมูล ผู้ใช้งานจึงจะสามารถนำข้อมูลดังกล่าวไปใช้งานตามวัตถุประสงค์ ดังปรากฏในรูปที่ 4.13



รูปที่ 4.13 ตัวอย่างการร้องขอข้อมูลเปิดเผยข้อมูลผ่านเครื่องมือสนับสนุน

- เมนูผลการร้องขอข้อมูล เมื่อผู้ใช้งานกดปุ่มผลการร้องขอซึ่งจะแสดงตัวเลขตามผลการร้องขอจากเจ้าของข้อมูลที่ได้อนุมัติคำร้อง ดังปรากฏในรูปที่ 4.14 โดยแสดงวันเวลาที่ร้องขอข้อมูลและวันเวลาที่เจ้าของข้อมูลพิจารณาอนุมัติ

*ข้อมูลที่ร้องขอ	ความถี่ข้อมูล	สถานะการร้องขอ	*วัตถุประสงค์การขอ	*ผู้อนุมัติ	*หน่วยงานข้อมูล	วันที่อนุมัติ	วันที่ร้องขอ	หมายเหตุ
ข้อมูลระดับน้ำ	ข้อมูลปัจจุบัน	ยื่นขอการร้องขอ	ขออนุญาตเปิดเผยข้อมูล	user6 user6 (นักวิจัย)	หน่วยงานที่ 1	2014-10-15	2014-10-15	ดาวน์โหลด
*ข้อมูลที่ร้องขอ	ความถี่ข้อมูล	สถานะการร้องขอ	*วัตถุประสงค์การขอ	*ผู้อนุมัติ	*หน่วยงานข้อมูล	วันที่อนุมัติ	วันที่ร้องขอ	หมายเหตุ

แสดง 1 ถึง 1 จากทั้งหมด 1 แถว

ถอยหลัง 1 เดินหน้า

รูปที่ 4.14 รายการผลการพิจารณาการร้องขอข้อมูล

4.3 การทดสอบเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

วัตถุประสงค์หลักของการทดสอบเครื่องมือสนับสนุนคลังสารสนเทศกลาง เพื่อตรวจสอบความถูกต้องและหาข้อผิดพลาดที่เกิดขึ้นของระบบ โดยแบ่งการทดสอบออกเป็น 3 การทดสอบคือ

- 1) การทดสอบระดับหน่วยย่อย (Unit testing)
- 2) การทดสอบระดับรวมหน่วย (Integration testing)
- 3) การทดสอบระดับระบบ (System testing)

4.3.1 การทดสอบเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางระดับหน่วยย่อย

การทดสอบระดับหน่วยย่อย (Unit testing) ได้ทำการทดสอบแบบกล่องดำ (Black-Box Testing) เป็นการทดสอบหน่วยย่อยๆ ของฟังก์ชันและการทำงานของเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลาง การทดสอบในลักษณะนี้จะเป็นการทดสอบที่อยู่ในช่วงของการพัฒนาเครื่องมือ

เครื่องมือสนับสนุนสำหรับใช้งานคลังสารสนเทศกลาง ทั้งนี้ก็เพื่อความถูกต้องและจัดซื้อผิดพลาดของหน่วยย่อยนั้น ตัวอย่างของกรณีทดสอบระดับหน่วยย่อยปรากฏอยู่ในตารางที่ 4.10 - 4.11

ตารางที่ 4.10 ตัวอย่างกรณีการบันทึกนโยบายการใช้งานเข้าสู่ระบบ

รหัสกรณีทดสอบ	TCUT-001			
ชื่อกรณีทดสอบ	บันทึกนโยบายการใช้งานเข้าสู่ระบบ			
วัตถุประสงค์	ทำการตรวจสอบว่าเครื่องมือสนับสนุนสามารถบันทึกนโยบายการใช้งานเข้าสู่ระบบได้			
เงื่อนไขเริ่มต้นทดสอบ	-			
เงื่อนไขจบทดสอบ	ข้อความบันทึกสำเร็จแจ้งให้เจ้าหน้าที่คลังสารสนเทศกลางทราบ			
ข้อมูลนำเข้า	- เนื้อหานโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี			
ข้อมูลนำออก	ข้อความบันทึกสำเร็จแจ้งให้เจ้าหน้าที่คลังสารสนเทศกลางทราบ			
ลำดับ	คำอธิบาย	ผลลัพธ์ที่คาดหวัง	ผลลัพธ์ที่ได้	ผลการประเมิน
1.	ระบบตรวจสอบฟิลด์ที่จำเป็นต้องระบุเนื้อหา	มีการกรอกข้อมูลในแบบฟอร์ม ที่ระบุว่าจำเป็นต้องกรอกข้อมูล	เป็นไปตามผลที่คาดหวัง	ผ่าน
2.	ระบบตรวจสอบเนื้อหานโยบายว่ามีเนื้อหามากกว่า 10 ตัวอักษร	มีการกรอกข้อมูลนโยบายการใช้งาน	เป็นไปตามผลที่คาดหวัง	ผ่าน
3.	ระบบตรวจสอบมีการกำหนดผู้รับผิดชอบนโยบายการใช้งาน	มีการกำหนดชื่อผู้รับผิดชอบนโยบาย	เป็นไปตามผลที่คาดหวัง	ผ่าน
4.	ระบบทำการบันทึกนโยบายการใช้งาน	ระบบบันทึกสำเร็จ	เป็นไปตามผลที่คาดหวัง	ผ่าน
สรุปผลการทดสอบ		ผ่าน		

ตารางที่ 4.11 ตัวอย่างกรณีทดสอบการค้นหानโยบายโดยระบุคำค้นหา

รหัสกรณีทดสอบ	TCUT-002			
ชื่อกรณีทดสอบ	บันทึกนโยบายการใช้งานเข้าสู่ระบบ			
วัตถุประสงค์	ทำการตรวจสอบว่าเครื่องมือสนับสนุนสามารถค้นหานโยบายจากคำค้นหาได้			
เงื่อนไขเริ่มต้นทดสอบ	-			
เงื่อนไขจบทดสอบ	แสดงนโยบายที่ตรงกับคำค้นหา			
ข้อมูลนำเข้า	- คำค้นหานโยบายการใช้งาน			
ข้อมูลนำออก	นโยบายการใช้งานคลังสารสนเทศกลางที่ตรงกับคำค้น			
ลำดับ	คำอธิบาย	ผลลัพธ์ที่คาดหวัง	ผลลัพธ์ที่ได้	ผลการประเมิน
1.	ระบบตรวจสอบคำค้นหาไม่เป็นค่าว่าง	ต้องมีการระบุคำค้นหานโยบายการใช้งาน	เป็นไปตามผลที่คาดหวัง	ผ่าน
2.	ระบบตรวจสอบคำค้นหาที่มีความยาวไม่ต่ำกว่า 3 ตัวอักษร	ต้องมีการระบุคำค้นหานโยบายการใช้งาน	เป็นไปตามผลที่คาดหวัง	ผ่าน
3.	ระบบค้นหานโยบายการใช้งานตามคำค้นหาในฐานข้อมูล	ได้จำนวนผลลัพธ์ที่ได้จากการค้นหา	เป็นไปตามผลที่คาดหวัง	ผ่าน
4.	ระบบแสดงนโยบายการใช้งานที่ตรงกับคำค้นหา	แสดงรายการนโยบายที่ตรงกับคำค้นหา	เป็นไปตามผลที่คาดหวัง	ผ่าน
สรุปผลการทดสอบ		ผ่าน		

4.3.2 การทดสอบเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางระดับรวมหน่วย

การทดสอบเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางระดับรวมหน่วย (Integration testing) เป็นการทดสอบการทำงานของกลุ่มฟังก์ชัน ทั้งนี้ก็เพื่อดูความสามารถของเครื่องมือสนับสนุนคลังสารสนเทศกลาง ในการทำงานร่วมกันได้ของฟังก์ชันหรือหน่วยย่อยดังกล่าวในขั้นตอนการทดสอบนี้ใช้การทดสอบระดับรวมหน่วยทั้งหมดแล้วทดสอบในครั้งเดียว (Big Bang) ตัวอย่างการทดสอบระดับรวมหน่วยปรากฏในตารางที่ 4.12 - 4.13

ตารางที่ 4.12 ตัวอย่างกรณีทดสอบการบันทึกประวัติข้อมูล

รหัสกรณีทดสอบ	TCIT-001			
ชื่อกรณีทดสอบ	การบันทึกประวัติข้อมูล			
วัตถุประสงค์	ทำการตรวจสอบการบันทึกประวัติข้อมูลของหน่วยงานได้			
เงื่อนไขเริ่มทดสอบ	-			
เงื่อนไขจบทดสอบ	แสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ			
ข้อมูลนำเข้า	-			
ข้อมูลนำออก	แสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ			
ลำดับ	คำอธิบาย	ผลลัพธ์ที่คาดหวัง	ผลลัพธ์ที่ได้	ผลการประเมิน
1.	ระบบตรวจสอบการเข้าสู่ระบบ	ผู้ใช้งานเข้าสู่ระบบ	เป็นไปตามผลที่คาดหวัง	ผ่าน
2.	ระบบตรวจสอบว่าผู้ใช้งานที่เข้าสู่ระบบเป็นเจ้าหน้าที่ประจำหน่วยงานประเภทผู้ดูแลระบบ	ผู้ใช้งานระบบต้องมีสิทธิเป็นผู้ดูแลระบบประจำหน่วยงาน	เป็นไปตามผลที่คาดหวัง	ผ่าน
3.	ระบบเรียกรายการข้อมูลที่สอดคล้องกับหน่วยงานที่ผู้ใช้งานปฏิบัติหน้าที่	แสดงรายการข้อมูลที่เกี่ยวข้องกับหน่วยงานผู้ใช้งาน	เป็นไปตามผลที่คาดหวัง	ผ่าน
4.	ระบบบันทึกประวัติข้อมูล	ระบบบันทึกประวัติข้อมูลสำเร็จ	เป็นไปตามผลที่คาดหวัง	ผ่าน
5.	ระบบแสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ	แสดงข้อความให้ผู้ใช้งานทราบ	เป็นไปตามผลที่คาดหวัง	ผ่าน
สรุปผลการทดสอบ		ผ่าน		

ตารางที่ 4.13 ตัวอย่างกรณีทดสอบการบันทึกเข้ารับการอบรม

รหัสกรณีทดสอบ	TCIT-002			
ชื่อกรณีทดสอบ	การบันทึกเข้ารับการอบรม			
วัตถุประสงค์	ทำการตรวจสอบการบันทึกการเข้ารับการอบรมได้			
เงื่อนไขเริ่มทดสอบ	-			
เงื่อนไขจบทดสอบ	แสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ			
ข้อมูลนำเข้า	-			
ข้อมูลนำออก	แสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ			
ลำดับ	คำอธิบาย	ผลลัพธ์ที่คาดหวัง	ผลลัพธ์ที่ได้	ผลการประเมิน
1.	ระบบตรวจสอบการเข้าสู่ระบบ	ผู้ใช้งานเข้าสู่ระบบ	เป็นไปตามผลที่คาดหวัง	ผ่าน
2.	ระบบแสดงหลักสูตรอบรมตามกลุ่มเป้าหมายที่ตรงกับผู้ใช้งานระบบ	แสดงหลักสูตรอบรมเฉพาะที่ผู้ใช้งานเกี่ยวข้อง	เป็นไปตามผลที่คาดหวัง	ผ่าน
3.	ระบบแสดงรายละเอียดหลักสูตรอบรม	แสดงรายละเอียดหลักสูตรอบรม	เป็นไปตามผลที่คาดหวัง	ผ่าน
4.	ระบบบันทึกเข้ารับหลักสูตรอบรม	ระบบบันทึกเข้ารับหลักสูตรอบรม	เป็นไปตามผลที่คาดหวัง	ผ่าน
5.	ระบบแสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ	แสดงข้อความให้ผู้ใช้งานทราบ	เป็นไปตามผลที่คาดหวัง	ผ่าน
สรุปผลการทดสอบ	ผ่าน			

4.3.3 การทดสอบเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางระดับระบบ

การทดสอบเครื่องมือสนับสนุนสำหรับคลังสารสนเทศกลางระดับระบบ (System testing) จะทำในช่วงที่พัฒนาระบบเสร็จแล้ว การทดสอบในระดับนี้จะเป็นการทดสอบฟังก์ชันงานและการทำงานของระบบในมุมมองของผู้ใช้งานระบบ ในขั้นตอนนี้ใช้การทดสอบระบบแบบอัลฟา (Alpha Testing) ซึ่งเป็นการทดสอบการใช้งานของเครื่องมือสนับสนุนทั้งหมด โดยดำเนินการทุกอย่างให้เสมือนสภาพแวดล้อมการใช้งานจริง ตัวอย่างของการทดสอบระดับระบบดังปรากฏในตารางที่ 4.14 - 4.15

ตารางที่ 4.14 ตัวอย่างกรณีทดสอบระบบการมอบหมายสิทธิให้ใช้งาน

รหัสกรณีทดสอบ	TCST-001			
ชื่อกรณีทดสอบ	การมอบหมายบทบาทให้ใช้งาน			
วัตถุประสงค์	ทำการตรวจสอบว่าเจ้าหน้าที่คลังสารสนเทศกลางสามารถมอบหมายสิทธิให้กับผู้ใช้งานเครื่องมือสนับสนุนได้			
เงื่อนไขเริ่มต้นทดสอบ	ผู้ใช้งานเครื่องมือสนับสนุนได้ลงทะเบียนใช้งานเครื่องมือสนับสนุนแล้ว			
เงื่อนไขจบทดสอบ	แสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ			
ข้อมูลนำเข้า	-			
ข้อมูลนำออก	แสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ			
ลำดับ	คำอธิบาย	ผลลัพธ์ที่คาดหวัง	ผลลัพธ์ที่ได้	ผลการประเมิน
1.	เจ้าหน้าที่คลังสารสนเทศกลางเข้าสู่ระบบ	ระบบนำเจ้าหน้าที่คลังสารสนเทศกลางไปยังหน้าแรกของระบบ	เป็นไปตามผลที่คาดหวัง	ผ่าน
2.	เจ้าหน้าที่คลังสารสนเทศกลางเรียกรายการผู้ใช้งานในระบบทั้งหมด	ระบบแสดงรายชื่อผู้ใช้งานเครื่องมือทั้งหมดที่ลงทะเบียนใช้งาน	เป็นไปตามผลที่คาดหวัง	ผ่าน
3.	เจ้าหน้าที่คลังสารสนเทศกลางเลือกแก้ไขข้อมูลผู้ใช้งานเครื่องมือสนับสนุน	ระบบแสดงแบบฟอร์มแก้ไขรายละเอียดผู้ใช้งาน	เป็นไปตามผลที่คาดหวัง	ผ่าน
4.	เจ้าหน้าที่คลังสารสนเทศกลางเลือกบทบาทที่จะมอบหมายให้ผู้ใช้งานเครื่องมือสนับสนุน	ระบบแสดงรายการบทบาทให้เจ้าหน้าที่คลังสารสนเทศกลางเลือกให้กับผู้ใช้	เป็นไปตามผลที่คาดหวัง	ผ่าน
5.	เจ้าหน้าที่คลังสารสนเทศกลางบันทึกการเปลี่ยนแปลง	ระบบบันทึกบทบาทและผู้ใช้งานลงในฐานข้อมูล พร้อมแสดงข้อความให้เจ้าหน้าที่คลังสารสนเทศกลางได้ทราบว่าบันทึกสำเร็จ	เป็นไปตามผลที่คาดหวัง	ผ่าน
สรุปผลการทดสอบ		ผ่าน		

ตารางที่ 4.15 ตัวอย่างกรณีทดสอบระบบการร้องขอข้อมูล

รหัสกรณีทดสอบ	TCST-001			
ชื่อกรณีทดสอบ	การร้องขอข้อมูล			
วัตถุประสงค์	ทำการตรวจสอบว่าผู้ใช้งานในแต่ละบทบาทที่ได้รับสามารถร้องขอข้อมูลจากผู้ใช้งานไม่มีสิทธิจากเจ้าของข้อมูล			
เงื่อนไขเริ่มต้นทดสอบ	ผู้ใช้งานเครื่องมือสนับสนุนได้รับการมอบหมายบทบาทการใช้งานในคลังสารสนเทศกลาง			
เงื่อนไขจบทดสอบ	แสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ			
ข้อมูลนำเข้า	-			
ข้อมูลนำออก	แสดงข้อความให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ			
ลำดับ	คำอธิบาย	ผลลัพธ์ที่คาดหวัง	ผลลัพธ์ที่ได้	ผลการประเมิน
1.	ผู้ใช้งานเครื่องมือสนับสนุนเข้าสู่ระบบ	ระบบนำเจ้าหน้าที่คลังสารสนเทศกลางไปยังหน้าแรกของระบบ	เป็นไปตามผลที่คาดหวัง	ผ่าน
2.	ผู้ใช้งานเลือกเมนูร้องขอข้อมูล	ระบบแสดงรายชื่อผู้ใช้งานเครื่องมือทั้งหมดที่ลงทะเบียนใช้งาน	เป็นไปตามผลที่คาดหวัง	ผ่าน
3.	ผู้ใช้งานเลือกหน่วยงานที่ต้องการร้องขอข้อมูล	ระบบแสดงรายการข้อมูลเฉพาะที่หน่วยงานที่ถูกเลือกเป็นเจ้าของข้อมูล	เป็นไปตามผลที่คาดหวัง	ผ่าน
4.	ผู้ใช้งานเลือกข้อมูลที่ต้องการร้องขอและเหตุผลที่ร้องขอข้อมูล	ระบบแสดงรายการบทบาทให้เจ้าหน้าที่คลังสารสนเทศกลางเลือกให้กับผู้ใช้	เป็นไปตามผลที่คาดหวัง	ผ่าน
5.	ผู้ใช้งานเลือกบันทึกคำร้องขอข้อมูล	ระบบบันทึกคำร้องขอข้อมูลลงในฐานข้อมูลพร้อมแสดงข้อความให้ผู้ใช้งานได้ทราบว่าบันทึกคำร้องขอสำเร็จ	เป็นไปตามผลที่คาดหวัง	ผ่าน
สรุปผลการทดสอบ	ผ่าน			

4.3.4 ผลการทดสอบเครื่องมือสนับสนุนคลังสารสนเทศกลาง

ผลการทดสอบเครื่องมือสนับสนุนการใช้งานคลังสารสนเทศกลาง ได้ดำเนินการทดสอบทั้ง 3 ประเภทของการทดสอบคือ การทดสอบระดับหน่วยย่อย การทดสอบระดับร่วมหน่วย และการทดสอบระดับระบบ พบว่าผ่านทุกส่วนการทดสอบโดยสามารถสรุปผลตัวอย่างกรณีทดสอบได้ในตารางที่ 4.16

ตารางที่ 4.16 สรุปผลตัวอย่างการทดสอบหน้าที่การทำงานของระบบ

ชื่อกรณีทดสอบ	รหัสกรณีทดสอบ	ผลการทดสอบ	
		ผ่าน	ไม่ผ่าน
บันทึกนโยบายการใช้งานเข้าสู่ระบบ	TCUT-001	✓	
บันทึกนโยบายการใช้งานเข้าสู่ระบบ	TCUT-002	✓	
การบันทึกประวัติข้อมูล	TCIT-001	✓	
การบันทึกเข้ารับการอบรม	TCIT-001	✓	
การมอบหมายบทบาทให้ผู้ใช้งาน	TCST-001	✓	
การร้องขอข้อมูล	TCST-002	✓	

บทที่ 5 สรุปผลการวิจัย

จากการวิจัยที่ได้นำเสนอการพัฒนาแอปพลิเคชันที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลางซึ่งเป็นเครื่องมือสนับสนุนการจัดการคลังสารสนเทศกลางโดยประยุกต์ใช้แนวปฏิบัติจากกรอบงานพีบีดีพีไอเอเอที่เหมาะสมกับคลังสารสนเทศกลาง ผู้วิจัยได้สรุปการวิจัยและข้อเสนอแนะรวมถึงแนวทางในการพัฒนาในอนาคตดังนี้

5.1 สรุปผลการวิจัย

วิทยานิพนธ์นี้ได้นำเสนอแนวทางการพัฒนาแอปพลิเคชันที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลาง โดยให้ความสำคัญทั้งในด้านไพรเวซีของข้อมูลและไพรเวซีของผู้ใช้งานในคลังสารสนเทศกลางโดยประยุกต์ใช้แนวปฏิบัติที่ระบุไว้ในกรอบการทำงานพีบีดีพีไอเอ [8] เพื่อให้องค์กรสามารถกำหนดนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซี ตลอดจนสกัดเอาตินโยบายการใช้งานสำหรับคลังสารสนเทศกลางเพื่อใช้ในการกำหนดบทบาทผู้ใช้งานผ่านเครื่องมือสนับสนุนทั้งได้ใช้หน่วยงานแห่งหนึ่งเป็นกรณีศึกษา โดยขั้นตอนการพัฒนาแอปพลิเคชันที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลางประกอบด้วย 3 ขั้นตอนดังนี้

1.) การสร้างนโยบายการใช้งานที่ตระหนักถึงไพรเวซีสำหรับคลังสารสนเทศกลางมีวัตถุประสงค์เพื่อให้คลังสารสนเทศกลางได้กำหนดนโยบายการใช้งานที่ตระหนักถึงไพรเวซีเพื่อให้เกิดการใช้งานข้อมูลที่อยู่ในคลังสารสนเทศกลางให้เป็นไปตามบทบาทที่ผู้ใช้งานได้รับ การสร้างนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซีจำเป็นต้องพิจารณาถึงวัตถุประสงค์ขององค์กร นโยบายการใช้งานเบื้องต้น พ.ร.บ.คอมพิวเตอร์ ลักษณะข้อมูลที่จัดเก็บ ความต้องการในการใช้งาน และแนวปฏิบัติของพีบีดีพีไอเอที่เหมาะสมกับนโยบายขององค์กร ในงานวิจัยนี้ได้นำเลือกแนวปฏิบัติพีบีดีพีไอเอที่เหมาะสมนำมาประยุกต์ 65 แนวปฏิบัติจากทั้งหมด 123 แนวปฏิบัติคิดเป็นร้อยละ 52.84 และแนวปฏิบัติที่ไม่ได้นำมาประยุกต์ 58 แนวปฏิบัติคิดเป็นร้อยละ 47.15 เนื่องจากไม่สอดคล้องกับวัตถุประสงค์ของคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

2.) การวิเคราะห์และออกแบบพัฒนาเครื่องมือสนับสนุนคลังสารสนเทศกลาง หลังจากที่ได้คลังสารสนเทศกลางมีนโยบายการใช้งานที่ตระหนักถึงไพรเวซีแล้ว นโยบายดังกล่าวจะเป็นส่วนหนึ่งของข้อมูลนำเข้าเพื่อวิเคราะห์รายการความต้องการ ออกแบบและพัฒนาเครื่องมือสนับสนุนเพื่อใช้ในการสกัดนโยบายและมอบหมายสิทธิบทบาทให้ผู้ใช้งานในคลังสารสนเทศกลางตามนโยบายการใช้งานคลังสารสนเทศกลางที่กำหนด

3.) การสกัดเอนทิตีและจัดเก็บข้อมูลนโยบาย ในขั้นตอนนี้จะเป็นการสกัดนโยบายการใช้งาน คลังสารสนเทศกลางที่ตระหนักถึงไพรเวซีผ่านเครื่องมือสนับสนุนที่ได้ออกแบบและพัฒนา การสกัดนโยบายใช้แนวทางการสกัดเอนทิตีจากงานวิจัย [11] โดยเอนทิตีที่สกัดจะถูกจัดเก็บไว้ในฐานข้อมูล เพื่อนำมาใช้ในการกำหนดสิทธิการให้กับผู้ใช้งานในคลังสารสนเทศกลาง

5.2 ข้อจำกัด

ข้อจำกัดของงานวิจัยมีดังต่อไปนี้ การเลือกแนวปฏิบัติพีดีพีไอเอขึ้นอยู่กับวัตถุประสงค์ของการนำไปใช้งานกับคลังข้อมูลในด้านต่างๆ ซึ่งในงานวิจัยนี้เลือกได้เลือกแนวปฏิบัติเพื่อให้เหมาะสมกับบริบทคลังสารสนเทศกลางซึ่งเป็นแหล่งจัดเก็บข้อมูลด้านทรัพยากรน้ำ แนวปฏิบัติพีดีพีไอเอที่ผ่านการวิเคราะห์เพื่อนำมาประยุกต์กับองค์กร บางส่วนของแนวปฏิบัติสามารถนำมาพัฒนาเป็นฟังก์ชันของเครื่องมือสนับสนุนได้ บางส่วนของแนวปฏิบัติไม่สามารถนำมาพัฒนาเป็นเครื่องมือสนับสนุนได้ ดังนั้นการดำเนินการในรูปแบบอื่นเช่น การออกแบบสอบถามและอัปโหลดเอกสารนั้นผ่านเครื่องมือสนับสนุน เครื่องมือสนับสนุนในงานวิจัยนี้พัฒนาเพื่อให้สอดคล้องกับนโยบายการใช้งานคลังสารสนเทศกลาง ดังนั้นองค์กรที่ต้องการนำเครื่องมือสนับสนุนไปใช้งานจะต้องมีการเพิ่มเติมหรือปรับแต่งองค์ประกอบของเครื่องมือเพื่อให้เกิดความเหมาะสมตามบริบทขององค์กร

5.3 งานวิจัยในอนาคต

แนวทางดำเนินการวิจัยในอนาคตคือ การนำนโยบายการใช้งานคลังสารสนเทศกลางที่ตระหนักถึงไพรเวซีและเครื่องมือสนับสนุนไปทดลองใช้ในสภาพแวดล้อมจริง เพื่อรับผลป้อนกลับจากการใช้งาน และนำมาปรับปรุงให้เหมาะสมเชิงคุณภาพ เช่น พิจารณาเรื่องความมั่นคงมากยิ่งขึ้น ประสิทธิภาพและประสิทธิผลของเครื่องมือสนับสนุน เป็นต้น เพื่อให้สอดคล้องกับสภาพแวดล้อมจริง

ทั้งนี้ในการสร้างนโยบายการใช้งานคลังสารสนเทศกลางนอกจากจะพิจารณาเรื่องไพรเวซีเป็นหลักแล้วยังต้องพิจารณาคุณภาพด้านอื่นร่วมด้วย เช่น ความมั่นคง สมรรถนะของเครื่องมือสนับสนุน เป็นต้น ตลอดจนการสร้างเกณฑ์ในการประเมินนโยบายการใช้งานและเครื่องมือสนับสนุน

5.4 ผลงานตีพิมพ์จากวิทยานิพนธ์

1) หัวเรื่อง “Privacy-aware Policy Establishment and Enforcement for Information Center Repository: A Case Study of Government Meteorological Information Center Repository” โดย ยศพนธ์ เลิศห้ำาเดชานนท์ และ นครทิพย์ พร้อมพูล ใน บัณฑิตการประชุม “The Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP2014) University of the Thai Chamber of Commerce (UTCC), Thailand, May 6-8, 2014 Proceedings” ซึ่งจัดขึ้น ณ มหาวิทยาลัยหอการค้า กรุงเทพมหานคร ประเทศไทย ระหว่างวันที่ 6-8 พฤษภาคม 2557



ภาคผนวก ก อภิธานศัพท์และรายการความต้องการของเครื่องมือสนับสนุน

สำหรับภาคผนวก ก ประกอบไปด้วยอภิธานศัพท์และรายการความต้องการของเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

ตารางที่ ก.1 อภิธานศัพท์

คำศัพท์	คำอธิบาย
Assignments	การกำหนดให้, การมอบหมาย (หน้าที่)
Authorization	การอนุญาต, การให้อำนาจ
Permission	การอนุญาต
Permission Assignments	การกำหนดมอบหมายอำนาจ
Privacy	ภาวะส่วนตัว
Privilege	เอกสิทธิ์

ตารางที่ ก.2 รายการความต้องการของเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงานกรณีศึกษา

หมายเลขความต้องการ	กลุ่มความสามารถ	รายการความต้องการ
FR1	การจัดการนโยบาย	เพิ่มนโยบายการใช้งาน
FR2		บันทึกนโยบายการใช้งาน
FR3		ค้นหานโยบายการใช้งาน
FR4		แก้ไขนโยบายการใช้งาน
FR5		ยกเลิก/ระงับนโยบายการใช้งาน

ตารางที่ ก.2 รายการความต้องการของเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงาน
กรณีศึกษา (ต่อ)

FR6		สกัดเอนทิตีนโยบายการใช้งาน
FR7		เพิ่มข้อมูลผู้รับผิดชอบนโยบายการใช้งาน
FR8		บันทึกข้อมูลผู้รับผิดชอบนโยบายการใช้งาน
FR9		แก้ไขข้อมูลผู้รับผิดชอบนโยบายการใช้งาน
FR10	การกำหนดค่าพื้นฐานการใ้ งานข้อมูล	เพิ่มรายการไพรเวซีข้อมูลเริ่มต้น
FR11		เรียกดูข้อมูลในคลังสารสนเทศกลาง
FR12		บันทึกรายการไพรเวซีข้อมูลเริ่มต้น
FR13		แก้ไขรายการไพรเวซีข้อมูลเริ่มต้น
FR14		กำหนดรายการไพรเวซีข้อมูลเริ่มต้น
FR15		ลบรายการไพรเวซีข้อมูลเริ่มต้น
FR16	ข้อมูลเข้าใช้งานระบบ	บันทึกการเข้าใช้งานระบบ
FR17		ค้นหาการเข้าใช้งานระบบ
FR18		ออกรายงานการเข้าใช้งานระบบ
FR19	การระบุตัวตน	บันทึกการลงทะเบียนเพื่อใช้งาน
FR20		ตรวจสอบการเข้าสู่ระบบ
FR21		แก้ไขข้อมูลส่วนตัวผู้ใช้งาน
FR22		กู้รหัสผ่านผู้ใช้งาน
FR23	การแนะนำรหัสผ่าน	แสดงตัวอย่างรหัสผ่านให้ผู้ใช้งาน
FR24		แสดงคำแนะนำในการสร้างรหัสผ่าน
FR25	การอบรมด้านไพรเวซี	เพิ่มหลักสูตรการอบรม
FR26		บันทึกหลักสูตรการอบรม

ตารางที่ ก.2 รายการความต้องการของเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงาน
กรณีศึกษา (ต่อ)

หมายเลขความ ต้องการ	กลุ่มความสามารถ	รายการความต้องการ
FR27	การอบรมด้านโปรแกรม	แก้ไขหลักสูตรการอบรม
FR28		ลบหลักสูตรการอบรม
FR29	การอบรมด้านโปรแกรม	กำหนดกลุ่มเป้าหมายหลักสูตรอบรม
FR30		บันทึกการเข้ารับหลักสูตรอบรม
FR31		ออกรายงานหลักสูตรอบรม
FR32	การเปิดเผยข้อมูล	บันทึกคำร้องขอใช้ข้อมูล
FR33		ตรวจสอบสถานะการพิจารณาเรื่องขอใช้ ข้อมูล
FR34		แสดงรายการคำร้องขอใช้ข้อมูล
FR35		ค้นหาคำร้องขอใช้ข้อมูล
FR36		แสดงรายงานคำขอใช้ข้อมูลที่ผ่านการ พิจารณา
FR37	การส่งต่อข้อมูล	บันทึกคำร้องขอส่งต่อข้อมูล
FR38		อนุมัติคำร้องขอส่งต่อข้อมูล
FR39		ตรวจสอบสถานะคำร้องขอส่งต่อข้อมูล
FR40		แสดงรายการคำร้องขอส่งต่อข้อมูล
FR41		ค้นหาคำร้องขอส่งต่อข้อมูล
FR42		แสดงรายการคำร้องที่ผ่านการพิจารณาส่งต่อ ข้อมูล

ตารางที่ ก.2 รายการความต้องการของเครื่องมือสนับสนุนคลังสารสนเทศกลางของหน่วยงาน
กรณีศึกษา (ต่อ)

หมายเลขความ ต้องการ	กลุ่มความสามารถ	รายการความต้องการ
FR43	การควบคุมสิทธิและ บทบาท	เพิ่มสิทธิและบทบาท
FR44		บันทึกสิทธิและบทบาท
FR45		แก้ไขสิทธิและบทบาท
FR46	การควบคุมสิทธิและ บทบาท	ลบสิทธิและบทบาท
FR47		บันทึกการมอบหมายสิทธิและบทบาท
FR48		แก้ไขการมอบหมายสิทธิและบทบาท
FR49		ตรวจสอบสิทธิและบทบาท
FR50	การเก็บรักษาและทำลาย	เพิ่มรายการเก็บรักษาและทำลายข้อมูล
FR51		บันทึกรายการเก็บรักษาและทำลายข้อมูล
FR52		แก้ไขรายการเก็บรักษาและทำลายข้อมูล
FR53		ลบรายการเก็บรักษาและทำลายข้อมูล
FR54		แสดงรายการการเก็บรักษาและทำลายข้อมูล

ภาคผนวก ข คำอธิบายตารางแบบจำลองข้อมูล

ตารางที่ ข.1 โครงสร้างตารางข้อมูล tbl_user_training

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>usertrain_id</u>	Integer	รหัสการอบรม	PK
user_id	Integer	รหัสผู้ใช้งานที่เข้าอบรม	FK
training_id	Integer	รหัสหลักสูตรการอบรม	FK
Attend	Boolean	เข้าร่วมการอบรม	
comment	text	บันทึก	

ตารางที่ ข.2 โครงสร้างตารางข้อมูล tbl_logs

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>log_id</u>	Integer	รหัสบันทึกการใช้งาน	PK
Ip	Character varying	หมายเลขไอพีของผู้ใช้งาน	
Host	Character varying	ชื่อโฮสของผู้ใช้งาน	
Datetime	Datetime	วันที่เวลาที่เข้าใช้งาน	
Userid	Integer	รหัสผู้ใช้งาน	FK
Lastpage	Character varying	ยูอาร์แอลสุดท้ายที่เข้าใช้งาน	
last_visit	Datetime	วันเวลาครั้งล่าสุดที่เข้าใช้งานระบบ	

ตารางที่ ข.3 โครงสร้างตารางข้อมูล tbl_privacy

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>privacy_id</u>	Integer	รหัสไพลเวซี	PK
user_id	Integer	รหัสผู้ใช้งาน	FK
Email	Boolean	อนุญาตให้เห็นข้อมูลอีเมล	
Fname	Boolean	อนุญาตให้เห็นชื่อ	
Lname	Boolean	อนุญาตให้เห็นนามสกุล	
Telno	Boolean	อนุญาตให้เห็นเบอร์โทรศัพท์	
Agency	Boolean	อนุญาตให้เห็นชื่อหน่วยงาน	
department	Boolean	อนุญาตให้เห็นชื่อสังกัดหน่วยงาน	
Ministry	Boolean	อนุญาตให้เห็นข้อมูลชื่อกระทรวง	
Role	Boolean	อนุญาตให้เห็นข้อมูลชื่อบทบาท	
Action	Boolean	อนุญาตให้เห็นข้อมูลการกระทำ	
created_date	Datetime	วันที่สร้างไพลเวซี	
created_by	Integer	รหัสผู้สร้างไพลเวซี	FK
updated_date	Datetime	วันที่ปรับปรุงข้อมูลไพลเวซี	
updated_by	Integer	รหัสผู้ทำการปรับปรุงไพลเวซี	FK

ตารางที่ ข.4 โครงสร้างตารางข้อมูล tbl_role_user

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>id</u>	Integer	รหัสไพลเวซี	PK
role_id	Integer	รหัสบทบาท	FK
user_id	Integer	รหัสผู้ใช้งาน	FK

ตารางที่ ข.5 โครงสร้างตารางข้อมูล tbl_training

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
training_id	Integer	รหัสหลักสูตรการอบรม	PK
Title	Character varying	ชื่อหลักสูตรอบรม	FK
description	Text	รายละเอียดการอบรม	
Target	Character varying	รหัสบทบาท	
Status	Boolean	สถานะของหลักสูตรการอบรม	
created_date	Datetime	วันที่สร้าง	
created_by	Integer	รหัสผู้สร้าง	FK
updated_date	Datetime	วันที่ปรับปรุงข้อมูล	
updated_by	Integer	รหัสผู้ทำการปรับปรุง	FK

ตารางที่ ข.6 โครงสร้างตารางข้อมูล tbl_usergroup

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
grp_id	Integer	รหัสไพรเวซี	PK
grp_name	Character varying	รหัสผู้ใช้งาน	
grp_nameth	Character varying	อนุญาตให้เห็นข้อมูลอีเมล	
grp_desc	Character varying	อนุญาตให้เห็นชื่อ	
created_date	Datetime	วันที่สร้าง	
updated_date	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.7 โครงสร้างตารางข้อมูล tbl_user

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
user_id	Integer	รหัสผู้ใช้งาน	PK
agency_id	Integer	รหัสหน่วยงาน	FK
username	Character varying	ชื่อผู้ใช้งาน	
password	Character varying	รหัสผ่านของผู้ใช้งาน	
Fname	Character varying	ชื่อจริงของผู้ใช้งาน	
Lname	Character varying	นามสกุลของผู้ใช้งาน	
Email	Character varying	อีเมลของผู้ใช้งาน	
Telno	Character varying	เบอร์ที่ใช้ในการติดต่อของผู้ใช้งาน	
Status	Boolean	สถานะของผู้ใช้งาน	
created_date	Datetime	วันที่สร้าง	
created_by	Integer	รหัสผู้สร้าง	FK
updated_date	Datetime	วันที่ปรับปรุงข้อมูล	
updated_by	Integer	รหัสผู้ทำการปรับปรุง	FK

ตารางที่ ข.8 โครงสร้างตารางข้อมูล tbl_agency

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>agency_id</u>	Integer	รหัสหน่วยงาน	PK
minstry_id	Integer	รหัสกระทรวง	FK
agency_code	Integer	โค้ดหน่วยงาน	
Tname	Character varying	ชื่อหน่วยงานภาษาไทย	
Abbr	Character varying	ชื่อย่อหน่วยงาน	
Status	Boolean	สถานะของหน่วยงาน	
created_date	Datetime	วันที่สร้าง	
created_by	Integer	รหัสผู้สร้าง	FK
updated_date	Datetime	วันที่ปรับปรุงข้อมูล	
updated_by	Integer	รหัสผู้ทำการปรับปรุง	FK

ตารางที่ ข.9 โครงสร้างตารางข้อมูล tbl_retain

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>retain_id</u>	Integer	รหัสไพลเวซี	PK
freqdata_id	Integer	รหัสผู้ใช้งาน	FK
created_at	Boolean	วันที่สร้าง	
updated_at	Boolean	วันที่อัปเดต	

ตารางที่ ข.10 โครงสร้างตารางข้อมูล tbl_schedule

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>schd_id</u>	Integer	รหัสรายการ	PK
disp_id	Integer	รหัสการทำลายข้อมูล	FK
retain_id	Boolean	รหัสการเก็บรักษาข้อมูล	FK
Status	Boolean	สถานะ	
created_date	Boolean	วันที่สร้าง	
updated_date	Boolean	วันที่ปรับปรุง	

ตารางที่ ข.11 โครงสร้างตารางข้อมูล tbl_dispose

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>disp_id</u>	Integer	รหัสการทำลายข้อมูล	PK
retain_id	Boolean	รหัสการเก็บรักษาข้อมูล	
Status	Boolean	สถานะ	
created_date	Boolean	วันที่สร้าง	
updated_date	Boolean	วันที่ปรับปรุง	

ตารางที่ ข.12 โครงสร้างตารางข้อมูล tbl_department

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>dep_id</u>	Integer	รหัสทบวงกรม	PK
Tname	Integer	ชื่อทบวงกรมภาษาไทย	
Ename	Boolean	ชื่อทบวงกรมภาษาอังกฤษ	
dep_code	Boolean	รหัสทบวงกรม	
ministry_id	Boolean	รหัสกระทรวง	
created_date	Datetime	วันที่สร้าง	
updated_date	Datetime	วันที่ปรับปรุงข้อมูล	

ตารางที่ ข.13 โครงสร้างตารางข้อมูล tbl_transfer

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>transf_id</u>	Boolean	รหัสการส่งข้อมูล	PK
freqdata_id	Boolean	รหัสความถี่ของข้อมูล	
Status	Boolean	สถานะ	
created_date	Datetime	วันที่สร้างโปรแกรม	
updated_date	Datetime	วันที่ปรับปรุงข้อมูล	

ตารางที่ ข.14 โครงสร้างตารางข้อมูล tbl_role

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
role_id	Integer	รหัสไพรเวซี	PK
role_name	Character varying	ชื่อบทบาท	
created_date	Datetime	วันที่สร้าง	
updated_date	Datetime	วันที่ปรับปรุงข้อมูล	

ตารางที่ ข.15 โครงสร้างตารางข้อมูล tbl_role_policy

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
rp_id	Integer	รหัสไพรเวซี	PK
role_id	Integer	รหัสบทบาท	FK
policy_id	Integer	รหัสนโยบาย	FK

ตารางที่ ข.16 โครงสร้างตารางข้อมูล tbl_policy

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
policy_id	Integer	รหัสไพรเวซี	PK
policy_content	Text	รหัสบทบาท	FK
Author	Character varying	รหัสนโยบาย	FK
Status	Boolean	สถานะ	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.17 โครงสร้างตารางข้อมูล tbl_rbac_policy

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>rbac_id</u>	Integer	รหัสหลัก	PK
cond_id	Integer	รหัสเงื่อนไข	
policy_id	Integer	รหัสนโยบาย	
action_id	Integer	รหัสการกระทำ	
obl_id	Integer	รหัสเงื่อนไขที่ต้องทำก่อน	
purp_id	Integer	รหัสวัตถุประสงค์	
data_id	Integer	รหัสข้อมูล	

ตารางที่ ข.18 โครงสร้างตารางข้อมูล tbl_purpose

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>purpose_id</u>	Integer	รหัสวัตถุประสงค์	PK
purpose_name	Character varying	ชื่อวัตถุประสงค์	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.19 โครงสร้างตารางข้อมูล tbl_data

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>data_id</u>	Integer	รหัสข้อมูล	PK
data_name	Character varying	ชื่อข้อมูล	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.20 โครงสร้างตารางข้อมูล tbl_frequencydata

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>freqdata_id</u>	Integer	รหัสหลัก	PK
data_id	Integer	รหัสข้อมูล	FK
freq_id	Integer	รหัสความถี่ข้อมูล	FK

ตารางที่ ข.21 โครงสร้างตารางข้อมูล tbl_action

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>action_id</u>	Integer	รหัสการกระทำ	PK
action_name	Character varying	ชื่อการกระทำภาษาไทย	
Action	Character varying	ชื่อการกระทำภาษาอังกฤษ	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.22 โครงสร้างตารางข้อมูล tbl_ministry

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
<u>Id</u>	Integer	รหัสหลัก	PK
ministry_id	Integer	เลขรหัสของกระทรวง	
Fullname	Character varying	ชื่อกระทรวงแบบเต็ม	
shortname	Character varying	ชื่อกระทรวงแบบย่อ	
Code	Character varying	โค้ดของกระทรวง	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.23 โครงสร้างตารางข้อมูล tbl_disclose

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
Id	Integer	รหัสหลัก	PK
freqdata_id	Integer	รหัสความถี่ข้อมูล	FK
Status	Boolean	สถานะ	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.24 โครงสร้างตารางข้อมูล tbl_frequency

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
Id	Integer	รหัสหลัก	PK
src_id	Integer	รหัสชื่อตารางข้อมูล	FK
fld_id	Integer	รหัสฟิลด์	FK
freq_name	Character varying	ชื่อความถี่ข้อมูล	
comment	Text	บันทึก/หมายเหตุ	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.25 โครงสร้างตารางข้อมูล tbl_condition

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
Id	Integer	รหัสหลัก	PK
cond_name	Integer	ชื่อเงื่อนไขภาษาไทย	
condition	Integer	ชื่อเงื่อนไขภาษาอังกฤษ	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.26 โครงสร้างตารางข้อมูล tbl_src_table

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
Id	Integer	รหัสหลัก	PK
src_name	Character varying	ชื่อตารางข้อมูล	
comment	Text	บันทึก/หมายเหตุ	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.27 โครงสร้างตารางข้อมูล tbl_src_field

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
ld	Integer	รหัสหลัก	PK
fld_name	Character varying	ชื่อฟิลด์	
fld_where	Character varying	เงื่อนไขการดึงข้อมูล	
fld_ord	Character varying	การเรียงลำดับข้อมูล	
fld_limit	Character varying	จำนวนแถวที่ต้องการดึง	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ตารางที่ ข.28 โครงสร้างตารางข้อมูล tbl_obligation

ชื่อคุณลักษณะ	ชนิด	คำอธิบาย	คีย์
ld	Integer	รหัสหลัก	PK
obl_name	Character varying	ชื่อข้อผูกพัน	
created_at	Datetime	วันที่สร้าง	
updated_at	Datetime	วันที่ปรับปรุง	

ภาคผนวก ค ส่วนต่อประสานของเครื่องมือสนับสนุน

สำหรับภาคผนวก จะกล่าวถึงส่วนต่อประสานและฟังก์ชันงานของเครื่องมือสนับสนุน โดยประกอบด้วย 2 ส่วนคือ ส่วนต่อประสานเครื่องมือสนับสนุนหลังบ้านสำหรับเจ้าหน้าที่คลังสารสนเทศกลาง ส่วนต่อประสานสำหรับผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลางดังนี้

ค.1 ส่วนต่อประสานเครื่องมือสนับสนุนหลังบ้านสำหรับเจ้าหน้าที่คลังสารสนเทศกลาง

ตารางที่ ค.1 ฟังก์ชันการใช้งานส่วนการจัดการหลังบ้านของเจ้าหน้าที่คลังสารสนเทศกลาง

ฟังก์ชันงาน/เมนู	คำอธิบาย
1) ค้นหา <ul style="list-style-type: none"> - ค้นหาตามบทบาท - ค้นหาตามชื่อข้อมูล - ค้นหาตามชื่อหน่วยงาน 	ค้นหาผู้ใช้งานตามบทบาทที่ได้รับ ค้นหาหน่วยงานตามชื่อข้อมูล ค้นหาชื่อข้อมูลตามหน่วยงานที่อยู่ในคลังสารสนเทศกลาง
2) นโยบายคลังฯ	เมนูสำหรับแสดงนโยบายการใช้งานคลังสารสนเทศกลาง
3) พ็อรัลบีเอซี <ul style="list-style-type: none"> - บทบาท - ข้อมูล - การกระทำ - วัตถุประสงค์ - เงื่อนไข - ข้อผูกพัน 	เมนูสำหรับเพิ่มชื่อบทบาทในระบบ เมนูสำหรับเพิ่มชื่อข้อมูลในระบบ เมนูสำหรับเพิ่มชื่อการกระทำในระบบ เมนูสำหรับเพิ่มชื่อวัตถุประสงค์ในระบบ เมนูสำหรับเพิ่มชื่อเงื่อนไขในระบบ เมนูสำหรับเพิ่มชื่อข้อผูกพันในระบบ
4) ผู้ใช้งานและหน่วยงาน <ul style="list-style-type: none"> - ผู้ใช้งานในระบบ - ผู้รับผิดชอบนโยบาย - หน่วยงาน 	แสดงรายชื่อผู้ใช้งานในระบบทั้งหมด แสดงรายชื่อผู้รับผิดชอบนโยบายทั้งหมด แสดงรายชื่อหน่วยงานทั้งหมด
5) สถิติและรายงาน <ul style="list-style-type: none"> - สถิติ - รายงาน 	เมนูแสดงสถิติการใช้งานระบบ เมนูสำหรับแสดงรายงานการใช้งานระบบโดยระบุตามบทบาท

ตารางที่ ค.1 ฟังก์ชันการใช้งานส่วนการจัดการหลังบ้านของเจ้าหน้าที่คลังสารสนเทศกลาง(ต่อ)

<p>6) หลักสูตรอบรม</p> <ul style="list-style-type: none"> - หลักสูตรอบรม - ออกรายงานรายบุคคล - ออกรายงานตามบทบาท - ออกรายงานตามช่วงเวลา - ออกรายงานตามชื่อหลักสูตร 	<p>เมนูบริหารจัดการหลักสูตรการอบรม เจ้าหน้าที่คลังสารสนเทศจะ เป็นผู้ นำเข้าข้อมูลหลักสูตรเพื่อแจ้งให้กับผู้ใช้งานตาม กลุ่มเป้าหมายที่กำหนด และเจ้าหน้าที่คลังสารสนเทศกลาง สามารถออกรายงานตามประเภทที่ต้องการได้</p>
<p>7) การตั้งค่า</p> <ul style="list-style-type: none"> - ตั้งค่าโปรเวซี - ตั้งค่าความมั่นคง - ข้อมูลบัญชี - พีบีดีพีไอเอ - การใช้งานระบบ - ฟังก์ชันใช้งานในระบบ 	<p>เมนูสำหรับปรับแต่โปรเวซีของผู้ใช้งาน เมนูสำหรับเปลี่ยนแปลงด้านความมั่นคง เมนูสำหรับแสดงข้อมูลส่วนตัวของผู้ใช้งาน แสดงตารางพีบีดีพีไอเอและคำถาม เหตุผลที่เลือกใช้ เอกสารแนะนำการใช้งานระบบ เอกสารแนะนำฟังก์ชันการใช้งานของแต่ละบทบาท</p>
<p>8) ออกจากระบบ</p>	<p>เมนูสำหรับออกจากระบบ</p>

จากตารางที่ ค.1 แสดงเมนูเครื่องมือสนับสนุน ละเอียดของส่วนต่อประสานเครื่องมือสนับสนุนหลังบ้านมีดังต่อไปนี้

1.) เมนูค้นหา เมื่อเจ้าหน้าที่คลังสารสนเทศกลางเข้าสู่ระบบ สำหรับการค้นหาแบ่งออกเป็น 3 ประเภทคือ

- การค้นหาตามบทบาท ดังปรากฏในรูปที่ ค.1 เป็นการค้นหาผู้ใช้งานในระบบโดยใช้บทบาทที่ผู้ใช้งานได้รับเป็นคำค้นในการค้นหา
- การค้นหาตามชื่อข้อมูล ดังปรากฏรูปที่ ค.2 เป็นการค้นหาหน่วยงานที่อยู่ในคลังสารสนเทศกลางโดยใช้ข้อมูลเป็นคำค้นในการค้นหา
- การค้นหาตามหน่วยงาน ดังปรากฏรูปที่ ค.3 เป็นการค้นหาข้อมูลตามหน่วยงานที่อยู่ในคลังสารสนเทศกลาง

NHC ค้นหา นโยบายคลังฯ ทิศทางบีเอสซี- ผู้ใช้งานและหน่วยงาน- สถิติและรายงาน- หลักสูตรอบรม- เอกสาร superadmin (กลุ่ม: SUPER ADMIN)

หน้าหลัก / ค้นหา / ค้นหาตามบทบาท

แผงรายการบทบาท

นักวิจัย ค้นหา

ลำดับ	ชื่อผู้ใช้งาน
1	user6
2	user5
3	user3

รูปที่ ค.1 การค้นหาตามบทบาท

NHC ค้นหา นโยบายคลังฯ ทิศทางบีเอสซี- ผู้ใช้งานและหน่วยงาน- สถิติและรายงาน- หลักสูตรอบรม- เอกสาร superadmin (กลุ่ม: SUPER ADMIN)

หน้าหลัก / ค้นหา / ค้นหาตามชื่อข้อมูล

แผงรายการข้อมูล

ปริมาณน้ำฝนราย 24 ชั่วโมง ค้นหา

รหัส	หน่วยงาน	ติดต่อ
1	หน่วยงานที่ 11	user4
2	หน่วยงานที่ 4	user3
3	หน่วยงานที่ 4	user2
4	หน่วยงานที่ 7	user1

รูปที่ ค.2 การค้นหาตามข้อมูล

NHC ค้นหา นโยบายคลังฯ ทิศารบีเอสอี-1 ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักสูตรอบรม superadmin (กลุ่ม: SUPER ADMIN) การตั้งค่า

หน้าหลัก / ค้นหา / ค้นหาตามหน่วยงาน

แผนรายการหน่วยงาน

กรมชลประทาน ค้นหา

ลำดับ	ชื่อข้อมูล	สถานะข้อมูล	วันสุดท้ายที่เก็บข้อมูล
1	ปริมาณน้ำฝนราย 24 ชั่วโมง	ไม่อนุญาตให้ร้องขอ	2015-07-15
2	ปริมาณน้ำฝนวันนี้	ไม่อนุญาตให้ร้องขอ	2015-07-08
3	ปริมาณน้ำฝนวานนี้	ไม่อนุญาตให้ร้องขอ	2015-07-08
4	ปริมาณน้ำฝนย้อนหลัง	ไม่อนุญาตให้ร้องขอ	2015-07-08
5	ข้อมูลระดับน้ำ	ไม่อนุญาตให้ร้องขอ	2017-07-08
6	ข้อมูลน้ำในเขื่อน	ไม่อนุญาตให้ร้องขอ	2017-07-08
7	ข้อมูลความเข้มแสง	ไม่อนุญาตให้ร้องขอ	2017-07-08
8	ข้อมูลความชื้น	ไม่อนุญาตให้ร้องขอ	2017-07-08
9	ข้อมูลความกดอากาศ	ไม่อนุญาตให้ร้องขอ	2021-07-08
10	ข้อมูลอุณหภูมิ	ไม่อนุญาตให้ร้องขอ	2019-07-08
11	ข้อมูลระดับน้ำทะเล	ไม่อนุญาตให้ร้องขอ	2024-07-08

รูปที่ ค.3 แสดงการค้นหาตามหน่วยงาน

2.) เมื่อนโยบายคลังสารสนเทศกลาง ดังปรากฏในรูปที่ ค.4 ซึ่งจะแสดงรายการนโยบายการใช้งานคลังสารสนเทศกลางทั้งหมดที่มีอยู่ในระบบ โดยเจ้าหน้าที่คลังสารสนเทศสามารถทำการเพิ่ม ลบ แก้ไข นโยบายการใช้งานดังกล่าวได้

NHC ค้นหา **นโยบายคลัง** **พีอาร์บีเอซี** **ผู้ใช้งานและหน่วยงาน** **สถิติและรายงาน** **หลักสูตรอบรม** **เอกสาร** **superadmin (กลุ่ม: SUPER ADMIN)**

หน้าหลัก / นโยบายคลัง

แผนนโยบาย

ค้นหา นโยบาย ค้นหา เพิ่ม

ลำดับ	เนื้อหาของนโยบาย	ผู้สร้าง	ผู้รับผิดชอบ	สถานะ	
1	นักวิจัยได้รับอนุญาตให้เรียกดูข้อมูล ปริมาณน้ำฝน โดยจะต้องเข้าสู่ระบบก่อนที่จะเรียกดูข้อมูลตามความถี่ของข้อมูลดังนี้ 1. ข้อมูลปริมาณน้ำฝนราย 24 ชั่วโมง 2. ข้อมูลปริมาณน้ำฝนวันนี้ 3. ข้อมูลปริมาณน้ำฝนวานนี้ 4. ข้อมูลปริมาณน้ำฝนย้อนหลัง 3 วัน 5. ข้อมูลปริมาณน้ำฝนย้อนหลัง 7 วัน โดยมีวัตถุประสงค์เพื่องานวิจัยข้อมูลเท่านั้น และเมื่อต้องการความถี่ของข้อมูลจะต้องได้รับความยินยอมจากเจ้าหน้าที่คลังข้อมูลแห่งชาติก่อนหลังจากออกจากระบบ ระบบจะทำการบันทึกประวัติการเรียกดูข้อมูลดังกล่าว	ผู้สร้างนโยบายทดสอบ	user1	เปิดใช้งาน	ปิดพีอาร์บีเอซี แก้ไข ปิดพีอาร์บีเอซี ลบ
2	นักวิจัยสามารถเรียกดูข้อมูลเมื่อเข้าสู่ระบบก่อนและเรียกดูข้อมูลระดับน้ำ ข้อมูลเขื่อน ความเข้มแสง ความชื้น ความกดอากาศ อุณหภูมิ ระดับน้ำทะเล ตามความถี่ของข้อมูลต่อไปนี้ 1. ข้อมูลปัจจุบัน 2. ข้อมูลราย 3 วัน 3. ข้อมูลราย 7 วัน โดยมีวัตถุประสงค์เพื่องานวิจัยข้อมูลเท่านั้น และเมื่อต้องการความถี่ของข้อมูลจะต้องได้รับความยินยอมจากเจ้าหน้าที่คลังข้อมูลแห่งชาติก่อน หลังจากออกจากระบบ ระบบจะทำการบันทึกประวัติการเรียกดูข้อมูลดังกล่าว	ผู้สร้างนโยบายทดสอบ	user1	เปิดใช้งาน	ปิดพีอาร์บีเอซี แก้ไข ปิดพีอาร์บีเอซี ลบ
3	นักพัฒนาระบบสามารถเรียกดูข้อมูลเมื่อเข้าสู่ระบบก่อนและแจ้งกลับไปยังเจ้าหน้าที่คลังข้อมูลคลังข้อมูลแห่งชาติ ในการนี้ข้อมูลไม่ถูกต้อง โดยสามารถเรียกดูข้อมูลปริมาณน้ำฝนได้ดังนี้ 1. ข้อมูลปริมาณน้ำฝนราย 24 ชั่วโมง 2. ข้อมูลปริมาณน้ำฝนวันนี้ 3. ข้อมูลปริมาณน้ำฝนวานนี้ 4. ข้อมูลปริมาณน้ำฝนย้อนหลัง 3 วัน 5. ข้อมูลปริมาณน้ำฝนย้อนหลัง 7 วัน โดยมีวัตถุประสงค์เพื่อการพัฒนาระบบเท่านั้น หลังจากออกจากระบบ ระบบจะทำการบันทึกประวัติการเรียกดูข้อมูลดังกล่าว	ผู้สร้างนโยบายทดสอบ	user1	เปิดใช้งาน	ปิดพีอาร์บีเอซี แก้ไข ปิดพีอาร์บีเอซี ลบ

« 1 2 3 4 »

รูปที่ ค.4 หน้านโยบายคลังสารสนเทศกลาง

การสกัดเอนทิตีนโยบายการใช้งาน เจ้าหน้าที่คลังสารสนเทศกลางสามารถทำได้โดยกดปุ่มพีอาร์บีเอซี ซึ่งปรากฏอยู่ในแต่ละรายการนโยบายการใช้งาน ระบบจะนำเจ้าหน้าที่คลังสารสนเทศกลางมายังหน้าสกัดเอนทิตีนโยบายการใช้งานดังปรากฏในรูปที่ ค.5 ซึ่งเจ้าหน้าที่คลังสารสนเทศกลางสามารถระบุได้ว่านโยบายการใช้งานที่กำลังดำเนินการสกัดเอนทิตี นั้นมีเอนทิตีอะไรบ้าง เมื่อทำการสกัดเอนทิตีเสร็จเจ้าหน้าที่คลังสารสนเทศกลางกดปุ่มบันทึกเพื่อเก็บไว้ในฐานข้อมูล

NHC ค้นหา นโยบายคลังฯ พีอาร์บีเอซี ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักศูรอบรม superadmin (กลุ่ม: SUPER ADMIN) การตั้งค่า

หน้าหลัก / นโยบายคลังฯ / แปลงนโยบายตามหลักอาร์บีเอซี / นโยบายคลังฯที่: 1

แผนอาร์บีเอซี/นโยบายคลังฯ

นักวิจัยได้รับอนุญาตให้เรียกดูข้อมูล ปริมาณน้ำฝน โดยจะต้องเข้าสู่ระบบก่อนที่จะเรียกดูข้อมูลตามความถี่ของข้อมูลดังนี้

- 1.ข้อมูลปริมาณน้ำฝนราย 24 ชั่วโมง
- 2.ข้อมูลปริมาณน้ำฝนวันนี้
- 3.ข้อมูลปริมาณน้ำฝนวานนี้
- 4.ข้อมูลปริมาณน้ำฝนย้อนหลัง 3 วัน
- 5.ข้อมูลปริมาณน้ำฝนย้อนหลัง 7 วัน โดยมีวัตถุประสงค์เพื่องานวิจัยข้อมูลเท่านั้น และเมื่อต้องการดาวน์โหลดข้อมูลจะต้องได้รับความยินยอมจากเจ้าหน้าที่คลังข้อมูลแห่งชาติก่อนหลังจากออกจากระบบ ระบบจะทำการบันทึกประวัติการเรียกดูข้อมูลดังกล่าว

บทบาท	ข้อมูล	การกระทำ	วัตถุประสงค์	เงื่อนไข	ข้อมูลพื้นที่
นักวิจัย	ปริมาณน้ำฝนราย 24 ชั่วโมง	เรียกดูข้อมูล	เพื่องานวิจัย	ข้อมูลปัจจุบัน	เข้าสู่ระบบก่อน
	ปริมาณน้ำฝนวันนี้			ข้อมูลย้อนหลัง 3 วัน	บันทึกประวัติการใช้งานก่อนออกจากระบบ
	ปริมาณน้ำฝนวานนี้			ข้อมูลย้อนหลัง 7 วัน	

บทบาท:

ข้อมูล: นักวิจัย นักพัฒนาระบบ

การกระทำ: ผู้ดูแลฐานข้อมูล วิศวกรระบบ

วัตถุประสงค์: เจ้าหน้าที่ประจำหน่วยงาน เจ้าหน้าที่คลังข้อมูล

เงื่อนไข: บุคคลทั่วไป

ข้อมูลพื้นที่:

รูปที่ ค.5 ขั้นตอนการสกัดเอนทิตีนโยบายการใช้งาน

3.) เมนูพีอาร์บีเอซี ประกอบด้วยเมนูย่อยตามเอนทิตีในงานวิจัย [11] ซึ่งในแต่ละเอนทิตีจะถูกใช้ในการสกัดเอนทิตีของนโยบายการใช้งานโดยประกอบไปด้วย ชื่อบทบาท ชื่อการกระทำ ชื่อข้อมูล ชื่อเงื่อนไข ชื่อข้อมูลพื้นที่ หรือชื่อวัตถุประสงค์ ดังปรากฏในรูปที่ ค.6

รหัส	ชื่อบทบาท	แก้ไข	ลบทิ้ง
1	นักวิจัย	แก้ไข	ลบทิ้ง
2	นักพัฒนาระบบ	แก้ไข	ลบทิ้ง
3	ผู้ดูแลฐานข้อมูล	แก้ไข	ลบทิ้ง
4	เจ้าหน้าที่ประจำหน่วยงาน	แก้ไข	ลบทิ้ง
5	เจ้าหน้าที่คลังข้อมูล	แก้ไข	ลบทิ้ง
6	บุคคลทั่วไป	แก้ไข	ลบทิ้ง

รูปที่ ค.6 การจัดเตรียมบทบาทผู้ใช้งานในคลังสารสนเทศกลาง

4.) เมนูผู้ใช้งานและหน่วยงานประกอบด้วยเมนูย่อยคือ

- ผู้ใช้งานในระบบ เป็นส่วนสำหรับจัดการผู้ใช้งานในระบบ เจ้าหน้าที่คลังสารสนเทศกลางสามารถเปลี่ยนแปลงประเภทผู้ใช้งานหรือมอบหมายบทบาทให้กับผู้ใช้งาน ดังปรากฏในรูปที่ ค.7
- ผู้รับผิดชอบนโยบาย คือเมนูที่เจ้าหน้าที่คลังสารสนเทศกลางใช้สำหรับจัดการผู้รับผิดชอบนโยบายโดยสามารถเพิ่ม แก้ไข หรือปิดการใช้งานผู้รับผิดชอบนโยบาย ดังปรากฏในรูปที่ ค.8
- หน่วยงาน คือเมนูที่ใช้สำหรับแสดงรายชื่อหน่วยงานทั้งหมดที่อยู่ในคลังสารสนเทศกลาง โดยเจ้าหน้าที่คลังสารสนเทศกลางสามารถเพิ่ม/ลบ หน่วยงานได้ดังปรากฏในรูปที่ ค.9

NHC ค้นหา นโยบายคลัง ทิวารีบีเอสอี ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักสูตรอบรม เอกสาร superadmin (กลุ่ม: SUPER ADMIN)

หน้าหลัก / รายการผู้ใช้งาน / ผู้ใช้งานในระบบ

แผงผู้ใช้งานในระบบ

10 แถวต่อหน้า ค้นหา :

รหัส	ชื่อผู้ใช้	นามสกุล	บทบาท	วันที่ลงทะเบียน	ประเภทผู้ใช้	สถานะ	
1	user1	User1_test	นักวิจัย	2014-06-10	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
2	user2	User2	เจ้าหน้าที่ประจำหน่วยงาน	2014-06-10	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
3	user3	User3	นักวิจัย	2014-06-10	ทั่วไป	เปิดใช้งาน	แก้ไข
4	user4	User4	ผู้ดูแลฐานข้อมูล	2014-06-10	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
5	user5	user5	นักวิจัย	2014-10-13	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
6	user6	user6	นักวิจัย	2014-10-13	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข
7	user7	user7	นักพัฒนาระบบ	2014-10-13	ผู้ดูแลระบบ	เปิดใช้งาน	แก้ไข

แสดง 1 ถึง 7 จากทั้งหมด 7 แถว

ถอยหลัง 1 1 หน้า

รูปที่ ค.7 รายการผู้ใช้งานในคลังสารสนเทศกลางทั้งหมด

NHC ค้นหา นโยบายคลัง ทิวารีบีเอสอี ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักสูตรอบรม เอกสาร superadmin (กลุ่ม: SUPER ADMIN)

รายการผู้ใช้งาน / ผู้รับผิดชอบนโยบาย / รายการผู้รับผิดชอบนโยบาย

แผงผู้ใช้งานในระบบ

10 แถวต่อหน้า ค้นหา :

เพิ่มผู้รับผิดชอบ

ลำดับ	ชื่อ	นามสกุล	ตำแหน่ง	เบอร์ติดต่อ	อีเมล	วันที่เพิ่ม	สถานะ	
1	user3	user3	หัวหน้ากลุ่มงานระบบคอมพิวเตอร์และระบบเครือข่าย	02 123 4567 ต่อ 003	user3@localhost	2014-07-08	ระงับใช้งาน	แก้ไข
2	user2	user2	หัวหน้ากลุ่มงานพัฒนาระบบงาน	02 123 4567 ต่อ 002	user2@localhost	2014-07-08	เปิดใช้งาน	แก้ไข
3	user1	user1	ผู้อำนวยการฝ่ายวิจัยและพัฒนา	02 123 4567 ต่อ 001	user1@localhost	2014-07-08	เปิดใช้งาน	แก้ไข

แสดง 1 ถึง 3 จากทั้งหมด 3 แถว

ถอยหลัง 1 1 หน้า

รูปที่ ค.8 รายชื่อผู้รับผิดชอบนโยบายในคลังสารสนเทศกลาง

NHC ค้นหา นโยบายคลังฯ ทิศวธิ์เอเชีย ใช้งานและหน่วยงาน สถิติและรายงาน สถิติสรุปรวม เอกสาร superadmin (กลุ่ม: SUPER ADMIN)

หน้าหลัก / หน่วยงาน / รายการหน่วยงาน

แผนรายการหน่วยงาน

เพิ่มหน่วยงาน

10 แถวต่อหน้า ค้นหา:

ลำดับ	รหัส	ชื่อหน่วยงาน	ชื่อย่อ	กระทรวง	
1	00006	หน่วยงานที่ 6	FFF	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
2	00002	หน่วยงานที่ 2	BBB	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
3	00008	หน่วยงานที่ 8	HHH	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
4	00009	หน่วยงานที่ 9	III	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
5	00012	หน่วยงานที่ 12	MMM	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
6	00001	หน่วยงานที่ 1	AAA	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
7	00003	หน่วยงานที่ 3	CCC	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
10	00005	หน่วยงานที่ 5	EEE	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
11	00011	หน่วยงานที่ 11	LLL	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง
12	00007	หน่วยงานที่ 7	GGG	แหล่งข้อมูลทดสอบ (ทดสอบ)	ลบทิ้ง

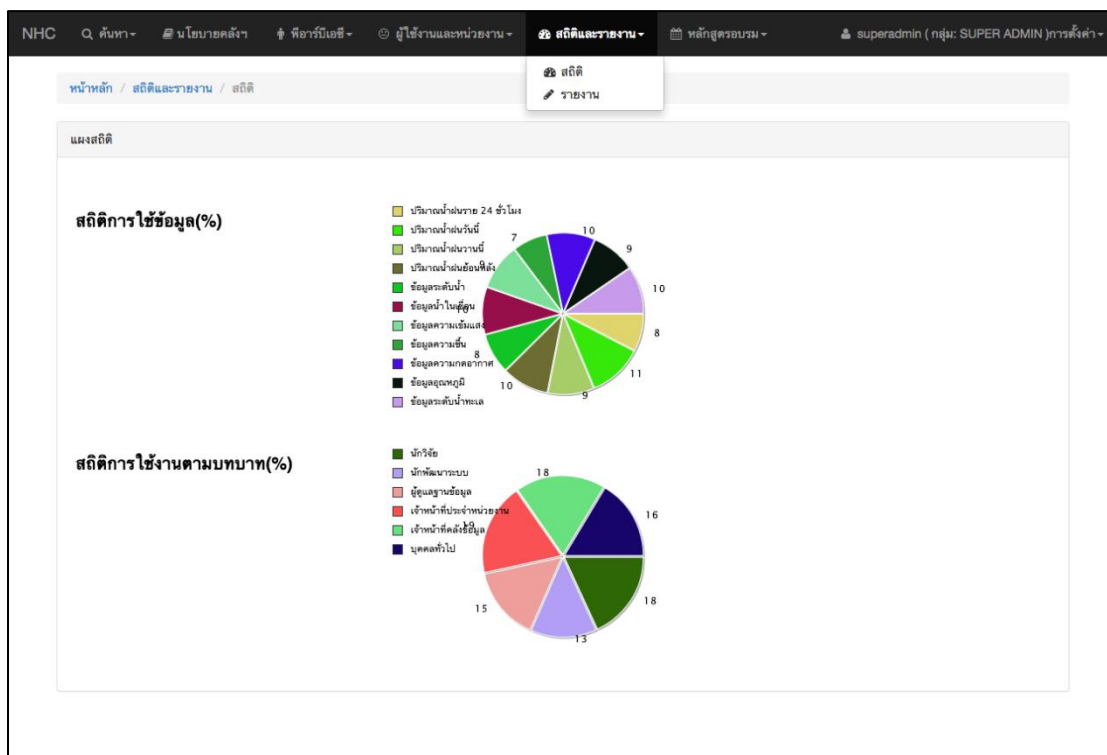
แสดง 1 ถึง 10 จากทั้งหมด 12 แถว

ถอยหลัง 1 2 หน้า

รูปที่ ค.9 รายชื่อหน่วยงานทั้งหมดในคลังสารสนเทศกลาง

5.) เมนูสถิติและรายงาน ประกอบด้วยเมนูย่อยคือ

- สถิติ ประกอบด้วยสถิติการใช้งานข้อมูลและสถิติการใช้งานดังปรากฏอยู่ในรูปที่ ค.10
- รายงานคือ การแสดงรายงานในส่วนการใช้งานของผู้ใช้โดยสามารถกรองผลการค้นหาโดยระบบพบการใช้งานได้ ดังปรากฏในรูปที่ ค.11



รูปที่ ค.10 สถิติการใช้งานคลังสารสนเทศกลาง

แผนรายงาน

นักวิจัย : 2014-07-01 23:33 - 2014-10-02 23:33 ค้นหา

10 แถวต่อหน้า ค้นหา :

ไอพี	โฮส	ล่าสุด	บทบาท	ข้อมูล
:::1	http://localhost/project/sites/public	2014-07-17 22:03:42	นักวิจัย (Super Admin)	ปริมาณเจ้าหน้าที่ 24 ชั่วโมง
:::1	http://localhost/project_nhc/sites/public	2014-07-10 19:02:04	นักวิจัย (Super Admin)	ปริมาณเจ้าหน้าที่ 24 ชั่วโมง

แสดง 1 ถึง 1 จากทั้งหมด 1 แถว

ถอยหลัง 1 หน้า

รูปที่ ค.11 รายงานการใช้งานคลังสารสนเทศกลาง

6.) เมนูหลักสูตรอบรม คือประกอบด้วยเมนูย่อยดังนี้

- หลักสูตรอบรม คือเมนูที่ให้เจ้าหน้าที่คลังสารสนเทศกลางได้กำหนดตารางการอบรม โดยระบุกลุ่มเป้าหมายของแต่ละการอบรม กำหนดวันที่ปีรับการเข้าร่วม หลักสูตรการอบรม
- รายงานตามบุคคล คือการออกรายงานการอบรมตามชื่อผู้ใช้งาน
- รายงานตามบทบาท คือการออกรายงานการอบรมตามบทบาทของผู้ใช้งาน
- รายงานตามช่วงเวลา คือการออกรายงานการอบรมโดยกำหนดระยะเวลาเริ่มต้นและสิ้นสุดของหลักสูตรอบรม
- รายงานตามชื่อหลักสูตร คือการออกรายงานตามชื่อหลักสูตรอบรม

ดังปรากฏในรูปที่ ค.12

ชื่อหลักสูตร	รายละเอียด	กลุ่มเป้าหมาย	สถานะ	วันที่สร้าง	วันสิ้นสุด	
การใช้งานเบื้องต้น คลังสารสนเทศกลาง	เนื้อหาการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลาง	นักวิจัย,นักพัฒนาระบบ,เจ้าหน้าที่ประจำหน่วยงาน,เจ้าหน้าที่คลังข้อมูล	เปิด	2014-07-08 08:30:00	2014-07-31 11:30:00	แก้ไข

รูปที่ ค.12 หน้าตารางการอบรม

7.) เมนูการตั้งค่า เป็นส่วนที่เจ้าหน้าที่คลังสารสนเทศกลางสามารถกำหนดค่าประกอบไปด้วย 6 เมนูย่อยคือ

- การตั้งค่าโปรเวซี คือส่วนการกำหนดโปรเวซีทั้งของตัวผู้ใช้งานปัจจุบันและโปรเวซีเริ่มต้นซึ่งจะมีเฉพาะเจ้าหน้าที่คลังสารสนเทศกลางเท่านั้นสามารถกำหนดได้ และส่วนสุดท้ายคือการกำหนดระยะเวลาการเก็บรักษาข้อมูลดังปรากฏในรูปที่ ค.13

- การตั้งค่าความมั่นคง คือส่วนที่เจ้าหน้าที่คลังสารสนเทศกลางใช้เพื่อเปลี่ยนแปลงรหัสผ่าน และยังประกอบไปด้วยเครื่องมือสำหรับวัดความเข้มแข็งของรหัสผ่าน คำแนะนำสำหรับการกำหนดรหัสผ่านที่เข้มแข็ง และส่วนสุดท้ายคือเครื่องมือสำหรับช่วยเจ้าหน้าที่คลังสารสนเทศในการสร้างรหัสผ่านดังปรากฏในรูปที่ ค.14
- ข้อมูลบัญชี คือส่วนที่แสดงข้อมูลบัญชีของเจ้าหน้าที่คลังสารสนเทศกลางดังปรากฏในรูปที่ ค.15
- พีบีดีพีไอเอ คือส่วนที่แสดงข้อมูลหลักการของพีบีดีพีไอเอ แนวปฏิบัติที่เลือก และเหตุผลของการเลือกแต่ละแนวปฏิบัติซึ่งเป็นที่มาของการสร้างเครื่องมือสนับสนุน และยังแนะนำผู้ใช้งานว่าแนวปฏิบัติข้อไหนจะสำเร็จเมื่อกระทำฟังก์ชันงานไหน และตรงกับหลักการพีบีดีพีไอเอไหนดังปรากฏในรูปที่ ค.16
- การใช้งานระบบ คือส่วนแนะนำการใช้งานระบบให้กับผู้ใช้งานดังปรากฏในรูปที่ ค.17
- ฟังก์ชันใช้งานในระบบ คือส่วนที่แจ้งให้ผู้ใช้งานได้ทราบถึงกรอบปัญหา ฟังก์ชันงานของเครื่องมือสนับสนุน ประเภทผู้ใช้งานที่สามารถใช้งานฟังก์ชันนั้นๆ ได้ และระบุว่าฟังก์ชันงานนั้นตรงกับหลักการไหนของพีบีดีพีไอเอดังปรากฏดังรูปที่ ค.18

ลำดับที่	ชื่อ	สถานะ	
1	ชื่อผู้ใช้งาน	เปิด	แก้ไข
2	เบอร์ติดต่อ	ปิด	แก้ไข
3	หน่วยงานสังกัด	ปิด	แก้ไข
4	ทบวงกรม	ปิด	แก้ไข
5	นามสกุล	ปิด	แก้ไข
6	บทบาท	ปิด	แก้ไข
7	อีเมลล์	ปิด	แก้ไข
8	กระทรวง	ปิด	แก้ไข

รูปที่ ค.13 การตั้งค่าไพรเวซี

หน้าหลัก / ตั้งค่าความมั่นคง

เปลี่ยนรหัสผ่าน มาตรฐานรหัสผ่าน แนะนำการตั้งรหัสผ่าน เครื่องมือสร้างรหัสผ่าน

แผงเปลี่ยนรหัสผ่าน

*รหัสผ่านเดิม

*รหัสผ่านใหม่

*ระบุรหัสผ่านอีกครั้ง

บันทึก

รูปที่ ค.14 การตั้งค่าความมั่นคง

หน้าหลัก / บัญชีผู้ใช้

แผงบัญชีผู้ใช้

ชื่อใช้งาน*

นามสกุล

เบอร์โทรศัพท์ติดต่อ

หน่วยงานสังกัด*

อีเมล*

บันทึกการเปลี่ยนแปลง

รูปที่ ค.15 การตั้งค่าบัญชี

หน้าหลัก / นโยบายคลังฯ / พีบีดีพีไอเอ		
แต่งตั้งหน่วยงานปฏิบัติพีบีดีพีไอเอที่เลือกใช้ให้เหมาะสมกับนโยบายองค์กร และนโยบายคลังสารสนเทศกลางตามแนวปฏิบัติที่เหมาะสม		
หลักการพีบีดี	คำถามพีบีดีพีไอเอที่เลือก	เหตุผลที่เลือก
1) การป้องกันและคาดการณ์ก่อนที่จะเกิดการรุกรานด้านโทรเวช	1) มีบุคคลที่ได้รับมอบหมายให้ทำหน้าที่รับผิดชอบในการพัฒนาบำรุงรักษา และดำเนินการในเรื่องสารสนเทศด้านโทรเวชขององค์กร และการปกป้องข้อมูลหรือไม่	เพื่อให้คลังสารสนเทศกลางสามารถกำหนดผู้ที่ทำหน้าที่รับผิดชอบด้านการบำรุงรักษา และปกป้องข้อมูลขององค์กร
	2) ผู้ที่เกี่ยวข้องที่ถึงข้อมูลจะต้องมีการอบรมตามบทบาทเพื่อให้เกิดความเข้าใจโทรเวชข้อมูลความปลอดภัยและขั้นตอนการทำงานเพื่อนำไปปฏิบัติอย่างถูกต้องหรือไม่	เพื่อให้ผู้ที่เกี่ยวข้องกับคลังสารสนเทศกลางได้ทราบถึงขั้นตอนการทำงานและเข้าใจถึงบทบาทผู้ใช้งาน ในคลังสารสนเทศกลาง
2) โทรเวชจะถูกฝังอยู่ในขั้นตอนการออกแบบสถาปัตยกรรมของระบบไอทีและการดำเนินงานกิจกรรมในองค์กร	1) มีการดำเนินการควบคุมการเข้าถึงข้อมูลบนพื้นฐานของการ "ระบุตัวตน" และ "สิทธิ์" ในการดำเนินการกับข้อมูลหรือไม่	เพื่อให้แน่ใจว่าผู้ใช้ที่มีสิทธิ์เท่านั้นที่สามารถกระทำกับข้อมูลได้โดยเป็นไปตามโทรเวชพื้นฐานที่ได้ถูกกำหนดไว้
3) โทรเวชได้รับการปกป้องตั้งแต่เริ่มใช้งานแม้ไม่มีการกำหนดโดยผู้ใช้งาน	1) มีการบังคับให้มีการตั้งรหัสผ่านที่ยากต่อการคาดเดาความไปถึงมีการกำหนดขนาดความยาวของรหัสผ่านหรือไม่	เพื่อสร้างความมั่นใจให้กับผู้ที่เกี่ยวข้องกับคลังสารสนเทศกลางว่ารหัสผ่านที่ใช้กำหนดขึ้นใช้งานในภาคการคาดเดา
4) ให้ความสำคัญกับกฎระเบียบและวัตถุประสงค์โดยพิจารณาทั้งเรื่องโทรเวชและความมั่นคง	1) มีการวางโครงสร้างและกลไกสำหรับผู้ที่เกี่ยวข้องเพื่อตรวจสอบให้แน่ใจว่าไม่มีการแยกหน้าที่การทำงานด้านโทรเวชและความมั่นคงออกจากกันหรือไม่	เพื่อสร้างความมั่นใจและความน่าเชื่อถือให้กับผู้ที่เกี่ยวข้องกับคลังสารสนเทศกลาง
5) โทรเวชได้ถูกฝังอยู่ระดับตั้งแต่เริ่มกิจกรรมจนถึงกิจกรรมของข้อมูล	1) ได้มีการสร้างตารางเวลาในการเก็บรักษาข้อมูลการทำลายข้อมูลด้านโทรเวชที่ปลอดภัยหรือไม่	เพื่อแสดงให้กับผู้ที่เกี่ยวข้องกับคลังสารสนเทศกลางได้รับทราบช่วงเวลาของการจัดเก็บทำลาย ข้อมูลด้านโทรเวช
6) ความโปร่งใสในการดำเนินกิจกรรมด้านโทรเวชภายในองค์กรตามนโยบายที่กำหนด	1) ได้มีการกำหนดช่องทางเพื่อใช้ในการสื่อสารเจ้าหน้าที่ที่มีความรับผิดชอบด้านโทรเวชและความมั่นคงมีการแจ้งให้ทราบ โดยทั่วถึงหรือไม่	เพื่ออำนวยความสะดวกแก่ผู้ที่เกี่ยวข้องกับคลังสารสนเทศกลาง
7) ผู้เกี่ยวข้องด้านโทรเวชต้องสนับสนุนเพื่อให้โทรเวชเกิดประโยชน์สูงสุดต่อผู้ใช้งาน	1) ทุกนโยบาย ขั้นตอนการปฏิบัติและข้อมูลจำเป็นต้องมีการแจ้งให้ผู้ใช้ทราบ โดยผ่านช่องทางที่ง่ายต่อการเข้าถึง และเขียนในรูปแบบภาษาที่ง่ายต่อการทำความเข้าใจหรือไม่	เพื่อสร้างความโปร่งใสในการปฏิบัติงานและการดำเนินงานของผู้เกี่ยวข้องคลังสารสนเทศกลาง
นโยบายคลังสารสนเทศกลางตามแนวปฏิบัติที่เหมาะสม	ตรงกับหลักการพีบีดี	เมื่อดำเนินการ
1) องค์กรจะต้องกำหนดผู้รับผิดชอบในการบำรุงรักษาจัดการเกี่ยวกับโทรเวชของข้อมูล และโทรเวชของผู้ใช้งาน ในคลังสารสนเทศกลาง โดยประกาศให้รับทราบ โดยทั่วถึง	ข้อที่ 1	กำหนดผู้รับผิดชอบในแต่ละนโยบาย
2) องค์กรจะต้องสร้างหลักสูตรอบรมการใช้งานข้อมูลในคลังสารสนเทศกลาง ให้กับผู้ใช้งานเพื่อความปลอดภัยระหว่างการใช้งาน	ข้อที่ 1	กำหนดหลักสูตรอบรมและกลุ่มเป้าหมายในการอบรม
3) องค์กรจะต้องมีกลไกในการตรวจสอบตัวตนและสิทธิ์ในการกระทำกับข้อมูลตามบทบาทของผู้ใช้งานที่ได้รับในคลังสารสนเทศกลาง เพื่อป้องกันการละเมิดบทบาทหน้าที่ของผู้ใช้งาน	ข้อที่ 2	การใช้งานระบบจะต้องผ่านหน้าเข้าสู่ระบบเพื่อตรวจสอบตัวตนและสิทธิ์
4) องค์กรจะต้องมีตัวช่วยหรือเครื่องมือแนะนำการตั้งรหัสผ่านที่ยากต่อการคาดเดาให้กับผู้ใช้งาน โดยรหัสผ่านจะต้องมีคุณสมบัติที่ดี เพื่อความปลอดภัยในการใช้งาน	ข้อที่ 3	ระบบได้จัดเตรียมเครื่องมือสำหรับตรวจสอบความแข็งแกร่งของรหัสผ่าน คำแนะนำการสร้างรหัสผ่าน และเครื่องมือสร้างรหัสผ่าน
5) องค์กรจะต้องมีกลไกในการตรวจสอบความมั่นคงโทรเวชของข้อมูลและโทรเวชของผู้ใช้งาน ในคลังสารสนเทศกลางเพื่อสร้างความมั่นใจในการใช้งาน	ข้อที่ 4	เจ้าหน้าที่ดำเนินการมอบหมายบทบาท ให้กับผู้ใช้งานในระบบ
6) องค์กรจะต้องมีการจัดทำตารางที่จะถึงการเก็บ การรักษา หรือการทำลายข้อมูลที่อยู่ในคลังสารสนเทศกลาง ให้กับผู้ใช้งาน เพื่อความโปร่งใสและรับทราบโดยทั่วถึง	ข้อที่ 5	เจ้าหน้าที่กำหนดระยะเวลาการเก็บรักษาข้อมูลในระบบ
7) องค์กรจะต้องจัดทำนโยบายการใช้งาน โดยใช้ภาษาที่ง่ายต่อการทำความเข้าใจง่าย เข้าถึงได้สะดวก ให้กับผู้ใช้งานและบุคคลทั่วไปรับทราบโดยทั่วถึง	ข้อที่ 1 และ ข้อ 7	เจ้าหน้าที่เผยแพร่นโยบายการใช้งาน ให้ผู้ใช้งานได้รับทราบ

รูปที่ ค.16 ตารางพีบีดีพีไอเอ

NHC ค้นหา นโยบายคลังฯ พอร์ตโฟลีโอ ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักฎครอบงวม superadmin (กลุ่ม: SUPER ADMIN) การตั้งค่า

หน้าหลัก / ช่วยเหลือ

แผนการใช้งานระบบ

ขั้นตอนการใช้งานระบบ

แนะนำการใช้งานระบบสำหรับผู้ดูแลระบบ

- นโยบายคลังสารสนเทศกลาง
 - บันทึกนโยบายที่ได้รับจากผู้บริหารในระบบ
 - แก้ไขรายการนโยบาย
 - ลบรายการนโยบาย
 - แสดงรายการที่ีดีโอเอที่เกี่ยวข้องกับนโยบาย
 - การแนบเอกสารนโยบายตามหลักการของพอร์ตโฟลีโอ
- พอร์ตโฟลีโอ
 - แสดงรายการเอกสารที่ดีและการเพิ่มเอกสารที่ดี
 - การแก้ไขและลบเอกสารที่ดี
- ผู้ใช้และหน่วยงาน
 - การเปลี่ยนประเภทผู้ใช้งานและการอนุญาตให้ผู้ใช้งานใช้งานระบบ
 - การมอบหมายบทบาทให้กับผู้ใช้งาน
 - การส่งรายการและเพิ่มผู้รับผิดชอบนโยบาย
 - การแก้ไขและลบผู้รับผิดชอบนโยบาย
 - การแสดงและเพิ่มหน่วยงานที่ให้ความร่วมมือกับคลังสารสนเทศฯ
- การค้นหา
 - การค้นหาผู้ใช้งานตามบทบาท
 - การค้นหาหน่วยงานตามข้อมูลที่มีความร่วมมือ
 - การหาข้อมูลตามหน่วยงาน
- สถิติและรายงาน
 - สถิติการใช้งาน

รูปที่ ค.17 ข้อมูลช่วยเหลือในการใช้งานคลังสารสนเทศกลาง



NHC ค้นหา นโยบายคลังฯ ทิวารีบีเอส ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักศูตบกรม superadmin (กลุ่ม: SUPER ADMIN) การตั้งค่า

หน้าหลัก /ช่วยเหลือ

แผงฟังก์ชันงานในระบบ

ตำแหน่งหน้าที่ผู้ใช้งานในระบบ

- เจ้าหน้าที่คลังสารสนเทศ
- ผู้ใช้งานประเภทผู้ดูแลระบบ (หนึ่งหน่วยงานมีได้คนเดียว)
- ผู้ใช้งานประเภททั่วไป

กรอบปัญหา	ฟังก์ชันงาน	ตำแหน่งหน้าที่	หลักการที่ดี	ระบบงานสนับสนุน
1.การกำหนดนโยบายการใช้งานข้อมูลตามสิทธิและบทบาท	<ul style="list-style-type: none"> สนับสนุนการจัดการนโยบาย <ul style="list-style-type: none"> สามารถค้นหา นโยบาย สามารถบันทึกนโยบายการใช้งาน สามารถแก้ไขนโยบาย สามารถเลิกใช้นโยบาย สามารถกำหนด/แก้ไข/ลบชื่อผู้รับผิดชอบเพื่อให้ผู้ใช้ติดต่อ กำหนดค่าพื้นฐานการใช้อีเมล <ul style="list-style-type: none"> สามารถบันทึกรายการโทรเวชικάเริ่มต้นข้อมูลที่อยู่ระบบ สามารถบันทึกรายการโทรเวชικάเริ่มต้นข้อมูลใช้งาน สามารถเพิ่มรายการโทรเวชικάเริ่มต้นข้อมูลใช้งาน สามารถแก้ไขรายการโทรเวชικάเริ่มต้นข้อมูลใช้งาน สามารถลบรายการโทรเวชικάเริ่มต้นข้อมูลใช้งาน ระบุตัวตน มีความสามารถคือ <ul style="list-style-type: none"> สามารถเรียกแก้ไข ในกรณีลืมรหัสผ่าน สามารถเข้าสู่ระบบ สามารถแก้ไขข้อมูลส่วนตัว สามารถเปลี่ยนรหัสผ่าน แนะนำรหัสผ่าน มีความสามารถคือ <ul style="list-style-type: none"> สามารถสร้างรหัสผ่านให้ผู้ใช้ สามารถให้คำแนะนำในการสร้างรหัสผ่าน สนับสนุนการอบรมด้านโทรเวช <ul style="list-style-type: none"> สามารถบันทึกการเข้ารับการอบรม สามารถสร้างตารางการอบรม สามารถแก้ไขตารางการอบรม สามารถกำหนดกลุ่มเป้าหมาย สามารถลบตารางการอบรม สามารถออกรายงานการอบรม <ul style="list-style-type: none"> สามารถบันทึกการขายการเก็บรักษาและทำลาย สามารถแสดงรายงานการเก็บรักษาและทำลาย 	<ul style="list-style-type: none"> ข้อที่ 1 - ข้อที่ 3 ข้อที่ 1 ข้อที่ 1 ข้อที่ 1 ข้อที่ 1 ข้อที่ 1 ข้อที่ 1 ข้อที่ 1 - ข้อที่ 3 ข้อที่ 1 - ข้อที่ 3 ข้อที่ 1 - ข้อที่ 3 ข้อที่ 1 - ข้อที่ 3 ข้อที่ 2 - ข้อที่ 3 ข้อที่ 1 ข้อที่ 1 ข้อที่ 1 ข้อที่ 1 ข้อที่ 1 - ข้อที่ 3 	ข้อที่ 2 และ ข้อที่ 4	✓
3.กระบวนการใช้อีเมล	<ul style="list-style-type: none"> เรียกดูข้อมูลการใช้งานระบบ <ul style="list-style-type: none"> สามารถออกรายงานการใช้งานระบบแบบรายวันหรือตามความต้องการโดยการระบุวัน เวลา สามารถค้นหาหรือการเข้าใช้ระบบ 	<ul style="list-style-type: none"> ข้อที่ 1 ข้อที่ 1 	ข้อที่ 3	✓

รูปที่ ค.18 ฟังก์ชันงานในคลังสารสนเทศกลาง

8.) เมนูออกจากระบบ คือเมนูสำหรับออกจากระบบเพื่อเลิกใช้งาน และระบบจะทำการออกจากระบบโดยอัตโนมัติในกรณีที่ผู้ใช้งานไม่มีกิจกรรมใดๆ ในระบบเป็นเวลานาน

ค.2 ส่วนต่อประสานสำหรับผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลาง

ตารางที่ ค.2 ฟังก์ชันการใช้งานสำหรับผู้ใช้งานเครื่องมือสนับสนุนคลังสารสนเทศกลาง

ฟังก์ชันงาน/เมนู	คำอธิบาย
1.) ค้นหา <ul style="list-style-type: none"> - ค้นหาตามบทบาท - ค้นหาตามชื่อข้อมูล - ค้นหาตามชื่อหน่วยงาน 	ค้นหาผู้ใช้งานตามบทบาทที่ได้รับ ค้นหาหน่วยงานตามชื่อข้อมูล ค้นหาชื่อข้อมูลตามหน่วยงานในคลังสารสนเทศกลาง
2.) ข้อมูล	เรียกดูข้อมูลสอดคล้องกับนโยบายที่ได้รับ
3.) ร้องขอข้อมูล	แสดงแบบฟอร์มเพื่อร้องขอเปิดเผยข้อมูล
4.) คำร้องขอข้อมูล	แสดงรายการที่ผู้ใช้งานท่านอื่นร้องขอเปิดเผยข้อมูล
5.) ผลการร้องขอข้อมูล	แสดงรายการเมื่อรายการที่ร้องขอข้อมูลได้รับการอนุญาต
6.) หลักสูตรอบรม	แสดงจำนวนหลักสูตรอบรมที่มีผู้ใช้งานเป็นกลุ่มเป้าหมาย
7.) การตั้งค่าโปรเวซี <ul style="list-style-type: none"> - ตั้งค่าโปรเวซี - ตั้งค่าความมั่นคง - ข้อมูลบัญชี - พีบีดีพีไอเอ - การใช้งานระบบ - ฟังก์ชันใช้งานในระบบ 	เมนูสำหรับปรับแต่งโปรเวซีของผู้ใช้งาน เมนูสำหรับเปลี่ยนแปลงด้านความมั่นคง เมนูสำหรับแสดงข้อมูลส่วนตัวของผู้ใช้งาน แสดงตารางพีบีดีพีไอเอและคำถาม เหตุผลที่เลือกใช้ เอกสารแนะนำการใช้งานระบบ เอกสารแนะนำฟังก์ชันการใช้งานของแต่ละบทบาท
8.) ออกจากระบบ	เมนูสำหรับออกจากระบบ

จากตารางที่ ค.2 รายละเอียดในส่วนการออกแบบส่วนต่อประสานผู้ใช้งานมีดังต่อไปนี้

1.) เมนูค้นหา สำหรับผู้ใช้งานระบบคลังสารสนเทศกลางสามารถค้นหาได้ 3 ประเภทคือ

- การค้นหาตามบทบาทคือ การค้นหาโดยใช้บทบาทผู้ใช้งานเป็นคำค้นหา ดังปรากฏในรูปที่ ค.19
- การค้นหาตามชื่อข้อมูลคือ การค้นหาโดยใช้ชื่อข้อมูลเป็นคำค้นหาดังปรากฏในรูปที่ ค.20

- การค้นหาตามชื่อหน่วยงาน คือการค้นหาข้อมูลโดยใช้ชื่อหน่วยงานเป็นคำค้นหาดังปรากฏดังรูปที่ ค.21

The screenshot shows a web application interface with a navigation bar at the top containing the text 'NHC' and several menu items. Below the navigation bar, there is a breadcrumb trail: 'หน้าหลัก / ค้นหา / ค้นหาตามบทบาท'. The main content area is titled 'แผงรายการบทบาท' and contains a search form with a dropdown menu set to 'นักวิจัย' and a 'ค้นหา' button. Below the search form is a table with the following data:

ลำดับ	ชื่อผู้ใช้งาน
1	user6
2	user5
3	user3

รูปที่ ค.19 หน้าค้นหาผู้ใช้ในระบบตามบทบาทของผู้ใช้งาน

The screenshot shows a web application interface with a navigation bar at the top containing the text 'NHC' and several menu items. Below the navigation bar, there is a breadcrumb trail: 'หน้าหลัก / ค้นหา / ค้นหาตามชื่อข้อมูล'. The main content area is titled 'แผงรายการข้อมูล' and contains a search form with a dropdown menu set to 'ปริมาณน้ำฝนราย 24 ชั่วโมง' and a 'ค้นหา' button. Below the search form is a table with the following data:

รหัส	หน่วยงาน	ติดต่อ
1	หน่วยงานที่ 11	user4
2	หน่วยงานที่ 4	user3
3	หน่วยงานที่ 4	user2
4	หน่วยงานที่ 7	user1

รูปที่ ค.20 หน้าค้นหาหน่วยงานตามชื่อข้อมูล

หน้าหลัก / ค้นหา / ค้นหาตามหน่วยงาน

แผนรายการหน่วยงาน

หน่วยงานที่ 1

ลำดับ	ชื่อข้อมูล	สถานะข้อมูล	วันสุดท้ายที่เก็บข้อมูล
1	ข้อมูลน้ำในเขื่อน	ไม่อนุญาตให้ร้องขอ	2017-07-08
2	ข้อมูลระดับน้ำ	อนุญาตให้ร้องขอ	2017-07-08

รูปที่ ค.21 หน้าค้นหาข้อมูลตามหน่วยงาน

2.) เมนูข้อมูล คือการแสดงผลข้อมูลนั้นขึ้นอยู่กับแต่ละบทบาทที่ใช้งานในระบบที่ได้รับ จะสอดคล้องกับนโยบายการใช้งานที่ได้ประกาศไว้เช่น นักวิจัย สามารถเรียกดูข้อมูลได้เฉพาะ ข้อมูลระดับน้ำ ข้อมูลปริมาณน้ำในเขื่อนและปริมาณน้ำฝนราย 24 ชั่วโมง เป็นต้น ระบบจะไม่แสดงข้อมูลอื่นนอกเหนือจากที่นโยบายได้กำหนดไว้ให้ผู้ใช้งาน ตัวอย่างของการเรียกดูข้อมูลปรากฏในรูปที่ ค.22

หน้าหลัก / เรียกดูข้อมูล

แผนเรียกดูข้อมูล

นโยบายที่เกี่ยวข้อง

ข้อมูลนำในเงื่อนไข: ข้อมูลปัจจุบัน จากหน่วยงานทั้งหมด? ค้นหา

10 แถวต่อหน้า ค้นหา:

รหัสสถานี	หน่วยงาน	วันที่	เวลา	ข้อมูลนำในเงื่อนไข ลาน.ม.
ldamrid0001	กรมชลประทาน	2013-10-08	00:10	6327.00
ldamrid0002	กรมชลประทาน	2013-10-08	00:10	5721.00
ldamrid0003	กรมชลประทาน	2013-10-08	00:10	176.00
ldamrid0004	กรมชลประทาน	2013-10-08	00:10	90.00
ldamrid0005	กรมชลประทาน	2013-10-08	00:10	99.00
ldamrid0006	กรมชลประทาน	2013-10-08	00:10	1080.00
ldamrid0007	กรมชลประทาน	2013-10-08	00:10	212.00
ldamrid0008	กรมชลประทาน	2013-10-08	00:10	132.00
ldamrid0009	กรมชลประทาน	2013-10-08	00:10	422.00
ldamrid0010	กรมชลประทาน	2013-10-08	00:10	1833.00

แสดง 1 ถึง 10 จากทั้งหมด 33 แถว

ถอยหลัง 1 2 3 4 เติมนำหน้า

รูปที่ ค.22 การเรียกดูข้อมูลตามบทบาทนักวิจัย

3.) ร้องขอข้อมูล ซึ่งทำหน้าที่ในกรณีที่ผู้ใช้งานจำเป็นต้องใช้ข้อมูลที่อยู่ในหน่วยงานอื่น ผู้ใช้งาน จะทำการกรอกคำร้องขอข้อมูลนั้นๆ เพื่อส่งไปยังหน่วยงานเจ้าของข้อมูลพิจารณาตามเหตุผลของคำ ร้อง หลังจากได้รับการอนุญาตจากหน่วยงานเจ้าของข้อมูลจึงจะสามารถนำข้อมูลดังกล่าวมาใช้ใน งานวิจัยหรือเพื่อนำไปเผยแพร่ดังปรากฏในรูปที่ ค.23

หน้าหลัก / ขอข้อมูล

แผนขอข้อมูล

นโยบายที่เกี่ยวข้อง

หน่วยงานที่ 1: ข้อมูลระดับน้ำ: ข้อมูลปัจจุบัน: ขออนุญาตเปิดแคชข้อมูล: ส่งคำขอ

เสร็จสิ้น คำร้องขอของท่านได้รับการบันทึกเรียบร้อยแล้ว.

รูปที่ ค.23 ตัวอย่างการร้องขอข้อมูล

4.) เมนูคำร้องขอข้อมูล เมื่อคำร้องขอข้อมูลจากหน่วยงานที่ร้องขอได้ถูกบันทึกในระบบ ระบบ จะทำการส่งคำร้องขอข้อมูลไปยังหน่วยงานเจ้าของข้อมูลซึ่งรายละเอียดคำร้องขอข้อมูลประกอบไปด้วย ชื่อผู้ร้องขอ หน่วยงานที่ร้อง วัตถุประสงค์ของคำร้องขอ เพื่อให้หน่วยงานเจ้าของข้อมูลได้พิจารณาคำร้อง ดังปรากฏในรูปที่ ค.24 การพิจารณาทำร้องขอข้อมูลปรากฏในรูปที่ ค.25

*ข้อมูลที่ร้องขอ	ความถี่ข้อมูล	สถานะการร้องขอ	วัตถุประสงค์การขอ	*ผู้ร้องขอ	*หน่วยงานผู้ร้องขอ	วันที่ร้องขอ	
ข้อมูลระดับน้ำ	ข้อมูลปัจจุบัน	อยู่ระหว่างพิจารณา	ขออนุญาตเปิดเผยข้อมูล	user1 User1 (นักวิจัย)	หน่วยงานที่ 2	2014-10-15	Edit

แสดง 1 ถึง 1 จากทั้งหมด 1 แถว

ถอยหลัง 1 | 1 | เดินหน้า

รูปที่ ค.24 รายการคำร้องขอข้อมูล

ข้อมูลที่ร้องขอ: ข้อมูลระดับน้ำ

ความถี่ข้อมูล: ข้อมูลปัจจุบัน

สถานะการร้องขอ: ยื่นขอการร้องขอ

ผู้ร้องขอ: user1 User1

หน่วยงานผู้ร้องขอ: หน่วยงานที่ 3

วันที่ร้องขอ: 2014-10-15 10:10 น.

หมายเหตุ: ขออนุญาตตามคำร้องขอ

บันทึก

รูปที่ ค.25 หน้าพิจารณาคำร้องขอข้อมูล

5.) เมนูผลการร้องขอข้อมูล หลังจากทีหน่วยงานเจ้าของข้อมูลอนุมัติ ผลของคำร้องขอจะแสดงเป็นตัวเลขหลังเมนูผลการร้องขอข้อมูล ดังปรากฏในรูปที่ ค.26 ซึ่งจะแสดงวันเวลาผลของการพิจารณาของหน่วยงานเจ้าของข้อมูล

*ข้อมูลที่ร้องขอ	ความถี่ข้อมูล	สถานะการร้องขอ	*วัตถุประสงค์การขอ	*ผู้อนุมัติ	*หน่วยงานข้อมูล	วันที่อนุมัติ	วันที่ร้องขอ	หมายเหตุ
ข้อมูลระดับน้ำ	ข้อมูลปัจจุบัน	ยินยอมการร้องขอ	ขออนุญาตเปิดเผยข้อมูล	user6 user6 (นักวิจัย)	หน่วยงานที่ 3	2014-10-15	2014-10-15	ดาวน์โหลด
*ข้อมูลที่ร้องขอ	ความถี่ข้อมูล	สถานะการร้องขอ	*วัตถุประสงค์การขอ	*ผู้อนุมัติ	*หน่วยงานข้อมูล	วันที่อนุมัติ	วันที่ร้องขอ	หมายเหตุ

แสดง 1 ถึง 1 จากทั้งหมด 1 แถว

ถอยหลัง 1 หน้า

รูปที่ ค.26 รายการผลการพิจารณาการร้องขอข้อมูล

6.) เมนูหลักสูตรการอบรม คือเมื่อเจ้าหน้าที่คลังสารสนเทศสร้างหลักสูตรอบรมและทำการระบุกลุ่มเป้าหมายซึ่งจะเป็นชื่อบทบาท และเมื่อผู้ใช้งานอยู่ในกลุ่มเป้าหมายเมื่อเข้าสู่ระบบเมนูหลักสูตรอบรมจะแสดงตัวเลข ซึ่งจะเป็นการบอกถึงว่ามีหลักสูตรอบรมที่ทางเจ้าหน้าที่คลังสารสนเทศได้จัดขึ้น และได้เลือกให้บทบาทที่ผู้ใช้งานได้รับนั้นเป็นหนึ่งในกลุ่มเป้าหมายของหลักสูตรอบรม โดยผู้ใช้งานสามารถตอบรับเพื่อเข้าร่วมในแต่ละหลักสูตรดังปรากฏในรูปที่ ค.27

NHC **บุษบาท: (นักพัฒนาระบบ)** ค้นหา ข้อมูล ร้องขอข้อมูล หลักสูตรอบรม ผลการร้องขอข้อมูล คำร้องขอข้อมูล user7 (กลุ่ม: ADMIN) การตั้งค่า

หน้าหลัก / รายการหลักสูตรอบรม

แผนรายการหลักสูตรอบรม

ค้นหา

ชื่อหลักสูตร	รายละเอียด	ประวัติการเข้าร่วม	สถานะหลักสูตร	วันที่สร้าง	วันสิ้นสุด	เข้าร่วม
การใช้งานเบื้องต้น คลังสารสนเทศกลาง ครั้งที่ 2	เนื้อหาการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลาง	N/A	เปิด	2014-10-15	2014-12-25	<input checked="" type="checkbox"/>
การใช้งานเบื้องต้น คลังสารสนเทศกลาง	เนื้อหาการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลาง	N/A	ปิด	2014-06-11	2014-07-31	

เข้าร่วม

รูปที่ ค.27 รายการหลักสูตรอบรม

7.) เมื่อกำหนดค่าโปรแกรมสำหรับผู้ใช้งานคลังสารสนเทศกลางมีลักษณะการทำงานเหมือนกับเจ้าหน้าที่คลังสารสนเทศกลางซึ่งได้กล่าวมาแล้ว ดังแสดงในรูปที่ ค.28 โดยเพิ่มในส่วนของผู้ใช้เจ้าหน้าที่ประจำหน่วยงานประเภทผู้ดูแลระบบจะสามารถกำหนดโปรแกรมข้อมูลของหน่วยงานได้

NHC ค้นหา นโยบายคลังฯ ศึกษามีเอชไอ ใช้งานและหน่วยงาน สถิติและรายงาน หลักสูตรอบรม superadmin (กลุ่ม: SUPER ADMIN) การตั้งค่า

หน้าหลัก / ตั้งค่าความมั่นคง

เปลี่ยนรหัสผ่าน มาตรฐานรหัสผ่าน แนะนำการตั้งรหัสผ่าน เครื่องมือสร้างรหัสผ่าน

แผนเปลี่ยนรหัสผ่าน

*รหัสผ่านเดิม

*รหัสผ่านใหม่

*ระบุรหัสผ่านอีกครั้ง

บันทึก

รูปที่ ค.28 หน้าการตั้งค่าความมั่นคง

ภาคผนวก ง รายการคำถามพีดีพีไอเอ

สำหรับภาคผนวก ง ประกอบไปด้วยรายการดังต่อไปนี้

- ตาราง ง.1 คือ รายการแนวปฏิบัติพีดีพีไอเอต้นฉบับ
- ตาราง ง.2 ตารางรายการแนวปฏิบัติที่ผ่านการพิจารณาประยุกต์ใช้กับคลังสารสนเทศกลาง คือ ตารางรายการแนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีดีพีไอเอรวมไปถึงเหตุผล และประโยชน์ที่ประยุกต์ใช้กับคลังสารสนเทศกลาง
- รูปที่ ง.1 – ง.39 คือ รูปแสดงฟังก์ชันงานเครื่องมือสนับสนุนที่อิมพลีเมนต์ตามรายแนวปฏิบัติพีดีพีไอเอที่พิจารณานำมาประยุกต์ใช้กับคลังสารสนเทศกลาง
- รูปที่ ง.40 – ง.46 คือ แผนภาพคลาสที่ผ่านการวิเคราะห์จากรายการแนวปฏิบัติพีดีพีไอเอ ในตาราง ง.1
- ตารางที่ ง.3 – ง.9 คือ ตารางคำอธิบายแผนภาพคลาสจากรูปที่ ง.40 – ง.46

โดยมีรายละเอียดดังต่อไปนี้

ง.1 รายการแนวปฏิบัติพีดีพีไอเอ

ตารางที่ ง.1 รายการแนวปฏิบัติพีดีพีไอเอ

Principle 1: Proactive not Reactive

Accountability:

- a) Has an ‘accountable’ person been assigned responsibility for developing, maintaining, and implementing your organization’s privacy and data protection practices?
- b) Has an ‘accountable’ person been assigned responsibility for developing, maintaining, and implementing your organization’s information security program?
- c) Is there visible executive commitment to continuously set and enforce high standards of privacy and security practices?
- d) Is this commitment demonstrably shared by user communities and stakeholders?

- e) Is there a procedure in place to ensure that executives and the board of directors are regularly updated on the privacy and security program, including policies and procedures?
- f) Has a privacy and security governance and accountability framework been developed to ensure compliance with the privacy and security policies and procedures that have been implemented?
- g) Are all employees, volunteers, and contractors who access PI required to sign Confidentiality Agreements? Are they required to re-execute their Confidentiality Agreements on an on-going basis, for example, annually?
- h) Have you ensured that privacy and security protection is built into the terms of service level agreements, data sharing agreements, third party agreements, and other legal instruments?

Policies and Procedures:

- i) Have you implemented a procedure for identifying and managing privacy breaches?
- j) Have you implemented a procedure for identifying and managing information security breaches?
- k) Have you established a schedule for the on-going review of your privacy and security policies and procedures to take account of evolving privacy and security standards and best practices and statutory and regulatory changes?

Privacy and Security Risk Management:

- l) Have you implemented a Corporate Risk Management Framework?
- m) Do your project plans for the development, or redesign, of your information technology, business practices, and physical design and networked infrastructures include 'privacy approval gateways?'
- n) Is a PIA required to be conducted at the conceptual, design, logical, and redesign stages of the Application?

o) Is the PIA reviewed and approved by senior executives of your organization?

p) To the extent possible, do you mitigate all of the risks identified in PIAs?

q) Are PIAs reviewed on an on-going basis to ensure they continue to be accurate and consistent with the organization's information practices, and to ensure that the recommendations have been, or are being, addressed by the organization?

r) Have you established standardized methods to proactively identify and address inadequate privacy technical designs and privacy practices?

Privacy and Security Training and Awareness:

s) Have you implemented a privacy and security awareness and training program?

t) Are all employees, volunteers, and contractors who access PI required to attend initial privacy and security training prior to being given access to PI?

u) Are employees, volunteers and contractors who access PI provided role-based training to understand how to apply the privacy and security policies and procedures of the organization in their daily employment, contractual or other responsibilities?

v) Are all employees, volunteers, and contractors who access PI required to attend privacy and security training on an on-going basis (e.g., annually)?

w) Is the privacy and security awareness and training program regularly updated as changes in the business or statutory environments require?

Audit and Compliance:

x) Have you implemented policies and procedures to monitor, evaluate, and verify compliance with your privacy and security policies and procedures and with the terms related to privacy and security contained in agreements and other legal instruments?

y) Do you have a mechanism for monitoring and reporting on compliance with

your privacy and security policies and procedures, and the terms related to privacy and security contained in agreements and other legal instruments?

z) Have you implemented a program of privacy and security audits?

aa) Do you retain independent third parties to audit your organization's practices against your privacy and security policies and procedures?

bb) Are procedures in place to ensure that the recommendations arising out of privacy and security audits are addressed?

Principle 2: Privacy as the Default Setting

a) Do you design information technologies, business processes, physical spaces and networked infrastructures around the principles of minimizing the identifiability, observability, and linkability of PI to the greatest degree possible?

b) Do you ensure that the purposes for which PI is collected, used, and disclosed are clear, limited, and relevant to the circumstances?

c) Do you ensure PI is collected, used, and disclosed according to the stated purposes for its collection, use, and disclosure?

d) Do you collect, use, and disclose PI only if other information would not serve the purpose?

e) Have policies and procedures been developed and implemented that require the use of encrypted, deidentified, or aggregate information, rather than PI, where PI is not necessary to serve the purpose?

f) Do these policies and procedures require the encryption of all PI collected, used, and disclosed using mobile devices?

g) Do you collect, use, and disclose the minimum amount of PI necessary to serve the purpose?

h) Are the categories of PI that are being collected reviewed on an on-going basis to ensure the collection of PI is limited to that which is required to fulfill the purposes for which it is collected?

- i) Have you determined that your collection of PI is fair and necessary for a lawful purpose?
- j) Are procedures in place to review de-identified and aggregate information prior to its use or disclosure to ensure the information does not identify an individual, and that it is not reasonably foreseeable that the information could be used to identify an individual?
- k) Have you implemented user access controls based on 'need to know,' and 'least privilege' principles? Does access control extend to technical staff?
- l) Do you ensure that if individuals take no action to protect their privacy, their privacy is nonetheless still protected?

Principle 3: Privacy Embedded into Design

Privacy and Security Program:

- a) Have you ensured your privacy and security program, and its associated policies and procedures, meet or exceed industry-accepted standards, frameworks, models, best practices, and guidelines, in addition to statutory requirements?
- b) Have privacy and security controls been developed and implemented in a manner that, to the extent possible, minimizes the risk of theft, loss, and unauthorized use or disclosure of PI?
- c) Are your privacy and security controls amenable to external reviews/audits?

Privacy and Security Architecture:

- d) Have you documented and distributed a Privacy Architecture for your organization to ensure established privacy protections are built into the design of all Applications that collect, use, and disclose PI? Does your Privacy Architecture:

- Ensure FIPS are built into the design or redesign of the Application;
- Classify data in terms of its level of identifiability and its sensitivity;

- Include a Glossary of Privacy Terminology to explain the meaning of the terms used in the documentation used by the organization;
- Impose restrictions on collection, use, and disclosure of PI;
- Limit the secondary uses of PI;
- Impose requirements for the use of encrypted, de-identified and aggregate information instead of PI, whenever possible; and
- Set out business rules for consent management, access control, audit logging, reporting and alerting, user notification, and individuals access to, and correction of, their PI?

e) Have you documented and distributed a Security Architecture to ensure established security safeguards (administrative, physical, and technical) are built into all Applications that collect, use, disclose, and retain PI?

f) Have you implemented procedures and/or mechanisms to verify that the privacy and security architectural requirements have been appropriately designed into the functionality of the Application? Do they include 'privacy and security review and approval gateways' throughout the design, development, and redesign processes?

g) Have you implemented user access controls based on 'need to know' and 'least privilege' principles?

Design Requirements for the Application:

h) Do you have a defined process for the design and redesign of any new IT systems, business practices, and physical design and networked infrastructures that must be followed and approved by the individual(s) responsible for privacy and security in the organization prior to it being implemented?

i) Is this process documented and distributed to all individuals within the organization responsible for the design or redesign of such Applications?

j) Do you conduct audits to ensure that this process is consistently applied?

k) Does this process include the following elements:

Consultations in the design or redesign stages of an Application with those internal and external to

the organization who will be collecting, using, or disclosing PI?

- Conducting PIAs and TRAs at the conceptual, physical, logical, and redesign stages of the Application?
- Procedure to manage and address risks identified in such PIAs and TRAs prior to the implementation of the specific Application?
- Ensuring PIAs and TRAs include the choices for remediation of privacy and security risks and the reasons those choices were made?
- Requirement that, where possible, privacy enhancing technologies appropriate to the Application and the sensitivity of the PI that is collected, used, or disclosed, such as strong encryption or deidentification, are incorporated into the design or redesign?
- Requirement to ensure that PI is required for purposes of the Application and that only the minimum amount of PI is collected, used, or disclosed in the Application?
- Incorporation of the privacy and security requirements into any Requests for Proposals issued by the organization in the event that the Application is to be built and implemented by a third party?
- Access controls and requirements for authentication and identification of individuals who will have access to the PI in the Application, and a mechanism for auditing such access?
- Establishment of rules to identify the individuals who require access to the PI based on 'need to know' and 'least privileges' principles and controls to limit access to such individuals?
- Enforcement of standards for strong passwords, including minimum and

maximum length of the password, and password composition?

l) Have you developed and implemented privacy and security policies to inform the design of IT functionality and organizational business procedures?

Principle 4: Full Functionality - Positive-Sum - Not Zero-Sum

a) For your Application, have you identified, documented, and made available throughout the organization:

- All individuals' interests related to the privacy, confidentiality, and security of their PI?
- All business interests, drivers, and objectives?
- Desired business functionality?
- Privacy functionality requirements?
- o Security functionality requirements?

b) Have you established structures and mechanisms whereby interested parties may enter into dialogue to ensure there are no trade-offs between functionality and privacy, and between privacy and security?

c) Have you developed agreed-upon metrics and assessed whether all interests and objectives have been met?

d) Do you reject privacy or security risk assessment recommendations that would result in trade-offs between functionality and privacy, and between privacy and security?

e) Have you considered all risk mitigation recommendations against the intent of the PbD Principles to ensure consistency?

f) Does the Application achieve all the interests and objectives sought to be achieved?

Principle 5: Full Life Cycle Protection

At each stage of the PI's life cycle, the following questions should be asked and

remedial actions taken where risks, or gaps, are identified in your organization's security posture:

a) Have you mapped the flows of PI from collection through use, disclosure, and destruction?

b) Have you completed a data sensitivity analysis?

c) Have physical and technical security risk assessments been conducted at every stage of a project?

d) Have you identified all of the "touch and hand-off points" for PI for which security safeguards need to be applied?

e) Have you assigned an 'accountable person' to be responsible for ensuring the mitigation of risks identified in your physical and technical security risk assessments?

f) Have you implemented administrative, technical, and physical safeguards that are reasonable in the circumstances? Are these safeguards:

- Based on industry-accepted standards, frameworks, models, best practices, and guidelines for security, and in compliance with statutory requirements?
- Based on a defense-in-depth strategy to address identified threats and risks?
- o Commensurate with the amount and sensitivity of the PI, and with the number and nature of those individuals with access to the PI?

g) Do these administrative, technical, and physical safeguards ensure the secure retention, transfer, and destruction of PI?

h) Have you ensured vendor and third party agreements clearly set out accountabilities and responsibilities for ensuring the implementation of safeguards and mandatory security controls?

i) Does your organization require that assessments of security controls are

conducted regularly throughout the life cycle of the PI to ensure its confidentiality, integrity, and availability?

j) Have you established a retention schedule and procedures for the secure destruction of PI?

k) Does the retention schedule:

- Clearly establish the length of time for which described categories of PI must be retained?
- Indicate the rationale for the retention of PI for these time periods?
- o Require documentation describing the PI and the manner in which it may be stored according to the retention schedule?

l) Do your destruction procedures:

- Require that PI must be destroyed in such a manner that it is not possible to recreate the information?
- Provide acceptable manners for destruction of PI in all formats in which it is held by the organization; e.g., electronic, paper?
- Remind individuals of the requirement to destroy PI that exists in electronic devices such as photocopier and facsimile machines before disposal of the device or its return to the supplier?
- o Require that a certificate of destruction be prepared to include the nature of the PI, the date, identification of the individual who destroyed the PI, and the reason for the destruction of the PI at that time?

Principle 6: Visibility and Transparency : Keep It Open

Accountability:

a) Is the identity and contact information of the individual(s) responsible for privacy and security in your organization made available to the public and known within your organization?

b) Have you implemented a policy that requires all 'public-facing' documents to

be written in 'plain language' that is easily understood by the individuals whose information is the subject of the policies and procedures, and which includes information on how to assess the next level of address?

c) Are the stated privacy and security practices of the Application subject to independent verification?

Openness:

d) Do you make information about the policies and procedures and controls relating to the management of PI readily available to individuals?

e) Do you publish summaries of all completed PIAs and TRAs?

f) Do you publish summaries of independent third party audits of your information practices?

g) Do you make available a list of data holdings of PI maintained by your organization?

Compliance:

h) Have you implemented policies and procedures to receive, document, track, investigate, remediate, and respond to complaints? Have you developed a redress procedure?

i) Have you implemented policies and procedures to receive, document, track, and respond to privacy inquiries?

Principle 7: Respect for User Privacy

Policies and Procedures

a) Have you implemented policies and procedures:

- To ensure individuals are informed (via a public notice or other mechanism) about the purposes for the collection, use, transfer and disclosure of their PI at, or before, the time the PI is collected?
- To obtain the consent of individuals to the collection, use, and disclosure of their PI, where appropriate, or where otherwise required by

law?

- For obtaining and recording consent for the collection, use, and disclosure of PI, taking account individuals' expectations and statutory or regulatory requirements?
- For individuals to withhold or withdraw their consent for the collection, use, and disclosure of their PI (except where otherwise permitted or required by law)?
- To ensure individuals may request access to, and correction of, their PI?
- To ensure individuals are aware of how to make a privacy complaint?
- To ensure individuals are aware of the redress mechanisms, including how to access the next level of redress?
- o To ensure individuals are aware of how to contact your organization's person accountable for privacy?

b) Are all policies, procedures, and information directed to individuals easily and freely accessible and written in easy-to-understand plain language?

c) Are your procedures simple to use?

d) Have you posted layered notices to enable individuals to understand your policies and procedures in more, or less, detail, as they wish?

e) Do your notices provide individuals with adequate information about how you protect their privacy, as well as inform them of their privacy rights, including their rights to withhold or withdraw their consent to the collection, use and disclosure of their PI?

f) Are your notices posted where they are likely to come to the attention of individuals or are individuals provided copies of such notices?

g) Have you implemented policies and procedures to ensure PI is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes for its collection and use?

Privacy Expectations

h) Have you completed an assessment of the expectations of individuals with respect to the purposes for which their PI is being collected, used, and disclosed?

i) Have you completed an assessment of the expectations of individuals with respect to the type of consent that is appropriate based on the nature of information being collected, used, and disclosed?

j) Have the privacy and security policies and procedures of the organization been aligned with these expectations to the extent possible? Consent

k) Are the procedures implemented to enable individuals to consent and to withhold or withdraw such consent easy to access and use?

l) Have mechanisms been implemented to manage individual consent, including the decision to withhold or withdraw such consent?

ตารางที่ ๖.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีรวมไปถึงเหตุผลและประโยชน์

หลักการพีบีที	แนวปฏิบัติพีบีที	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
1) การป้องกันและคาดการณ์ที่จะเกิดการรุกรานด้านไพรเวซี	<p>a) มีบุคคลได้รับมอบหมายให้ทำหน้าที่รับผิดชอบในการพัฒนา บำรุงรักษา และดำเนินการเรื่องสารสนเทศด้านไพรเวซีขององค์กร และดำเนินการป้องกันการป้องกันข้อมูลหรือไม่ ?</p> <p>b) มีบุคคลได้รับมอบหมายให้หน้าที่รับผิดชอบในการพัฒนา การบำรุงรักษา และได้มีการนำดำเนินการด้านความมั่นคงสารสนเทศภายในองค์กร ?</p> <p>c) ผู้บริหารมีความมุ่งมั่นเพื่อให้เกิดความต่อเนื่องในการกำหนดและบังคับใช้มาตรฐานด้านไพรเวซีและความมั่นคงในระดับสากล ?</p> <p>d) มีความมุ่งมั่นที่แสดงให้เห็นว่าได้รับความร่วมมือจากกลุ่มผู้ใช้งานและผู้มีส่วนได้ส่วนเสีย ?</p>	<p>เพื่อให้คลังสารสนเทศกลางดำเนินการกำหนดผู้ที่ทำหน้าที่รับผิดชอบด้านการบำรุงรักษา ป้องกันข้อมูลและดูแลสารสนเทศด้านไพรเวซีขององค์กร</p> <p>เพื่อให้คลังสารสนเทศกลางดำเนินการกำหนดผู้ที่ทำหน้าที่รับผิดชอบด้านการบำรุงรักษา และดำเนินการด้านความมั่นคงสารสนเทศภายในองค์กร</p> <p>เนื่องจากยังไม่ได้กำหนดทีมผู้บริหารชัดเจน</p> <p>ผู้ใช้งานและผู้มีส่วนได้ส่วนเสียได้เห็นถึงความสำคัญของการมีข้อมูลร่วมกัน</p>	<p>ช่วยให้คลังสารสนเทศกลางมีเจ้าหน้าที่ดูแลรับผิดชอบด้านการปกครององค์กรอย่างชัดเจน</p> <p>ช่วยให้คลังสารสนเทศกลางมีเจ้าหน้าที่ดูแลรับผิดชอบด้านการปกครองด้านความรู้รักษา และดำเนินการด้านความมั่นคงสารสนเทศขององค์กรอย่างชัดเจน</p>	<p>๖.1</p> <p>๖.1</p> <p>๖.2</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีที (✓) ไม่มีความเหมาะสมของคำถามพีบีที (✗) ไม่มีความเหมาะสมของคำถามพีบีที (⊙) อยู่ระหว่างพิจารณา

ตารางที่ ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
1) การป้องกันและคาดการณ์ก่อนที่จะเกิดการรุกรานด้านไพรเวจซี	<p>e) มีขั้นตอนเพื่อประเมินใจว่าผู้บริหารและกรรมการบริหารมีบทบาทเรื่องกฎระเบียบ มีการปรับปรุงนโยบายและขั้นตอนการปฏิบัติงานไพรเวจซีและความมั่นคง ?</p> <p>f) มีการตรวจสอบด้านไพรเวจซีและความมั่นคง มีการพัฒนากรอบความรับผิดชอบเพื่อประเมินใจว่ามีการปฏิบัติตามนโยบายด้านไพรเวจซีและความมั่นคง อีกทั้งขั้นตอนเหล่านั้นได้ปฏิบัติตามใช้งานจริงในองค์กร ?</p>	<p>เนื่องจากคลังสารสนเทศกลางไม่ได้ยังไม่ได้กำหนดผู้บริหารชัดเจน</p>	-	
	<p>g) บุคคลที่เกี่ยวข้องที่เข้าถึงข้อมูลส่วนบุคคลจะต้องมีการฝึกอบรมเพื่อรักษาความลับ กลุ่มคนเหล่านี้อาจจะต้องการลงชื่อยอมรับแต่ต้องกรอกกำหนดเช่นทุก 1 ปี ?</p>	<p>เนื่องจากคลังสารสนเทศกลางมีข้อมูลจากหลายหน่วยงาน จำเป็นจะต้องมีการ ลงทะเบียนและบันทึกการใช้งานข้อมูล</p>	<p>มีความปลอดภัยในการใช้งาน</p>	<p>ง.3,ง.4</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของค่าตามพีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (☉) นำมาประยุกต์ใช้ในองค์กร, (☑) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีทีพีไอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีดี	แนวปฏิบัติพีทีพีไอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
1) การป้องกันและคาดการณ์ก่อนที่จะเกิดการรุกรานด้านไพรเวซี	<p>k) ได้มีการกำหนดช่วงเวลาสำหรับทบทวนนโยบายไพรเวซีและนโยบายความมั่นคงและขั้นตอนปฏิบัติเพื่อปรับปรุงนโยบายไพรเวซีและนโยบายความมั่นคงให้ได้มาตรฐานสากลและทันต่อการเปลี่ยนแปลงของกฎหมาย?</p> <p>l) ได้มีการดำเนินการปฏิบัติตามกรอบการบริหารจัดการความเสี่ยงขององค์กร ?</p> <p>m) มีแผนงานโครงการสำหรับการพัฒนาหรือการรีไซเคิล เทคโนโลยีสารสนเทศ การดำเนินการทางธุรกิจ และการออกแบบเชิงกายภาพและเครือข่ายโครงสร้างพื้นฐาน รวมไปถึงการกำหนดจุดประเมินแผนงาน ก่อนที่ดำเนินการขั้นตอนต่อไปของการพัฒนาหรือการรีไซเคิล ?</p>	<p>เพื่อให้คลังสารสนเทศกำหนดช่วงเวลาในการทบทวนปรับปรุงนโยบายด้านไพรเวซีและความมั่นคงตามมาตรฐานสากลและการเปลี่ยนแปลงด้านกฎหมาย</p> <p>เนื่องจากคลังสารสนเทศกลางขาดทรัพยากรบุคคลเพื่อดำเนินการ</p> <p>เพื่อให้คลังสารสนเทศมีแผนงานและช่วงเวลาในการพิจารณากระบวนการดำเนินงานรวมถึงสถาปัตยกรรมของคลังสารสนเทศกลาง</p>	<p>เพื่อให้คลังสารสนเทศกลางมีนโยบายที่มีความเป็นสากลและเป็นปัจจุบัน</p>	<p>ง.26</p> <p>ง.27</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีทีพีไอ (✖) ไม่ผ่านมาตรฐานที่ใช้ในองค์กร, (✓) ผ่านมาตรฐานที่ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
1) การป้องกันและคาดการณ์ก่อนที่จะเกิดการรุกรานด้านไพรเวซี	ก) มีการประเมินผลกระทบด้านไพรเวซี (PIA) ในระดับแนวคิด การออกแบบ ตรรกะ และ ขั้นตอนการรีไซเคิลแอปพลิเคชัน ? o) มีการทบทวนและการอนุมัติการประเมินผลกระทบด้านไพรเวซี (PIA) โดยผู้บริหารระดับสูงในองค์กร ? p) มีการลดความเสี่ยงที่ระบุได้ใน การประเมินผลกระทบด้านไพรเวซี(PIA) ในขอบเขตที่เป็นไปได้ ? q) การทบทวนการประเมินด้านไพรเวซี (PIA) เพื่อแน่ใจว่ามีความต่อเนื่องของความถูกต้องสอดคล้องกับการปฏิบัติในองค์กร และเพื่อให้แน่ใจว่าคำแนะนำต่างๆที่ได้รับนั้นได้มีการดำเนินการแล้วในองค์กร ?	คลังสารสนเทศกลางไม่ได้ดำเนินการในส่วนนี้ เนื่องจากขาดผู้มีความรู้ด้านนี้ - คลังสารสนเทศกลางไม่ได้ดำเนินการในส่วนนี้ เนื่องจากขาดผู้มีความรู้ด้านนี้ - คลังสารสนเทศกลางไม่ได้ดำเนินการในส่วนนี้ เนื่องจากขาดผู้มีความรู้ด้านนี้ - คลังสารสนเทศกลางไม่ได้ดำเนินการในส่วนนี้ เนื่องจากขาดผู้มีความรู้ด้านนี้ -	-	

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติการที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติการพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
1) การป้องกันและคาดการณ์ก่อนที่จะเกิดการรุกรานด้านไพรเวซี	r) มีการสร้างขั้นตอนที่เป็นมาตรฐานเพื่อระบุก่อนการเกิดขึ้นของปัญหาที่มาจากกรอกแอกแบบด้านไพรเวซีที่ไม่ดีพอ ? s) ได้มีการดำเนินการอบรมเพื่อให้เกิดการตระหนักถึงเรื่องความมั่นคงและไพรเวซี ?	เพื่อให้คลังสารสนเทศกำหนดแผนงานเพื่อตรวจสอบการออกแบบด้านไพรเวซีที่ใช้งานอยู่ในปัจจุบัน เพื่อให้ผู้ที่เกี่ยวข้องกับคลังสารสนเทศกลางได้ทราบถึงขั้นตอนการทำงาน และเข้าใจถึงบทบาทผู้ใช้งานในคลังสารสนเทศกลาง	ทำให้คลังสารสนเทศกลางมีขั้นตอนการตรวจสอบก่อนปัญหาด้านการออกแบที่เมติพอจะเกิดขึ้น ช่วยให้ผู้ใช้งานมีความเข้าใจในการใช้งานเครื่องมือรวมถึงบทบาทที่ได้รับ	ง.28 ง.7,ง.8
	t) พนักงาน อาสมัคร ผู้รับเหมาทุกคนที่สามารถเข้าถึงข้อมูลส่วนบุคคลต้องรับการอบรมเรื่องไพรเวซีและความมั่นคงก่อนการเข้าถึงข้อมูลส่วนบุคคล ?	เพื่อคลังสารสนเทศกลางมีช่องทางสื่อสาร อบรมกับผู้มีส่วนเกี่ยวข้องกับข้อมูลในคลังสารสนเทศกลาง	เพื่อสร้างความเข้าใจที่ถูกต้องในการใช้งานข้อมูลในคลังสารสนเทศกลาง	ง.7,ง.8

สัญลักษณ์ : ผลการพิจารณาของคำถามพีบีทีพีเอ (✗) ไม่น่ามาประยุกต์ใช้ในองค์กร, (✓) น่ามาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีไอเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีไอเอ		เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
1) การป้องกันและคาดการณ์ก่อนที่จะเกิดการรุกรานด้านไซเบอร์	u) พนักงาน อาสาสมัคร ผู้รับเหมาทุกคนที่สามารถเข้าถึงข้อมูลส่วนบุคคลจะต้องรับการอบรมตามบทบาทที่ได้รับเพื่อทำความเข้าใจนโยบายความเป็นส่วนตัวมั่นคงและขั้นตอนปฏิบัติในองค์กรเพื่อใช้ในการทำงานตามสัญญาจ้างงานหรืองานอื่นที่รับผิดชอบ ?	✓	เพื่อให้คลังสารสนเทศกลางได้อบรมให้ผู้มีส่วนเกี่ยวข้องรับรู้อุทิสตามบทบาทที่ได้รับ	ผู้ใช้งานได้รับทราบสิทธิตามบทบาทที่ได้รับในการใช้งานข้อมูลที่อยู่ในคลังสารสนเทศกลาง	ง.7,ง.8
	v) พนักงาน อาสาสมัคร ผู้รับเหมาทุกคนที่สามารถเข้าถึงข้อมูลส่วนบุคคลจะต้องรับการอบรมความรู้พื้นฐานเช่นปีละหนึ่งครั้ง?	✓	เพื่อให้คลังสารสนเทศกลางกำหนดช่วงเวลาชัดเจนในการอบรมให้กับผู้ที่เกี่ยวข้อง	เพื่อให้คลังสารสนเทศมั่นคงใจได้ว่ามีการอบรมเกี่ยวกับการนำข้อมูลในคลังสารสนเทศกลางไปใช้งาน	ง.7,ง.8
	w) หัวข้ออบรมเรื่องการตระหนักรถึงไซเบอร์เวสและความมั่นคงได้รับการปรับปรุงให้เป็นปัจจุบันและสอดคล้องกับกระบวนการทางธุรกิจหรือกฎหมายที่เปลี่ยนแปลง ?	✓	เพื่อให้คลังสารสนเทศกลางมีการปรับปรุงแก้ไขเนื้อหาการอบรมด้านไซเบอร์เวสและความมั่นคงให้ทันกับกฎหมายที่เปลี่ยนแปลง	บุคคลที่เกี่ยวข้องได้รับเนื้อหาการอบรมที่เป็นปัจจุบันสอดคล้องกับเป้าหมายขององค์กร	ง.7,ง.8

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีไอเอ (✗) ไม่นำมาประยุกต์ใช้เององค์กร, (✓) นำมาประยุกต์ใช้เององค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีดีพีไอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีดี	แนวปฏิบัติพีดีพีไอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
1) การป้องกันและคาดการณ์ก่อนที่จะเกิดการรุกรานด้านไซเบอร์	<p>x) มีการจัดทำนโยบายและขั้นตอนดำเนินการเพื่อตรวจสอบ ประเมิน และทดสอบการปฏิบัติตาม นโยบายไซเบอร์และนโยบายความมั่นคงตามที่เราจะชี้แจงในข้อตกลงหรือตามที่กฎหมายกำหนด ?</p> <p>y) มีกลไกสำหรับการตรวจสอบและรายงานการปฏิบัติตาม นโยบายไซเบอร์และความมั่นคงตามที่ระบุไว้ในข้อตกลงหรือตามกฎหมาย ?</p> <p>z) ได้มีการตรวจสอบด้านไซเบอร์และความมั่นคง ?</p> <p>aa) มีการรักษาความเป็นอิสระของหน่วยงานภายนอกในการตรวจสอบการปฏิบัติตามขององค์กรว่าขัดต่อนโยบายไซเบอร์และความมั่นคง ?</p>	<p>เพื่อให้เกิดการตรวจสอบ ประเมิน คลังสารสนเทศว่าได้ปฏิบัติตามนโยบายที่กำหนดไว้หรือไม่</p> <p>เพื่อให้คลังสารสนเทศกลางมีกลไกในการตรวจสอบ และรายงานการปฏิบัติตามนโยบายที่กำหนดไว้</p> <p>เพื่อให้คลังสารสนเทศกลางได้รับการตรวจสอบด้านไซเบอร์และความมั่นคง</p> <p>คลังสารสนเทศกลางไม่ได้ดำเนินการในส่วนนี้เนื่องจากไม่มีหน่วยงานภายนอกที่ทำหน้าที่</p>	<p>มีการตรวจสอบว่าได้ปฏิบัติตามคลังสิ่งที่กำหนดไว้ และทวนสอบขั้นตอนเพื่อปรับปรุงต่อไป</p> <p>คลังสารสนเทศกลางมีกลไกที่ชัดเจนในการรายงาน และการตรวจสอบการปฏิบัติตามนโยบาย</p> <p>เพื่อให้การดำเนินงานของคลังสารสนเทศมีมาตรฐานพร้อมสำหรับการตรวจสอบอยู่เสมอ</p> <p>-</p>	<p>ง.29</p> <p>ง.29</p> <p>ง.30</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีดีพีไอ (x) ไม่นำมาประยุกต์ใช้ในองค์กร, (y) นำมาประยุกต์ใช้ในองค์กร, (z) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่	
1) การป้องกันและลดการก่อมลพิษก่อนที่จะเกิดการรุกรานด้านโพรวเรซี	bb) มีขั้นตอนสำหรับตรวจสอบว่าคำแนะนำที่เกิดจากการตรวจสอบด้านโพรวเรซีและความมั่นคง ได้รับการนำไปพิจารณาปรับปรุง?	✗	คลังสารสนเทศกลางไม่ได้ดำเนินการในส่วนนี้เนื่องจากไม่มีหน่วยงานภายนอกที่ทำหน้าที่นี้	-	
2) โพรวเรซีจะได้รับการปกป้องตั้งแต่เริ่มต้นใช้งาน แม้ไม่มีการกำหนดโดยผู้ใช้งาน	a) มีการออกแบบเทคโนโลยีสารสนเทศ กระบวนการทางธุรกิจ พื้นที่ทางกายภาพ และเครือข่ายพื้นฐานโดยใช้หลักการการเก็บน้อยที่สุดทั้งสำหรับการระบุตัวตน ตรวจสอบการเชื่อมต่อข้อมูลส่วนบุคคลอย่างเข้มงวด?	✓	เพื่อให้คลังสารสนเทศสามารถระบุข้อมูลได้บ้างที่นำไปใช้งาน เชื่อมต่อจากคลังสารสนเทศกลาง	-	
	b) ความมั่นใจว่าวัตถุประสงค์ที่กำหนดขึ้นมีความชัดเจน มีการกำหนดขอบเขต และมีความเกี่ยวข้องกับสถานการณ์ที่เกิดขึ้นในการจัดเก็บการนำไปใช้และการเปิดเผยข้อมูลส่วนบุคคล?	✓	เพื่อให้คลังสารสนเทศกลางมีขอบเขตของวัตถุประสงค์ในจัดเก็บข้อมูลที่ชัดเจน	สร้างความเชื่อมั่นให้กับคลังสารสนเทศกลางว่าได้ปฏิบัติตามขอบเขตที่ระบุไว้ในวัตถุประสงค์	ง.31
					ง.32

สัญลักษณ์ : ผลการพิจารณาของคํากฎหมายพีบีทีพีเอ (✗) ไม่นำมาประยุกต์ใช้เองครั้ง, (✓) นำมาประยุกต์ใช้เองครั้ง, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
2) ใครจะได้รับการปกป้องตั้งแต่เริ่มต้นใช้งาน แม้ไม่มีการกำหนดโดยผู้ใช้งาน	<p>c) มั่นใจได้ว่าข้อมูลส่วนบุคคลที่เก็บรวบรวม นำไปใช้งาน และเปิดเผยนั้นเป็นไปตามวัตถุประสงค์ที่กำหนด ?</p> <p>d) มีการเก็บรวบรวม ใช้ข้อมูลเปิดเผยข้อมูลส่วนบุคคลก็ต่อเมื่อข้อมูลในส่วนอื่นไม่ได้เป็นไปตามวัตถุประสงค์ ?</p> <p>e) มีการพัฒนานโยบายและขั้นตอนการทำงานที่กำหนดให้มีการเข้ารหัสและป้องกันการรวบรวมการระบุตัวตนการเชื่อมต่อ ?</p> <p>f) นโยบายและขั้นตอนการปฏิบัติในองค์กรจะต้องเข้ารหัสข้อมูลส่วนบุคคลที่จัดเก็บ รวบรวม นำไปใช้งาน และเปิดเผยผ่านอุปกรณ์เคลื่อนที่ ?</p>	<p>เพื่อให้คลังสารสนเทศกลางกำหนดขั้นตอนการตรวจสอบกระบวนการดำเนินการว่าเป็นตามวัตถุประสงค์</p> <p>คลังสารสนเทศกลางขอความร่วมมือในการส่งข้อมูลเข้าคลังสารสนเทศกลาง จึงเก็บทุกอย่างที่หน่วยงานส่งมอบให้</p> <p>คลังสารสนเทศกลางขอความร่วมมือในการส่งข้อมูลเข้าคลังสารสนเทศกลาง จึงเก็บทุกอย่างที่หน่วยงานส่งมอบให้</p> <p>คลังสารสนเทศกลางไม่ได้ดำเนินการในส่วนนี้</p>	<p>สร้างความมั่นใจได้ว่าข้อมูลที่จัดเก็บเป็นไปตามข้อกำหนดที่ได้แจ้งกับผู้ใช้งาน</p> <p>-</p> <p>-</p> <p>-</p> <p>-</p>	<p>ง.33</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้เองครั้ง, (✓) นำมาประยุกต์ใช้เองครั้ง, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
2) ใครจะได้รับการปกป้องตั้งแต่เริ่มต้นใช้งาน แม้ไม่มีการกำหนดโดยผู้ใช้งาน	<p>g) มีการเก็บรวบรวม ใช้งาน และเปิดเผยข้อมูลส่วนบุคคลน้อยที่สุดเพื่อให้เป็นไปตาม วัตถุประสงค์ ?</p> <p>h) มีการจัดหมวดหมู่ของข้อมูลส่วนบุคคลซึ่งได้เก็บรวบรวมและมีการทบทวนอย่างต่อเนื่องเพื่อให้แน่ใจว่าการเก็บข้อมูลส่วนบุคคลมีขอบเขตเพื่อให้เป็นไปตามวัตถุประสงค์ในการจัดเก็บ ?</p>	<p>คลังสารสนเทศกลางไม่ได้ดำเนินการในส่วนนี้</p> <p>เพื่อให้คลังสารสนเทศกลางจัดเก็บข้อมูลตามหมวดหมู่และทบทวนตามวัตถุประสงค์การจัดเก็บ</p>	-	
	<p>i) ข้อมูลส่วนบุคคลที่จัดเก็บมีความเป็นธรรมและเป็นไปตามวัตถุประสงค์หรือตามที่กฎหมายกำหนด ?</p>	<p>เพื่อให้คลังสารสนเทศเก็บและแบ่งปัน เฉพาะข้อมูลที่หน่วยงานในคลังสารสนเทศกลางเห็นชอบเท่านั้น</p>	<p>ฝ่ายจัดการบริหารจัดการทบทวนเมื่อจัดเก็บข้อมูลตามหมวดหมู่</p>	ง.21
	<p>j) มีขั้นตอนวิธีตรวจสอบการเข้าถึงข้อมูลที่มิได้ระบุตัวตนก่อนที่จะมีการใช้งานข้อมูลหรือเปิดเผยข้อมูล ?</p>	<p>การเข้าถึงข้อมูลในคลังสารสนเทศจำเป็นต้องระบุตัวตนก่อนใช้งานข้อมูล</p>	-	ง.33

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้เององค์กร, (☉) นำมาประยุกต์ใช้เององค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
2) เพรเวซีซีได้รับการปกป้องตั้งแต่เริ่มต้นใช้งาน แม้ไม่มีการกำหนดโดยผู้ใช้งาน	<p>k) ได้มีการนำหลักการเข้าถึงตามบทบาทมาใช้งานโดยอยู่บนฐาน 'จำเป็นต่อรู้' และ 'สิทธิพื้นฐาน' ?</p> <p>l) มีขั้นตอนที่ทำให้แน่ใจว่าเมื่อผู้ใช้มีการกำหนดค่าใดๆ ในการป้องกันภาวะส่วนตัว ข้อมูลของผู้ใช้งานยังคงได้รับการปกป้อง ?</p>	<p>เพื่อให้คลังสารสนเทศกลางกำหนดบทบาทที่ชัดเจนในการเข้าถึงข้อมูล</p> <p>เพื่อให้คลังสารสนเทศกลางกำหนดรายการปกป้องเพรเวซีซีข้อมูลพื้นฐาน</p>	<p>เพื่อเป็นการป้องกันการเข้าถึงข้อมูล จำเป็นต้องกำหนดบทบาทและสิทธิการเข้าถึง</p>	<p>ง.9,ง.11</p> <p>ง.10</p>
3) เพรเวซีซีถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินกิจกรรมในองค์กร	<p>a) ได้มีการจัดทำโปรแกรมเพรเวซีซีและความมั่นคง เกี่ยวข้องนโยบายและกระบวนการเป็นไปตามมาตรฐานระดับอุตสาหกรรม โมเดล วิธีปฏิบัติที่เป็นเลิศหรือตามที่ถูกหมายกำหนด ?</p> <p>b) ได้มีการดำเนินการควบคุม พัฒนา เพรเวซีซีและความมั่นคงสอดคล้องกับลักษณะข้อมูลเพื่อป้องกันการคุกคามการสูญเสีย การเข้าถึงโดยไม่รับอนุญาต หรือเปิดเผยข้อมูล?</p>	<p>-</p> <p>เพื่อให้คลังสารสนเทศกลางมีการป้องกันและลดความเสี่ยงจากภัยคุกคาม</p>	<p>-</p> <p>ลดความเสี่ยงจากการใช้งานโดยไม่ได้รับอนุญาต</p>	<p>ง.14</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีเอ (✖) ไม่นำมาประยุกต์ใช้ในองค์กร, (✔) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีไอโดยรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีไอเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
3) ไพร์เวซีได้ถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินงานกิจกรรมในองค์กร	<p>c) มีการควบคุมด้านไพร์เวซีและความมั่นคงผ่านการรับรองหรือทบทวนจากหน่วยงานออกองค์กร ?</p> <p>d) ได้มีการจัดทำเอกสารและเปิดเผยสถาปัตยกรรมไพร์เวซีขององค์กร เพื่อให้เกิดการแน่ใจว่าได้สร้างการปกป้องที่สำคัญสำหรับไพร์เวซีโดยถูกบรรจุในขั้นตอนการออกแบบทุกแอปพลิเคชันที่เกี่ยวข้อง และเปิดเผยข้อมูลส่วนบุคคล ? โดยสถาปัตยกรรมไพร์เวซีควรพูดถึง</p> <ul style="list-style-type: none"> ได้บรรจุมาตรฐานการประมวลผลสารสนเทศ (FIPS: Federal Information Processing Standard) ในขั้นตอนการออกแบบแอปพลิเคชัน 	<p>คำสั่งสารสนเทศกลางไม่ได้ดำเนินการในส่วนนี้</p> <p>คำสั่งสารสนเทศกลางดำเนินเพียงบางส่วน เช่น การเปิดเผยสถาปัตยกรรมด้านไพร์เวซีเพื่อความโปร่งใสในการทำงานและสถาปัตยกรรมความมั่นคงในภาพรวมเพื่อรับผลป้อนกลับจากผู้ที่เกี่ยวข้อง โดยรวมไปถึงการบริหารจัดการการเข้าถึงและตรวจสอบย้อนหลังได้</p>	-	

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีไอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีไอเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีไอเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
3) ไพร์เวซีได้ถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินงานกิจกรรมในองค์กร	<ul style="list-style-type: none"> มีการจัดแบ่งระดับข้อมูลอ่อนไหว มีอภิธานศัพท์ที่เกี่ยวข้องกับไพร์เวซีหรือที่ใช้ในเอกสารภายในองค์กร กำหนดข้อจำกัดในการเก็บรวบรวม ใช้งาน และเปิดเผยข้อมูลส่วนบุคคล จำกัดการใช้งาน กำหนดรายการความต้องการเพื่อเข้ารหัสข้อมูล กำหนดกฎในการบริหารจัดการการยินยอม การควบคุมการเข้าถึง การบันทึกการตรวจสอบรายงานและการแจ้งเตือน 	<p>✘</p> <p>✔</p> <p>✘</p> <p>✘</p> <p>✘</p> <p>⊙</p>		ง.15

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีไอเอ (✘) ไม่เหมาะสมยกเว้นในองค์กร, (✔) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
3) โพรเวซึ่ได้ถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินการกิจกรรมในองค์กร	<p>e) จัดทำเอกสารและเผยแพร่สถาปัตยกรรมด้านความมั่นคงเพื่อให้แน่ใจได้มีการสร้างการปกป้อง (การบริหารจัดการ, ทางกายภาพ, และด้านเทคนิค) ทุกแอปพลิเคชันที่เก็บรวบรวม ใช้งาน เปิดเผยแพร่ และรักษาข้อมูลส่วนบุคคล ?</p> <p>f) มีการจัดทำกระบวนการและ/หรือกลไกเพื่อทวนสอบรายการความต้องการด้านสถาปัตยกรรมไอที และความสามารถมีกระบวนการออกแบบอย่างเหมาะสมอยู่ในฟังก์ชันงานของแอปพลิเคชัน ?</p> <p>g) ได้มีการนำเอาหลักการเข้าถึงตามบทบาทมาใช้หรือไม่ ?</p>	<p>คำสั่งสารสนเทศกลางดำเนินการเพียงบางส่วนเช่นการเปิดเผยสถาปัตยกรรมด้านความมั่นคงเพื่อรับส่วนบ่อนักจากผู้เกี่ยวข้อง</p> <p>คำสั่งสารสนเทศกลางยังไม่ได้ดำเนินการในส่วนนี้</p>	<p>แสดงออกถึงการมีส่วนร่วมของผู้มีส่วนเกี่ยวข้อง</p>	<p>ง.31</p>
		<p>เพื่อให้ถ่ายทอดการบริหารจัดการการเข้าถึงและสิทธิ</p>	<p>เกิดความชัดเจนในหน้าที่รับผิดชอบของผู้ที่เกี่ยวข้อง</p>	<p>ง.9</p>

สัญลักษณ์ : ผลการพิจารณาเหมาะสมของค่าตามพีบีทีพีเอ (✖) ไม่เหมาะสมทุกที่ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีไอเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีไอเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
3) ใครเวซี้ได้ถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินงานกิจกรรมในองค์กร	h) ได้มีการกำหนดกระบวนการสำหรับการสื่อสารกับการออกแบบและวิธีที่ชนของระบบไอที กระบวนการดำเนินการทางธุรกิจและการออกแบบทางกายภาพโดยมีการรับฟังความเห็นจากผู้ใช้งานก่อนที่จะมีการดำเนินการ ?	คลังสารสนเทศกลางยังไม่ได้นำดำเนินการในส่วนนี้	-	
	i) มีกระบวนการจัดทำเอกสารและเผยแพร่ให้กับเจ้าหน้าที่ทุกคนในองค์กรที่มีหน้าที่เกี่ยวข้องในการออกแบบและวิธีที่ชนแอปพลิเคชัน ?	เพื่อให้เกิดการเปิดเผยและโปร่งใสในการออกแบบ	เพื่อให้การมีส่วนร่วมในการออกแบบ	
	j) มีการทำการตรวจสอบเพื่อให้แน่ใจว่ากระบวนการในข้อ (i) ได้ดำเนินการอย่างสม่ำเสมอ ?	คาดหวังให้คลังสารสนเทศกลางกำหนดกระบวนการตรวจสอบ		

สัญลักษณ์ : ผลการพิจารณาของความเหมาะสมของคำถามพีบีทีพีไอเอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
3) เพรอวิชได้ถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินงานกิจกรรมในองค์กร	<p>k) กระบวนการออกแบบและริตช์ประกอบด้วย:</p> <ul style="list-style-type: none"> ● มีการปรึกษาหารือในการออกแบบหรือการริตช์ไอทีในแอปพลิเคชันทั้งในภายในและภายนอกองค์กรที่ทำหน้าที่ในการเก็บรวบรวม ใช้งาน หรือการเปิดเผยข้อมูลส่วนบุคคล ? 	<p>คลังสารสนเทศกลางได้ดำเนินการเพียงบางส่วน เช่นการควบคุมการเข้าถึงและการแจ้งสิทธิให้กับผู้ใช้งานได้ทราบ</p>		

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
3) ไพเราะซึ่งได้ถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินงานกิจกรรมในองค์กร	<ul style="list-style-type: none"> มีการทำการประเมินผลกระทบไพเราะซึ่งและการประเมินภัยคุกคามในระดับแนวคิด ภายภาพ ตรรกะและขั้นตอนการรีไซเคิลแอปพลิเคชัน ? มีกระบวนการในจัดการและการระบุความเสี่ยงเช่น การประเมินผลกระทบไพเราะซึ่งและการประเมินภัยคุกคามก่อนที่จะมีการดำเนินการของแอปพลิเคชันที่ระบุ ? 	✘		
		✘		

สัญลักษณ์ : ผลการพิจารณาของความเหมาะสมของคำถามพีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีทีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีทีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
3) ใครเวซี้ได้ถูกฝังอยู่ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินงานกิจกรรมในองค์กร	<ul style="list-style-type: none"> มีรายการความต้องการที่ระบุว่าการใช้ข้อมูลส่วนบุคคลเป็นไปตามวัตถุประสงค์ของแอปพลิเคชัน ? มีการระบุความต้องการด้านไพรเวซีและความมั่นคงเข้าเป็นส่วนหนึ่งของรายการความต้องการในข้อเสนอโครงการที่แอปพลิเคชันนั้นถูกพัฒนาโดยบุคคลภายนอก ? 	<p>✓</p> <p>✗</p>		ง.16

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีทีเอ (✗) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีไอเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีไอเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
3) ใครเว็บไซต์ที่ผู้ปฏิบัติงานสามารถเข้าถึงได้ในขั้นตอนการออกแบบ สถาปัตยกรรมของระบบไอที และการดำเนินงานกิจกรรมในองค์กร	<ul style="list-style-type: none"> มีการควบคุมการเข้าถึงและระบุรายการความต้องการเพื่อการระบุตัวตนของบุคคลที่เข้าถึงข้อมูลส่วนบุคคลและมีกลไกตรวจสอบการเข้าถึง ? สร้างกฎการเข้าถึงข้อมูลส่วนบุคคลนั้นบนพื้นฐานของ 'จำเป็นต้องรู้' และ 'ต้องมิติธิ' และควบคุมจำกัดการเข้าถึง ? ต้องมีการบังคับให้มีการตั้งรหัสผ่านที่ยากต่อการเดา รวมไปถึงมีการกำหนดขนาดความยาวอย่างน้อยเท่าไร ? 	<p>✓</p> <p>✓</p> <p>✓</p>		<p>ง.17</p> <p>ง.9</p> <p>ง.12,ง.13</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของค่าตามพีบีทีพีไอเอ (✗) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีไอเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีไอเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
	1) ได้มีการพัฒนา ดำเนินการด้านนโยบายไปรษณีย์และควมมั่นคงเพื่อแจ้งให้รับทราบการออกแบไปเอทีและขั้นตอนดำเนินการทางธุรกิจ ?			
4) ให้ความสำคัญกับกฎระเบียบและวัตถุประสงค์โดยพิจารณาทั้งเรื่องไปรษณีย์และควมมั่นคง	<p>a) ได้มีการกำหนด จัดทำเอกสาร และเผยแพร่เหล่านี้ให้รับทราบทั้งองค์กรดังนี้</p> <ul style="list-style-type: none"> - ทุกอย่างที่ใช้ใช้งานสนใจเกี่ยวข้องกับไปรษณีย์ ข้อมูลควมลับ และควมมั่นคงของ ข้อมูลส่วนบุคคล ? 	เพื่อให้คลังสารสนเทศเกิดความโปร่งใสโดยเผยแพร่เอกสารให้หน่วยงานและผู้ใช้งานได้รับทราบ	เกิดความโปร่งใสในการดำเนินการและการบริหารจัดการข้อมูลที่อยู่ในคลังสารสนเทศกลาง	ง.5
	<ul style="list-style-type: none"> - ทุกกระบวนการทางธุรกิจที่สนใจ แร่งพลัดต้น และวัตถุประสงค์ ? - พึ่งพิงงานทางธุรกิจ ? - ความต้องการไปรษณีย์เชิงหน้าที่ ? - ความต้องการควมมั่นคงเชิงหน้าที่ ? 			<p>ง.5,ง.6</p> <p>ง.5,ง.6</p> <p>ง.5,ง.6</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีไอเอ (✗) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
4) ให้ความสำคัญกับกฎระเบียบและวัตถุประสงค์โดยพิจารณาทั้งเรื่องไพรเวซีและความมั่นคง	b) กำหนดโครงสร้างและกลไกเมื่อหน่วยงานภายนอกต้องการเข้าถึงข้อมูลอาจจะต้องนำเข้าสู่ที่ประชุมหารือ เพื่อให้มั่นใจได้ว่าไม่มีการแยกฟังก์ชันหน้าที่ของไพรเวซีออกจากความมั่นคง ?	เพื่อให้คลังสารสนเทศกลางมีมาตรฐานในการให้บริการข้อมูลกับหน่วยงานอื่น	คลังสารสนเทศกลางมีหลักการขอบเขตชัดเจนในการให้บริการข้อมูลกับหน่วยงานโดยพิจารณาจากเรื่องไพรเวซีและความมั่นคง	ง.34
	c) ได้มีการพัฒนาตัวชี้วัดและการประเมินว่าผลประโยชน์ที่ได้รับและวัตถุประสงค์ตรงกัน ?	เพื่อให้คลังสารสนเทศกลางได้มีวัตถุประสงค์ที่ชัดเจน	เกิดความโปร่งใสในการดำเนินงาน เพื่อให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้	ง.35
	d) ได้มีการปฏิเสธข้อเสนอแนะที่ได้จากการประเมินความเสี่ยงที่มีผลลัพธ์ให้มีการแยกฟังก์ชันกันระหว่างไพรเวซีและความมั่นคง ?	เพื่อให้คลังสารสนเทศกลางไม่แบ่งแยกฟังก์ชันงานของไพรเวซีและความมั่นคง	เกิดความมั่นใจว่าคลังสารสนเทศกลางรักษาไพรเวซีและความมั่นคงควบคู่กันไป	
	e) ได้มีการพิจารณาคำแนะนำเพื่อลดความเสี่ยงสอดคล้องกับหลักการพีบีที ?	เพื่อให้คลังสารสนเทศกลางใช้หลักการในระดับสากล	คลังสารสนเทศกลางใช้หลักการที่รับการพัฒนาในระดับสากล	

สัญลักษณ์ : ผลการพิจารณาเหมาะสมของคำถามพีบีทีพีเอ (✗) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีดีพีไอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีดี	แนวปฏิบัติพีดีไอเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่	
4) ให้ความสำคัญกับกระบวนการและวัตถุประสงค์โดยพิจารณาทั้งเรื่องไพรเวจี้และความมั่นคง	f) แอปพลิเคชันที่พัฒนาขึ้นบรรลุผล ประโยชน์และวัตถุประสงค์ตามที่กำหนด ?	✓	เพื่อให้เกิดการตรวจสอบว่า ประโยชน์ของการเชื่อมโยงข้อมูล กับวัตถุประสงค์ขององค์กร สารสนเทศสอดคล้องกัน	เกิดการทำงานสอดคล้องกัน และวัตถุประสงค์ที่กำหนด ผลลัพธ์ที่ได้จะนำไปสู่การ พัฒนาต่อไป	ง.16
5) มีการปกป้องข้อมูลส่วนบุคคลตั้งแต่เริ่มกิจกรรมสิ้นสุดกิจกรรมของข้อมูล	a) ได้มีการแสดงให้เห็นถึงกระบวนการทั้งหมดของการเก็บ การเปิดเผย และการทำลายข้อมูลส่วนบุคคล ? b) ได้ทำการวิเคราะห์ข้อมูลก่อนไหม ? c) ได้มีการประเมินความเสี่ยงด้านความมั่นคงทั้งในด้านกายภาพและด้านเทคนิคโดยได้ทำทุกกระบวนการในโครงการ ? d) มีการกำหนดการป้องกันทุกจุดที่สามารถเข้าถึงข้อมูลส่วนบุคคล ?	✓	เพื่อให้คลังสารสนเทศได้แสดงถึง กระบวนการทั้งหมดตั้งแต่ได้รับ ข้อมูลจากหน่วยงาน	เพื่อปรับปรุงข้อมูลก่อนไหม ให้อยู่ในรูปแบบเดียวกันเพื่อ ใช้ในการวิเคราะห์ต่อไป	ง.19
		✗	เพื่อคลังสารสนเทศกลางได้ทำการ วิเคราะห์ข้อมูลทั้งหมดที่ได้รับมา จากหน่วยงาน	-	ง.36
		✓	คลังสารสนเทศกลางยังไม่ได้ ดำเนินการในส่วนนี้		
		✓	เพื่อสร้างความมั่นคงในการใช้งาน	สร้างความเชื่อมั่นต่อผู้ใช้งาน	

สัญลักษณ์ : ผลการพิจารณาของคำถามพีดีพีไอเอ (✗) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
5) มีการปกป้องข้อมูลส่วนบุคคลตั้งแต่เริ่มกิจกรรมจนถึงสิ้นสุดกิจกรรมของข้อมูล	<p>e) ได้มีการกำหนดบุคคลเพื่อทำหน้าที่ในการประเมินความเสี่ยงเพื่อลดความเสี่ยงที่จะเกิดขึ้นในระดับกายภาพและทางด้านเทคนิค ?</p> <p>f) ได้มีการดำเนินการบริหารจัดการทั้งทางเทคนิคและทางกายภาพเพื่อป้องกันอย่างสมเหตุสมผลแล้วแต่กรณี ?</p> <p>การปกป้องเหล่านี้คือ:</p> <ul style="list-style-type: none"> • อ้างอิงตามมาตรฐานการยอมรับในระดับอุตสาหกรรม <p>กรอบการทำงาน แบบจำลองวิธีปฏิบัติที่เป็นเลิศ และแนวทางการปฏิบัติสำหรับความมั่นคง และสอดคล้องกับกฎหมาย</p>	<p>คำสั่งสารสนเทศกลางยังไม่ได้นำดำเนินการในส่วนนี้</p> <p>เพื่อให้คลังสารสนเทศกลางได้ศึกษาและพัฒนาตามหลักสากลทั้งทางด้านเทคนิคที่ดำเนินการ</p>	-	

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (✔) นำมาประยุกต์ใช้ในองค์กร, (◎) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
5) มีการปกป้องข้อมูลส่วนบุคคลตั้งแต่เริ่มกิจกรรมจนถึงสิ้นสุดกิจกรรมของข้อมูล	<ul style="list-style-type: none"> • บนพื้นฐานของกลยุทธ์การปกป้องในเชิงลึกเพื่อระงับภัยคุกคามและความเสี่ยง • เปรียบเทียบสัดส่วนปริมาณและข้อมูลอ่อนไหวส่วนบุคคลกับจำนวนและการเข้าถึงข้อมูลส่วนบุคคล ? 	<p>☉</p> <p>✘</p>		
	<p>g) มีการบริหารจัดการ เทคนิค และการป้องกันเชิงกายภาพ เพื่อให้แน่ใจว่ามีความปลอดภัยในการเก็บ การเคลื่อนย้าย และการทำลายข้อมูลส่วนบุคคล ?</p>	<p>✓</p> <p>เพื่อให้มีการกำหนดขั้นตอนที่ชัดเจนในการเก็บ เคลื่อนย้าย และทำลายข้อมูลในคลังสารสนเทศกลาง</p>	<p>มีหลักการปฏิบัติชัดเจนเพื่อป้องกันความผิดพลาดในการเก็บ เคลื่อนย้าย ทำลายข้อมูล</p>	<p>ง.36</p>
	<p>h) มีความแน่ใจว่าผู้มีส่วนเกี่ยวข้องและผู้บุคคลที่สามเห็นชอบภาระหน้าที่ เพื่อให้เกิดการป้องกันและการควบคุมความมั่นคงที่ควรจะเป็น ?</p>	<p>✓</p> <p>เพื่อให้คลังสารสนเทศกลางที่กำหนด ภา ร ะ หน้ า ที่ ความรับผิดชอบของผู้เกี่ยวข้องสามารถควบคุมความมั่นคงได้</p>	<p>มีการกำหนดขอบเขตหน้าที่อย่างชัดเจนของผู้เกี่ยวข้อง</p>	<p>ง.36</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของค่าตามพีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (☉) นำมาประยุกต์ใช้ในองค์กร, (☺) อยู่ระหว่างพิจารณา

ตาราง ๑.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
5) มีการปกป้องข้อมูลส่วนบุคคลตั้งแต่เริ่มกิจกรรมจนถึงสิ้นสุดกิจกรรมของข้อมูล	<p>i) องค์กรได้ทำการประเมินการควบคุมความมั่นคงผ่านวงจรชีวิตข้อมูลส่วนบุคคล เพื่อมั่นใจได้ว่าข้อมูลส่วนบุคคลถูกเก็บเป็นความลับ มีความสมบูรณ์ และพร้อมใช้งาน ?</p> <p>j) ได้มีการกำหนดตารางเวลาในการเก็บรักษาและมีขั้นตอนการทำลายข้อมูลส่วนบุคคล ?</p> <p>k) ตารางเวลามีรายละเอียดเหล่านี้คือ:</p> <ul style="list-style-type: none"> ● มีการกำหนดช่วงเวลาของกลุ่มข้อมูลที่เก็บรักษา ? ● มีค่าใช้จ่ายถึงเหตุผลการเก็บรักษาข้อมูลตามช่วงเวลาต่างกัน ? ● มีการจัดทำเอกสารเพื่ออธิบายว่าข้อมูลไหนมีระยะเวลาเท่าไรในการเก็บรักษาเพื่อให้เป็นไปตามตารางที่กำหนด ? 	<p>เพื่อให้ความมั่นคงอยู่เสมอ</p> <p>เพื่อให้คลังสารสนเทศกำหนดระยะเวลาข้อมูลที่เกี่ยวข้องได้รับทราบ</p>	-	๑.36
		✘	มีการกำหนดระยะเวลาชัดเจนเพื่อเป็นข้อมูลให้ผู้เกี่ยวข้องได้รับทราบ	๑.18

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้เององค์กร, (✓) นำมาประยุกต์ใช้เององค์กร, (◎) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีดีพีไอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีดี	แนวปฏิบัติพีบีดีพีไอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
5) มีการปกป้องข้อมูลส่วนบุคคลตั้งแต่เริ่มกิจกรรมจนถึงสิ้นสุดกิจกรรมของข้อมูล	<p>1) ขั้นตอนการทำลายข้อมูลส่วนบุคคล:</p> <ul style="list-style-type: none"> ● การทำลายข้อมูลส่วนบุคคลนั้นจะตั้งอยู่ในรูปแบบที่ไม่สามารถกู้คืนมาได้ ? ● ได้กำหนดรูปแบบการทำลายข้อมูลส่วนบุคคลที่องค์กรมีอยู่ ? 	x		
	<ul style="list-style-type: none"> ● แจ้งผู้ใช้งานทราบเมื่อจะมีการทำลายข้อมูลส่วนบุคคลที่อยู่ในอุปกรณ์อิเล็กทรอนิกส์เช่นเครื่องแฟกซ์ก่อนที่จะมีการส่งต่อให้กับซัพพลายเออร์ ? ● จะต้องมีเอกสารรับรองการทำลายซึ่งจะต้องแสดงข้อมูลต่อไปนี้เป็นชื่อข้อมูลทั่วไปของบุคคล วันที่ ข้อมูลของใครที่ถูกทำลาย เหตุผลของการทำลายนั้น ? 	x		

สัญลักษณ์ : ผลการพิจารณาเหมาะสมของคำถามพีบีดีพีไอ (x) ไม่น่ามาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ		เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
6) ความโปร่งใสในการดำเนินกิจกรรมด้านไปรษณีย์ภายในองค์กรตามนโยบายที่ได้กำหนด	a) ได้มีการกำหนดข้อมูลที่ใช้ในการติดต่อสื่อสารของบุคคลในองค์กรที่ทำหน้าที่รับผิดชอบด้านไปรษณีย์และความมั่นคง และเปิดเผยข้อมูลเหล่านี้ให้รับรู้ทั่วองค์กร ? b) ได้มีการจัดทำเอกสารในลักษณะที่เรียกว่า “พับลิสติกซิง” และเขียนด้วยภาษาที่เข้าใจง่ายโดยผู้ที่มีหน้าที่รับผิดชอบด้านนโยบายและขั้นตอนการดำเนินงานภายในองค์กร รวมถึงข้อมูลแจ้งให้ทราบถึงวิธีการเข้าถึงข้อมูลรายละเอียดต่อไป ? c) ได้มีการกำหนดถ้อยแถลงด้านไปรษณีย์และความมั่นคงที่สามารถตรวจสอบได้โดยอิสระ ?	✓	เพื่อให้คลังสารสนเทศมีผู้รับผิดชอบโดยตรงเพื่อเป็นช่องทางในการติดต่อสอบถามจากผู้ที่เกี่ยวข้อง	มีช่องทางในการติดต่อชัดเจน และรับทราบทั่วทั้งองค์กร	ง.1
		✗	คลังสารสนเทศกลางเปิดเผยข้อมูลและรายละเอียดในการดำเนินงานเฉพาะหน่วยงานที่เข้าร่วม แต่จะเปิดเผยเฉพาะข้อมูลที่ไม่กระทบต่อคลังสารสนเทศกลางเท่านั้น	-	
		✗		คลังสารสนเทศกลางยังไม่ได้ดำเนินการในส่วนนี้	

สัญลักษณ์ : ผลการพิจารณาของคำถามพีบีทีพีเอ (✗) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ๖.2 แนวปฏิบัติการที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและผลประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติการพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
6) ความโปร่งใสในการดำเนินงาน กิจกรรมด้านโปรแกรมภายใต้กำหนด องค์การตามนโยบายที่ได้กำหนด	j) ได้มีการจัดทำนโยบายหรือขั้นตอน ปฏิบัติการสำหรับการสอบถาม การรับ เรื่อง เอกสาร การติดตาม และการ ตอบสนองต่อไพรเวซี ?	✓ เพื่อให้ขั้นตอนที่กำหนดเป็น มาตรฐานเดียวกันในองค์กร	-	๖.22
7) ผู้เกี่ยวข้องด้านโปรแกรมจะต้อง สนับสนุนเพื่อให้โปรแกรมผู้ใช้เกิด ประโยชน์สูงสุดต่อผู้ใช้ใช้งาน	a) ได้มีการจัดทำนโยบายและขั้นตอน ปฏิบัติเหล่านี้ ● เพื่อแจ้งให้เจ้าของข้อมูลได้รับทราบ เกี่ยวกับวัตถุประสงค์ก่อนที่จะมี การเก็บรวบรวม ใช้ งาน เคลื่อนย้าย และเปิดเผยข้อมูล ? ● ได้รับการยินยอมของเจ้าของ ข้อมูลในการรวบรวม ใช้ งาน เปิดเผย ซึ่งเป็นตามความ เหมาะสมหรือตามที่กฎหมาย กำหนด ?	✓ เพื่อให้คลังสารสนเทศกลางให้ ความสำคัญกับเจ้าของข้อมูลโดย การแสดงคำร้องขอข้อมูลและ วัตถุประสงค์การใช้ข้อมูลอย่าง ชัดเจนเพื่อให้เจ้าของข้อมูลได้ พิจารณาก่อนการเชื่อมโยง	เพื่อแสดงความโปร่งใสดำ วัตถุประสงค์ของการเชื่อมโยง ข้อมูล โดยหน่วยงานที่ เชื่อมโยงข้อมูลสามารถระบุ หรือเพิกถอนการเปิดเผย ข้อมูลของหน่วยงานได้	๖.23

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีเอ (✓) ไม่นำมาประยุกต์ใช้ในองค์กร, (✗) ไม่นำมาประยุกต์ใช้ในองค์กร, (◎) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
7) ผู้เกี่ยวข้องด้านไปรษณีย์จะต้องสนับสนุนเพื่อให้ไปรษณีย์เกิดประโยชน์สูงสุดต่อผู้ใช้งาน	<ul style="list-style-type: none"> ● สำหรับการเดิมและการบันทึก ซึ่งความยินยอมสำหรับการรวบรวม ใช้งาน และเปิดเผยข้อมูลส่วนบุคคล จะต้องเป็นไปตามที่เจ้าของข้อมูลคาดหวัง และเป็นไปตามกฎหมายกำหนด ? ● เจ้าของข้อมูลสามารถเพิกถอน หรือระงับความยินยอมในการรวบรวม ใช้งาน และการเปิดเผยข้อมูลส่วนบุคคล เว้นแต่กฎหมายกำหนด ? 	✓		ง.23
	<ul style="list-style-type: none"> ● เจ้าของข้อมูลสามารถทำการร้องขอเพื่อเข้าถึงข้อมูลส่วนบุคคลและการแก้ไขข้อมูลถูกต้อง ? ● เพื่อแน่ใจได้ว่าเจ้าของข้อมูลตระหนักถึงทำอย่างไรในร้องเรียนเรื่องไปรษณีย์ ? 	✓		ง.14
	<ul style="list-style-type: none"> ● เจ้าของข้อมูลสามารถทำการร้องขอเพื่อเข้าถึงข้อมูลส่วนบุคคลและการแก้ไขข้อมูลถูกต้อง ? ● เพื่อแน่ใจได้ว่าเจ้าของข้อมูลตระหนักถึงทำอย่างไรในร้องเรียนเรื่องไปรษณีย์ ? 	✗		ง.37

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีเอ (✗) ไม่นำมาประยุกต์ใช้ในองค์กร, (✓) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีไอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีไอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
7) ผู้เกี่ยวข้องด้านโทรเวชจะต้องสนับสนุนเพื่อให้แพรวะซีเกิดประโยชน์สูงสุดต่อผู้ใช้งาน	<ul style="list-style-type: none"> ● เพื่อแน่ใจได้ว่าเจ้าของข้อมูลตระหนักถึงกลไกในการแก้ไข รวมถึงไปถึงวิธีการเข้าถึงการแก้ไขในลำดับต่อไป ? ● เพื่อให้เจ้าของข้อมูลตระหนักถึงวิธีติดต่อสื่อสารกับเจ้าหน้าที่ในองค์กรที่ทำหน้าที่รับผิดชอบด้านโทรเวช ? 	<p>x</p> <p>เพื่อให้คลังสารสนเทศกลางจัดทำนโยบายการใช้งานที่เข้าข่ายเพื่อสื่อสารกับผู้ใช้นโยบายการใช้งานที่เกี่ยวข้อง</p> <p>✓</p> <p>เพื่อให้คลังสารสนเทศกลางพิจารณาถึงความง่ายต่อการใช้งาน</p>		<p>ง.24</p> <p>ง.20</p>
	<p>b) ทุกนโยบาย ขั้นตอนปฏิบัติและข้อมูลข่าวสารเขียนอยู่ภาษาที่เข้าใจง่ายและผู้ใช้งานสามารถเข้าถึงได้โดยง่ายและเข้าถึงได้ทุกเมื่อ ?</p> <p>c) กระบวนการในการเข้าถึงง่ายต่อการใช้ ?</p>	<p>✓</p> <p>เพื่อให้คลังสารสนเทศกลางพิจารณาถึงความง่ายต่อการใช้งาน</p>	<p>เพื่อให้เกิดการสื่อสารกับผู้ใช้งานและหน่วยงานให้เข้าใจตรงกัน ผกานนโยบายการใช้งานที่เขียนในรูปแบบเข้าใจง่าย</p> <p>คาดว่า จะได้รับการยอมรับจากผู้ใช้งาน หรือหน่วยงานที่เกี่ยวข้องใช้งานได้ง่าย</p>	<p>ง.20</p>

สัญลักษณ์ : ผลการพิจารณาความเหมาะสมของคำถามพีบีทีพีไอ (**x**) ไม่นำมาประยุกต์ใช้ในองค์กร, (**✓**) นำมาประยุกต์ใช้ในองค์กร, (**⊙**) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีพีเอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีพีเอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
7) ผู้เกี่ยวข้องด้านไพรเวซีซีจะต้องสนับสนุนเพื่อให้ไพรเวซีซีเกิดประโยชน์สูงสุดต่อผู้ใช้งาน	<p>h) ได้มีการทำการประเมินความคาดหวังของผู้ใช้งานที่มีต่อวัตถุประสงค์กับข้อมูลส่วนบุคคลของผู้ใช้งานก่อนที่จะมีการเก็บรวบรวม ใช้ งาน และเปิดเผย ?</p> <p>i) ได้มีการทำการประเมินความคาดหวังของผู้ใช้งานประเภทของการยินยอมที่เหมาะสมที่จะมีการเก็บรวบรวม ใช้งาน เบ็ดเตล็ด ?</p> <p>j) ได้มีการจัดทำนโยบายไพรเวซีและ ความมั่นคงและกระบวนการขององค์กรที่สอดคล้องกับความคาดหวังเท่าเป็นไปได้ ?</p> <p>k) ได้มีการสร้างกระบวนการเพื่อให้ผู้ใช้งานสามารถเข้าถึงได้ง่ายเพื่อเพิกถอน หรือระงับการยินยอม ?</p>	<p>คลังสารสนเทศกลางไม่ได้ทำในส่วนนี้</p> <p>คลังสารสนเทศกลางไม่ได้ทำในส่วนนี้</p> <p>คลังสารสนเทศกลางไม่ได้ทำในส่วนนี้</p>	-	<p>ง.39</p> <p>ง.14</p>

สัญลักษณ์ : ผลการพิจารณาเหมาะสมของค่าเกณฑ์พีบีทีพีเอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (☉) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ตาราง ง.2 แนวปฏิบัติที่เหมาะสมในแต่ละหลักการของพีบีทีที่เอรวมไปถึงเหตุผลและประโยชน์ (ต่อ)

หลักการพีบีที	แนวปฏิบัติพีบีทีที่เอ	เหตุผล	ประโยชน์ที่ได้รับ	รูปที่
7) ผู้เกี่ยวข้องด้านโปรแกรมเมอร์จะต้องสนับสนุนเพื่อให้โปรแกรมเมอร์สูงสุดได้ใช้งาน	1) ได้มีการสร้างกลไกเพื่อจัดการการยินยอมของผู้ใช้งาน รวมไปถึงการระบุหรือเพิกถอนการยินยอมเหล่านั้น ?	เพื่อให้คลังสารสนเทศกลางสร้างเครื่องมือเพื่อให้หน่วยงานสามารถระบุรับ เพิกถอนการยินยอมเชื่อมโยงข้อมูลได้	เพื่ออำนวยความสะดวกให้กับหน่วยงานที่เชื่อมโยงข้อมูล	ง.14

สัญลักษณ์ : ผลการพิจารณาเหมาะสมของคำถามพีบีทีที่เอ (✘) ไม่นำมาประยุกต์ใช้ในองค์กร, (✔) นำมาประยุกต์ใช้ในองค์กร, (⊙) อยู่ระหว่างพิจารณา

ง.3 ฟังก์ชันงานเครื่องมือสนับสนุนที่อิมพลีเมนต์ตามรายแนวปฏิบัติพีดีพีไอเอ

NHC ค้นหา นโยบายคลัง ทิวารีเอซี ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักสูตรอบรม superadmin (กลุ่ม: SUPER ADMIN) การตั้งค่า

รายการผู้ใช้งาน / ผู้รับผิดชอบนโยบาย / เพิ่มผู้รับผิดชอบนโยบาย

แผนเพิ่มผู้รับผิดชอบนโยบาย

ชื่อผู้รับผิดชอบ* ชื่อผู้รับผิดชอบ

นามสกุล* นามสกุล

ตำแหน่ง* ตำแหน่ง

เบอร์ติดต่อ* 02-1234567 Ext. 890

อีเมล* user@somedoman.com

ประเภทความรับผิดชอบ*

- ✓ รับผิดชอบด้านนโยบาย
- รับผิดชอบด้านโปรแกรมในองค์กร
- รับผิดชอบด้านความมั่นคงในองค์กร

รูปที่ ง.1 การมอบหมายบุคคลให้ทำหน้าที่ด้านต่างๆ

NHC ค้นหา นโยบายคลัง ทิวารีเอซี ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักสูตรอบรม ... superadmin (กลุ่ม: SUPER ADMIN)

หน้าหลัก / อีเมลเอกสารแนบเครื่องส่งสารสนเทศกลาง

อีเมลเอกสารแนบเครื่องส่งสารสนเทศกลาง

ความมุ่งหวังที่แสดงให้เห็นว่าได้รับความร่วมมือจากกลุ่มผู้ใช้งานและมีส่วนได้เสีย

รายละเอียดเอกสาร	อัปโหลด
เอกสารรายละเอียดความร่วมมือจากหน่วยงานภายนอก	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="border: 1px solid #ccc; width: 100px; height: 100px; margin-bottom: 5px;"></div> <div style="font-size: 8px; color: #ccc;">cooperate_outsrc.txt</div> <div style="display: flex; justify-content: space-between; align-items: center;"> cooperate_outs Remove Upload Browse ... </div> </div>

รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด
เอกสารการประชุมรอบความร่วมมือ	meeting_outsrc.txt	📄

บันทึก

รูปที่ ง.2 อัปโหลดเอกสารความมุ่งมั่นว่าได้รับความร่วมมือจากกลุ่มผู้ใช้งานและผู้ส่วนได้เสีย

แผงลงทะเบียนผู้ใช้งาน

ชื่อผู้ใช้งาน

นามสกุล

เบอร์ติดต่อ

หน่วยงานสังกัด

อีเมล

ชื่อผู้ใช้งาน

รหัสผ่าน

ระบุรหัสผ่านอีกครั้ง

ยอมรับข้อตกลงการใช้งาน

รูปที่ ง.3 บุคคลที่เกี่ยวข้องขอมรับข้อตกลงการใช้งาน

NHC ค้นหา นโยบายคลังฯ ทิวารีบีเอซี- ผู้ใช้งานและหน่วยงาน- สถิติและรายงาน- หลักฐานอบรม- เอกสาร superadmin (นาม: SUPER ADMIN)

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารชี้แจงการรักษาความลับข้อมูลในคลังสารสนเทศกลาง

รายละเอียดเอกสาร	อัปโหลด	
ระบุรายละเอียดเอกสาร	<input type="text"/> <input type="button" value="Browse ..."/>	
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด
รายชื่อผู้เกี่ยวข้องกับข้อมูลและการลงชื่อรับทราบเพื่อรักษาความลับ	/data/www/html/hail/project/sites/public/upload/proactive/รายชื่อผู้เซ็น ยอมรับการรักษาข้อมูล.bt	<input checked="" type="checkbox"/>

รูปที่ ง.4 อีพโหลดเอกสารเกี่ยวข้องกับการรักษาความลับในคลังสารสนเทศกลาง

NHC ค้นหา นโยบายคลังฯ ทิวารีบีเอสอี ใช้งานและหน่วยงาน สถิติและรายงาน หลักสตรอบรม เอกสาร superadmin (กลุ่ม: SUPER ADMIN)

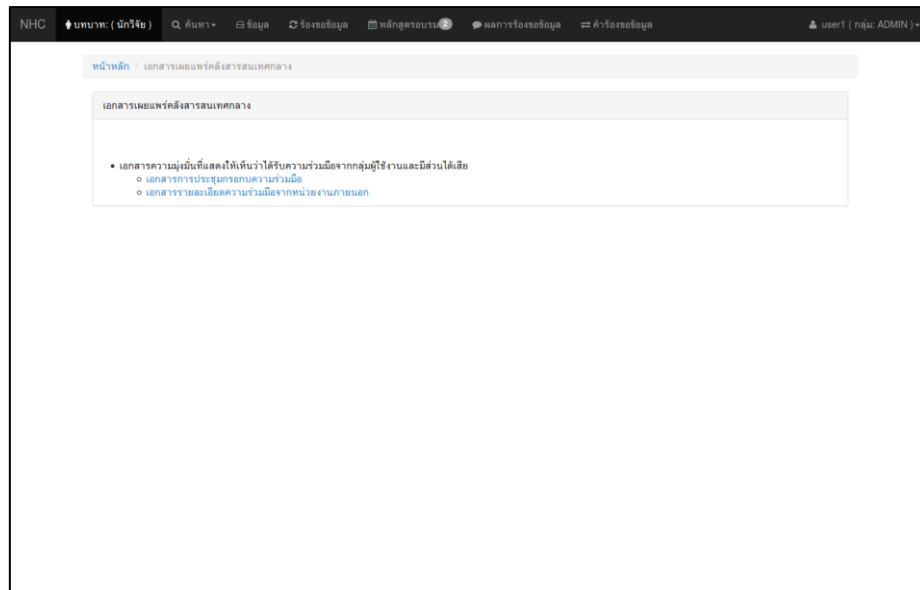
หน้าหลัก / เอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารเผยแพร่คลังสารสนเทศกลาง

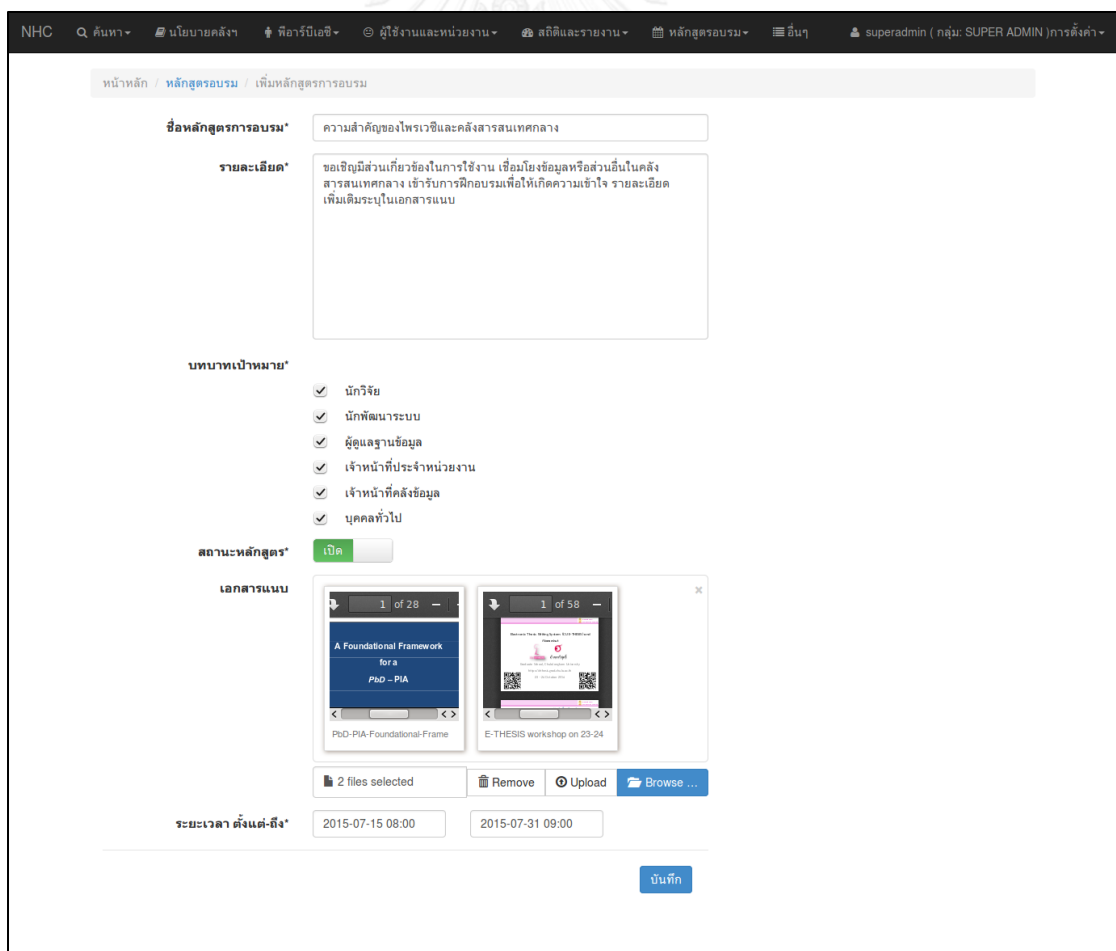
เพิ่มรายการเอกสาร

#	รายการ	อัปเดตไฟล์เอกสาร
1	เอกสารความมุ่งมั่นที่แสดงให้เห็นว่าได้รับความร่วมมือจากกลุ่มผู้ใช้งานและมีส่วนได้เสีย	อัปเดตเอกสาร
2	เอกสารชี้แจงการรักษาความลับข้อมูลในคลังสารสนเทศกลาง	อัปเดตเอกสาร
3	เอกสารขึ้นตอนการรักษาความลับและข้อกำหนดการแบ่งปันข้อมูลคลังสารสนเทศกลาง	อัปเดตเอกสาร
4	เอกสารชี้แจงช่วงเวลากำหนดบทวนนโยบายโทรเวชและความมั่นคงในคลังสารสนเทศกลาง	อัปเดตเอกสาร
5	เอกสารแผนงานโครงการพัฒนา วิดีโอเทคโนโลยีของคลังสารสนเทศกลาง	อัปเดตเอกสาร
6	เอกสารมาตรฐานสำหรับการประเมินการออกแบบด้านโทรเวช	อัปเดตเอกสาร
7	เอกสารขึ้นตอนการดำเนินการประเมินการตรวจสอบการปฏิบัติตามนโยบายโทรเวชและความมั่นคงของคลังสารสนเทศกลาง	อัปเดตเอกสาร
8	เอกสารตรวจสอบด้านโทรเวชและความมั่นคง	อัปเดตเอกสาร
9	เอกสารชี้แจงวัตถุประสงค์การเก็บข้อมูลในคลังสารสนเทศกลาง	อัปเดตเอกสาร
10	เอกสารตรวจสอบการใช้ข้อมูลและวัตถุประสงค์ที่กำหนด	อัปเดตเอกสาร
11	เอกสารการออกแบบและสถาปัตยกรรมเทคโนโลยีสารสนเทศ กระบวนการทางธุรกิจของคลังสารสนเทศกลาง	อัปเดตเอกสาร
12	เอกสารข้อกำหนดการขอใช้งานข้อมูลในคลังสารสนเทศกลางสำหรับบุคคลภายนอก	อัปเดตเอกสาร
13	เอกสารตัวชี้วัดประสิทธิภาพการใช้งานข้อมูลและวัตถุประสงค์ของคลังสารสนเทศกลาง	อัปเดตเอกสาร
14	เอกสารประเมินความเสี่ยง	อัปเดตเอกสาร
15	เอกสารชี้แจงสิทธิเพื่อการเพิกถอน ระบุการใช้งานและเปิดเผยข้อมูลในคลังสารสนเทศกลาง และขึ้นตอนการร้องเรียนด้านโทรเวช	อัปเดตเอกสาร
16	เอกสารประเมินความถูกต้องข้อมูล	อัปเดตเอกสาร
17	เอกสารผลการประเมินความคาดหวังของผู้ใช้ข้อมูลแก่คลังสารสนเทศกลาง	อัปเดตเอกสาร

รูปที่ 5.5 รายการเอกสารที่อัปเดตเพื่อให้ผู้เกี่ยวข้องรับทราบ



รูปที่ ๖.6 รายการเอกสารเผยแพร่ส่วนผู้ใช้งาน



รูปที่ ๖.7 จัดทำหลักสูตรอบรมพร้อมกำหนดกลุ่มผู้รับการอบรม แนบเอกสารคำสั่งการอบรม

NHC | บทบาท: (นักวิจัย) | ค้นหา | ข้อมูล | ร่องขอข้อมูล | หลักสูรอบรม | ผลการร้องขอข้อมูล | คำร้องขอข้อมูล | user1 (กลุ่ม: ADMIN) การตั้งค่า

หน้าหลัก / รายการหลักสูตรอบรม

แผนรายการหลักสูตรอบรม

ค้นหา

ชื่อหลักสูตร	รายละเอียด	ประวัติการเข้าร่วม	สถานะหลักสูตร	ไฟล์แนบ	วันที่สร้าง	วันสิ้นสุด	เข้าร่วม
การใช้งานเบื้องต้น คลังสารสนเทศกลาง ครั้งที่ 2	เนื้อหาการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลาง	เข้าร่วม	เปิด		2014-10-15	2014-12-25	
การใช้งานเบื้องต้น คลังสารสนเทศกลาง	เนื้อหาการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลางการใช้งานเบื้องต้น คลังสารสนเทศกลาง	เข้าร่วม	ปิด		2014-06-11	2014-07-31	
ความสำคัญของโปรเวอีและคลังสารสนเทศกลาง	ขอเชิญมีส่วนร่วมเรื่องในการใช้งาน เชื่อมโยงข้อมูลหรือส่วนอื่นในคลังสารสนเทศกลาง เข้าร่วมการฝึกอบรมเพื่อให้เกิดความเข้าใจ รายละเอียดเพิ่มเติมระบุในเอกสารแนบ	N/A	เปิด	PbD-PIA-Foundational-Framework.pdf E-THESIS workshop on 23-24 Oct 2014.pdf	2015-07-15	2015-07-31	

เข้าร่วม

รูปที่ ๙.8 รายการหัวข้ออบรมพร้อมเอกสารแนบ

NHC | บทบาท: (นักวิจัย) | ค้นหา | ข้อมูล | ร่องขอข้อมูล | หลักสูรอบรม | ผลการร้องขอข้อมูล | คำร้องขอข้อมูล | user1 (กลุ่ม: ADMIN) การตั้งค่า

หน้าหลัก / รายการสิทธิขออนุญาต

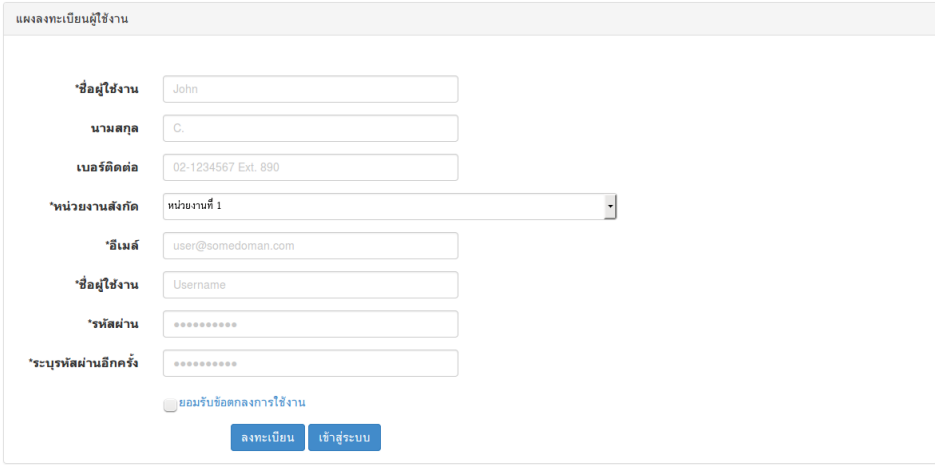
แผนรายละเอียดสิทธิขออนุญาตที่ได้รับ

บทบาท	ข้อมูล	การกระทำ	วัตถุประสงค์	เงื่อนไขการใช้งาน	สิ่งที่ต้องทำก่อน
นักวิจัย	ข้อมูลความรู้	ดาวน์โหลด	เพื่อนวิจัย	ข้อมูลปัจจุบัน	เข้าสู่ระบบก่อน
นักวิจัย	ข้อมูลความรู้	ดาวน์โหลด	เพื่อนวิจัย	ข้อมูลปัจจุบัน	บันทึกประวัติการใช้งานก่อนออกจากระบบ
นักวิจัย	ข้อมูลความรู้	ดาวน์โหลด	เพื่อนวิจัย	ข้อมูลย้อนหลัง 3 วัน	เข้าสู่ระบบก่อน
นักวิจัย	ข้อมูลความรู้	ดาวน์โหลด	เพื่อนวิจัย	ข้อมูลย้อนหลัง 3 วัน	บันทึกประวัติการใช้งานก่อนออกจากระบบ
นักวิจัย	ข้อมูลความรู้	ดาวน์โหลด	เพื่อนวิจัย	ข้อมูลย้อนหลัง 7 วัน	เข้าสู่ระบบก่อน
นักวิจัย	ข้อมูลความรู้	ดาวน์โหลด	เพื่อนวิจัย	ข้อมูลย้อนหลัง 7 วัน	บันทึกประวัติการใช้งานก่อนออกจากระบบ
นักวิจัย	ข้อมูลความรู้	เรียกดูข้อมูล	เพื่อนวิจัย	ข้อมูลปัจจุบัน	เข้าสู่ระบบก่อน
นักวิจัย	ข้อมูลความรู้	เรียกดูข้อมูล	เพื่อนวิจัย	ข้อมูลปัจจุบัน	บันทึกประวัติการใช้งานก่อนออกจากระบบ
นักวิจัย	ข้อมูลความรู้	เรียกดูข้อมูล	เพื่อนวิจัย	ข้อมูลย้อนหลัง 3 วัน	เข้าสู่ระบบก่อน
นักวิจัย	ข้อมูลความรู้	เรียกดูข้อมูล	เพื่อนวิจัย	ข้อมูลย้อนหลัง 3 วัน	บันทึกประวัติการใช้งานก่อนออกจากระบบ
นักวิจัย	ข้อมูลความรู้	เรียกดูข้อมูล	เพื่อนวิจัย	ข้อมูลย้อนหลัง 7 วัน	เข้าสู่ระบบก่อน
นักวิจัย	ข้อมูลความรู้	เรียกดูข้อมูล	เพื่อนวิจัย	ข้อมูลย้อนหลัง 7 วัน	บันทึกประวัติการใช้งานก่อนออกจากระบบ
นักวิจัย	ข้อมูลความรู้	ดาวน์โหลด	เพื่อนวิจัย	ข้อมูลปัจจุบัน	เข้าสู่ระบบก่อน
นักวิจัย	ข้อมูลความรู้	ดาวน์โหลด	เพื่อนวิจัย	ข้อมูลปัจจุบัน	บันทึกประวัติการใช้งานก่อนออกจากระบบ
นักวิจัย	ข้อมูลความรู้	ดาวน์โหลด	เพื่อนวิจัย	ข้อมูลย้อนหลัง 3 วัน	เข้าสู่ระบบก่อน

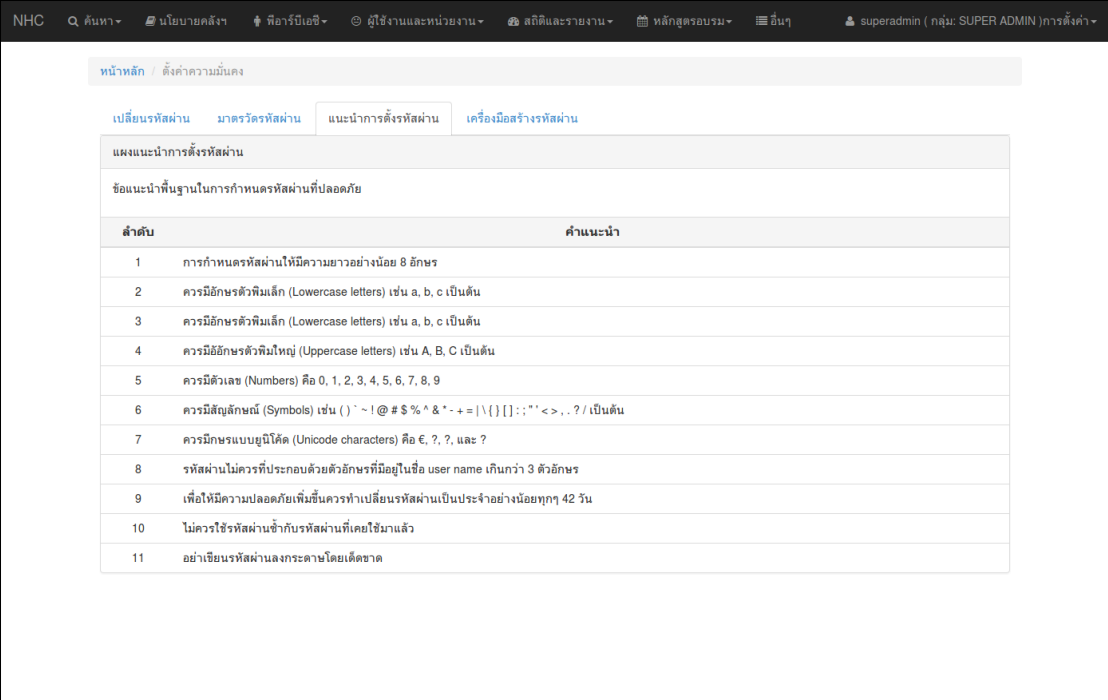
รูปที่ ๙.9 แสดงรายการสิทธิขออนุญาต ขอบเขตการใช้งาน

รูปที่ ง.10 กำหนดโปรเวซีค่าเริ่มต้นสำหรับใช้งานคลังสารสนเทศกลาง

รูปที่ ง.11 กำหนดบทบาทให้กับผู้ใช้งาน

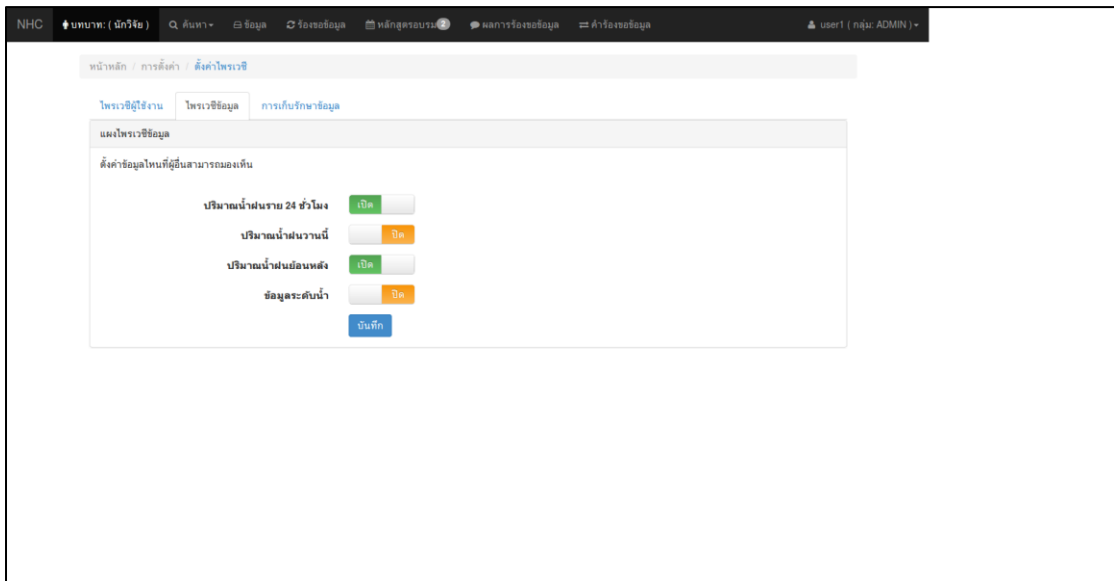


รูปที่ ง.12 การสร้างรหัสผ่านที่ยากต่อการคาดเดา

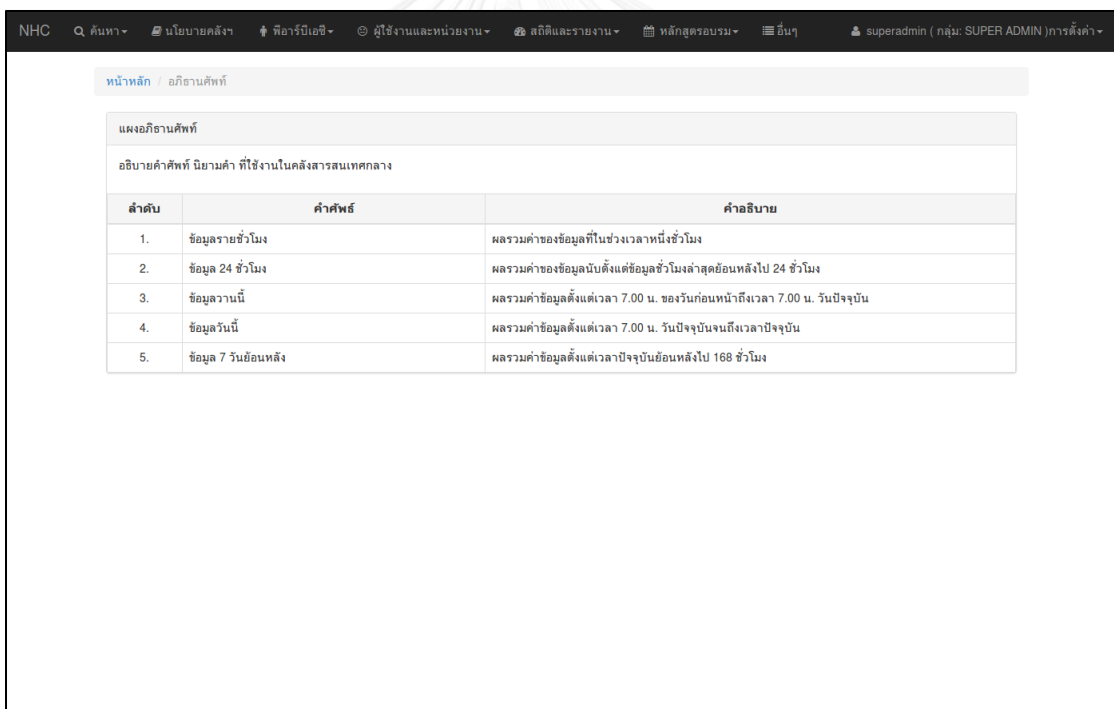


ลำดับ	คำแนะนำ
1	การกำหนดรหัสผ่านให้มีความยาวอย่างน้อย 8 อักขร
2	ควรมีอักขรตัวพิมพ์เล็ก (Lowercase letters) เช่น a, b, c เป็นต้น
3	ควรมีอักขรตัวพิมพ์เล็ก (Lowercase letters) เช่น a, b, c เป็นต้น
4	ควรมีอักขรตัวพิมพ์ใหญ่ (Uppercase letters) เช่น A, B, C เป็นต้น
5	ควรมีตัวเลข (Numbers) คือ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
6	ควรมีสัญลักษณ์ (Symbols) เช่น () `~!@#\$%^&*'+= \\{}[]:;'"<>.,~/ เป็นต้น
7	ควรมีอักขรแบบยูนิโคด (Unicode characters) คือ €, ?, ?, และ ?
8	รหัสผ่านไม่ควรประกอบด้วยตัวอักษรที่มีอยู่ในชื่อ user name เกินกว่า 3 ตัวอักษร
9	เพื่อให้มีความปลอดภัยเพิ่มขึ้นควรทำเปลี่ยนรหัสผ่านเป็นประจำอย่างน้อยทุกๆ 42 วัน
10	ไม่ควรใช้รหัสผ่านซ้ำกับรหัสผ่านที่เคยใช้มาแล้ว
11	อย่าเขียนรหัสผ่านลงกระดาษโดยเด็ดขาด

รูปที่ ง.13 คำแนะนำในการสร้างรหัสผ่านที่ยากต่อการคาดเดา



รูปที่ ง.14 ผู้ใช้งานสามารถเปิดถอนการยินยอมการใช้งานข้อมูล



รูปที่ ง.15 อภิธานศัพท์ที่ใช้ในคลังสารสนเทศกลาง

NHC | บบบาท: (นักรวิจัย) | ค้นหา | ข้อมูล | ร่องข้อมูล | หลักสูตรบวม | ผลการร่องข้อมูล | คำร่องข้อมูล | user1 (กลุ่ม: ADMIN)

แผงฟังก์ชันงานในระบบ

ตำแหน่งหน้าที่ผู้ใช้งานในระบบ

1. เจ้าหน้าที่คลังสารสนเทศ
2. ผู้ใช้งานประเภทผู้ดูแลระบบ (หนึ่งหน่วยงานมีได้คนเดียว)
3. ผู้ใช้งานประเภททั่วไป

กรอบปัญหา	ฟังก์ชันงาน	ตำแหน่งหน้าที่	หลักการพีดี	ระบบงานสนับสนุน
1.การกำหนดนโยบายการใช้งานข้อมูลตามสิทธิและบทบาท	<ul style="list-style-type: none"> สนับสนุนการจัดการนโยบาย <ul style="list-style-type: none"> สามารถค้นหานโยบาย สามารถบันทึกนโยบายการใช้งาน สามารถแก้ไขนโยบาย สามารถเลิกใช้นโยบาย สามารถกำหนด/แก้ไข/ลบชื่อผู้รับผิดชอบเพื่อให้ผู้ใช้ติดต่อ กำหนดค่าพื้นฐานการใช้งานข้อมูล <ul style="list-style-type: none"> สามารถบันทึกรายการการโพรวีซีค่าเริ่มต้นข้อมูลที่อยู่ระบบ สามารถบันทึกรายการการโพรวีซีค่าเริ่มต้นข้อมูลผู้ใช้งาน สามารถเพิ่มรายการการโพรวีซีค่าเริ่มต้นข้อมูลผู้ใช้งาน สามารถแก้ไขรายการการโพรวีซีค่าเริ่มต้นข้อมูลผู้ใช้งาน สามารถลบรายการการโพรวีซีเริ่มต้นข้อมูลผู้ใช้งาน ระบบตัวตน มีความสามารถคือ <ul style="list-style-type: none"> สามารถเรียกแก้ไขในกรณีลืมรหัสผ่าน สามารถเข้าสู่ระบบ สามารถแก้ไขข้อมูลส่วนตัว สามารถเปลี่ยนรหัสผ่าน แนะนำรหัสผ่าน มีความสามารถคือ <ul style="list-style-type: none"> สามารถสร้างรหัสผ่านให้ผู้ใช้ สามารถให้คำแนะนำในการสร้าง 	<ul style="list-style-type: none"> • ข้อที่ 1 - ข้อที่ 3 • ข้อที่ 1 • ข้อที่ 1 • ข้อที่ 1 • ข้อที่ 1 	ข้อที่ 2 และ ข้อที่ 4	<ul style="list-style-type: none"> ✓ ✓ ✓ ✓

รูปที่ ง.16 ฟังก์ชันงานของแอปพลิเคชัน

NHC | ค้นหา | นโยบายคลังฯ | พิอาร์บีเอซี | ผู้ใช้งานและหน่วยงานฯ | สถิติและรายงานฯ | หลักสูตรบวม | อื่นๆ | superadmin (กลุ่ม: SUPER ADMIN) การตั้งค่า

หน้าหลัก / สถิติและรายงาน / รายงาน

แผงรายงาน

นักรวิจัย | 2015-07-12 15:36 | 2015-07-15 15:36 | ค้นหา [CSV]

10 แถวต่อหน้า ค้นหา:

ไอพี	โอส	ล่าสุด	บบบาท	ข้อมูล
127.0.0.1	http://localhost/project/sites/public	2015-07-15 14:43:48	นักรวิจัย (user1)	ปริมาณนำฝนราย 24 ชั่วโมง
127.0.0.1	http://localhost/project/sites/public	2015-07-15 14:38:45	นักรวิจัย (Super Admin)	ข้อมูลระดับน้ำ
127.0.0.1	http://localhost/project/sites/public	2015-07-15 13:25:23	นักรวิจัย (user1)	ปริมาณนำฝนราย 24 ชั่วโมง
127.0.0.1	http://localhost/project/sites/public	2015-07-15 13:25:05	นักรวิจัย (user1)	ข้อมูลระดับน้ำ
127.0.0.1	http://localhost/project/sites/public	2015-07-15 13:20:40	นักรวิจัย (Super Admin)	ปริมาณนำฝนย้อนหลัง
127.0.0.1	http://localhost/project/sites/public	2015-07-15 10:26:04	นักรวิจัย (Super Admin)	ข้อมูลอุณหภูมิ
:::1	http://localhost/project/sites/public	2015-07-14 21:36:03	นักรวิจัย (user1)	ปริมาณนำฝนวันนี้
:::1	http://localhost/project/sites/public	2015-07-14 21:19:56	นักรวิจัย (Super Admin)	ปริมาณนำฝนวานนี้
:::1	http://localhost/project/sites/public	2015-07-14 21:17:35	นักรวิจัย (Super Admin)	ข้อมูลความเข้มแสง
:::1	http://localhost/project/sites/public	2015-07-13 19:46:28	นักรวิจัย (Super Admin)	ปริมาณนำฝนวานนี้
:::1	http://localhost/project/sites/public	2015-07-13 19:46:11	นักรวิจัย (user1)	ข้อมูลความภาคอากาศ

แสดง 1 ถึง 1 จากทั้งหมด 1 แถว | 1 | เติหน้า

รูปที่ ง.17 รายการบันทึกประวัติการใช้งานและการเข้าถึงข้อมูล

NHC ค้นหา นโยบายคลัง พิจารณิเอชไอ ผู้ใช้งานและหน่วยงาน สถิติและรายงาน หลักสูตรอบรม superadmin (กลุ่ม: SUPER ADMIN) การตั้งค่า

หน้าหลัก / การตั้งค่า / ตั้งค่าโทรเวชิ

โทรเวชิผู้ใช้งาน โทรเวชิเริ่มต้น การเก็บรักษาข้อมูล

แผนการเก็บรักษาข้อมูล

กำหนดอายุการเก็บรักษาข้อมูล โดยระบุวันเริ่มต้นและระยะเวลาเก็บรักษา

ปริมาณนำหน้าราย 24 ชั่วโมง 2015-07-15 ระยะเก็บรักษาข้อมูล 1 วัน บันทึก เรียกดู

ชื่อข้อมูล	วันเริ่มต้น	วันสุดท้าย	ระยะเวลาเก็บ
ปริมาณนำหน้าราย 24 ชั่วโมง	2015-07-14	2015-07-15 00:00:00	ระยะเก็บรักษาข้อมูล 1 วัน
ปริมาณนำหน้าวันนี้	2014-07-08	2015-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 1 ปี
ปริมาณนำหน้าวานนี้	2014-07-08	2015-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 1 ปี
ปริมาณนำหน้าย้อนหลัง	2014-07-08	2015-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 1 ปี
ข้อมูลระดับน้ำ	2014-07-08	2017-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 3 ปี
ข้อมูลน้ำในเขื่อน	2014-07-08	2017-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 3 ปี
ข้อมูลความเข้มแสง	2014-07-08	2017-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 3 ปี
ข้อมูลความชื้น	2014-07-08	2017-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 3 ปี
ข้อมูลความกดอากาศ	2014-07-08	2021-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 7 ปี
ข้อมูลอุณหภูมิ	2014-07-08	2019-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 5 ปี
ข้อมูลระดับน้ำทะเล	2014-07-08	2024-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 10 ปี

รูปที่ ง.18 กำหนดช่วงเวลาการเก็บรักษาข้อมูล

NHC บุพบท: (นักวิจัย) ค้นหา ข้อมูล ร้องขอข้อมูล หลักสูตรอบรม ผลการร้องขอข้อมูล คำร้องขอข้อมูล user1 (กลุ่ม: ADMIN)

หน้าหลัก / การตั้งค่า / ตั้งค่าโทรเวชิ

โทรเวชิผู้ใช้งาน โทรเวชิข้อมูล การเก็บรักษาข้อมูล

แผนการเก็บรักษาข้อมูล

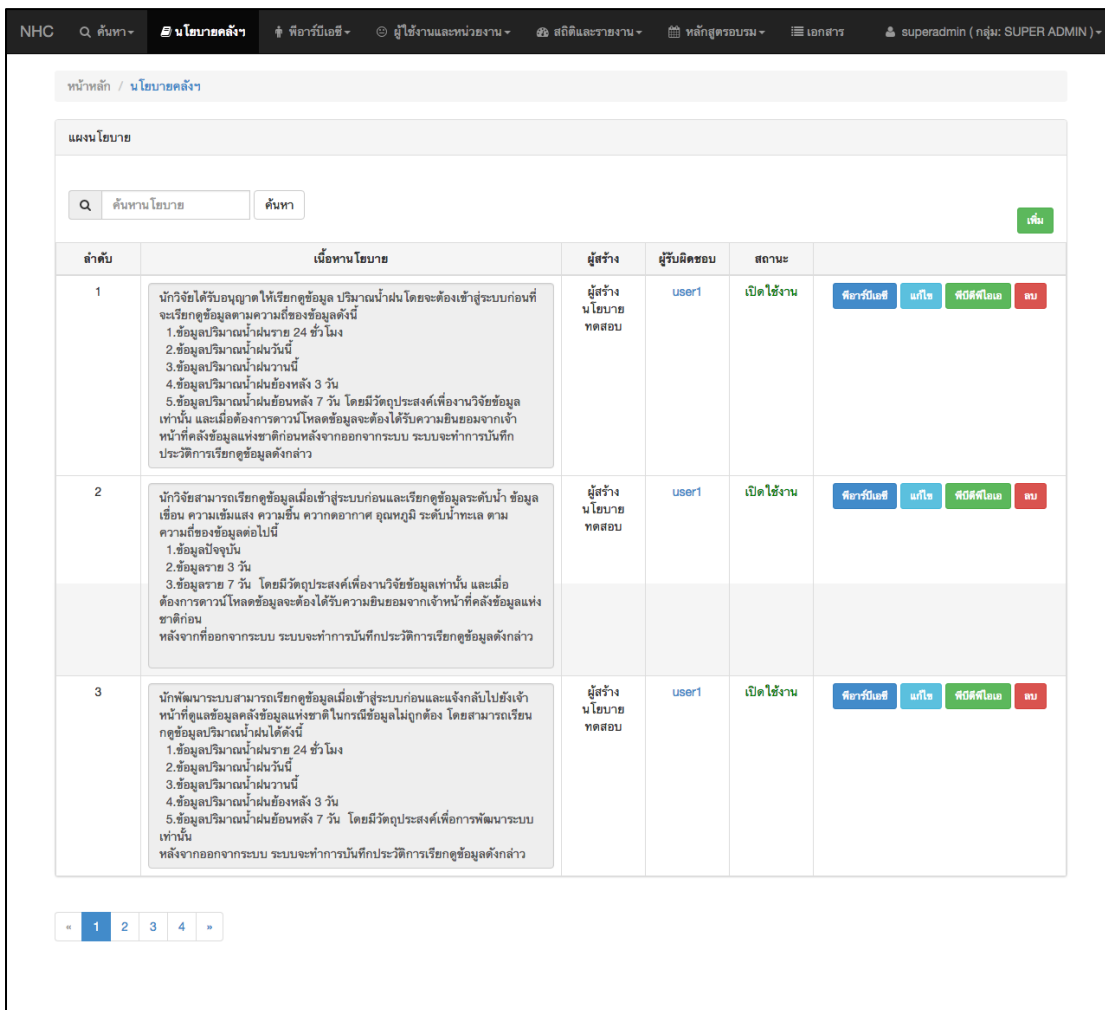
10 แถวต่อหน้า ค้นหา :

ชื่อข้อมูล	วันเริ่มต้น	วันสุดท้าย	ระยะเวลาเก็บ
ข้อมูลความกดอากาศ	2014-07-08	2021-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 7 ปี
ข้อมูลความชื้น	2014-07-08	2017-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 3 ปี
ข้อมูลความเข้มแสง	2014-07-08	2017-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 3 ปี
ข้อมูลน้ำในเขื่อน	2014-07-08	2017-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 3 ปี
ข้อมูลระดับน้ำ	2014-07-08	2017-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 3 ปี
ข้อมูลระดับน้ำทะเล	2014-07-08	2024-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 10 ปี
ข้อมูลอุณหภูมิ	2014-07-08	2019-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 5 ปี
ปริมาณนำหน้าย้อนหลัง	2014-07-08	2015-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 1 ปี
ปริมาณนำหน้าราย 24 ชั่วโมง	2015-07-14	2015-07-15 00:00:00	ระยะเก็บรักษาข้อมูล 1 วัน
ปริมาณนำหน้าวันนี้	2014-07-08	2015-07-08 00:00:00	ระยะเก็บรักษาข้อมูล 1 ปี

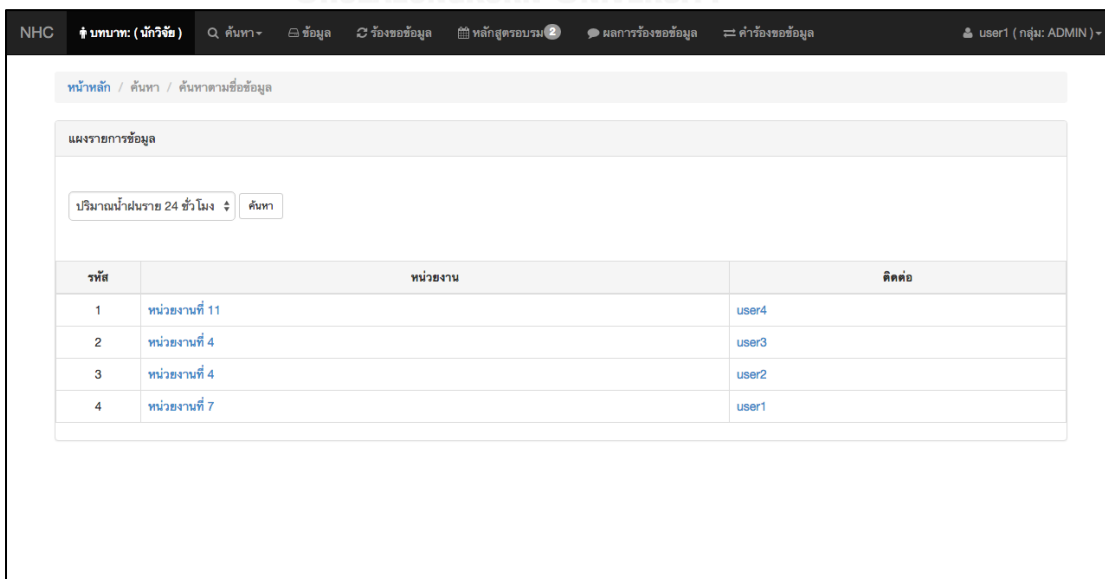
แสดง 1 ถึง 10 จากทั้งหมด 11 แถว

ถอยหลัง 1 2 เดินหน้า

รูปที่ ง.19 แสดงช่วงเวลาการเก็บรักษาข้อมูลเพื่อให้ผู้ใช้งานรับทราบ



รูปที่ ง.20 รายการนโยบายการใช้งานข้อมูล



รูปที่ ง.21 แสดงรายการข้อมูล หน่วยงานที่จัดเก็บในคลังสารสนเทศกลาง

หน้าหลัก / ขอข้อมูล

แผนขอข้อมูล

นโยบายที่เกี่ยวข้อง

หน่วยงานที่ 1 | ข้อมูลระดับน้ำ | ข้อมูลปัจจุบัน | ขออนุญาตเปิดเผยข้อมูล | **ส่งคำขอ**

เสร็จสิ้น คำร้องขอของท่านได้รับการบันทึกเรียบร้อยแล้ว.

รูปที่ ง.22 ขั้นตอนในการร้องขอข้อมูลจากหน่วยงานเจ้าของข้อมูล

หน้าหลัก / คำร้องขอข้อมูล / รายการคำร้องขอข้อมูล

แผนรายการคำร้องขอ

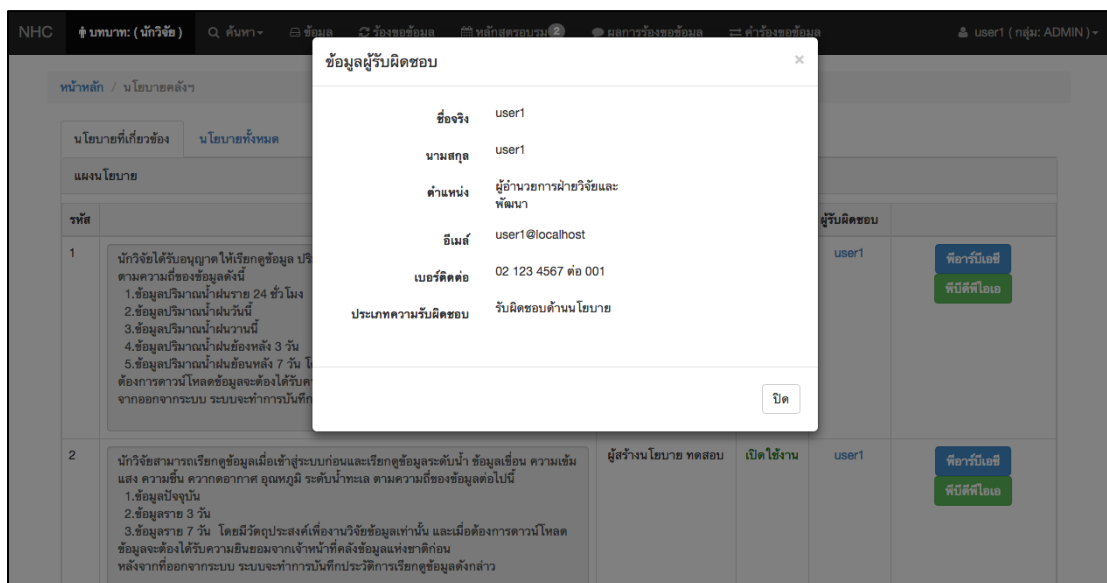
10 | แสดงต่อหน้า | ค้นหา :

*ข้อมูลที่ร้องขอ	ความถี่ข้อมูล	สถานะการร้องขอ	วัตถุประสงค์การขอ	*ผู้ร้องขอ	*หน่วยงานผู้ร้องขอ	วันที่ร้องขอ	
ข้อมูลระดับน้ำ	ข้อมูลปัจจุบัน	อยู่ระหว่างพิจารณา	ขออนุญาตเปิดเผยข้อมูล	user1 User1 (นักวิจัย)	หน่วยงานที่ 2	2014-10-15	Edit

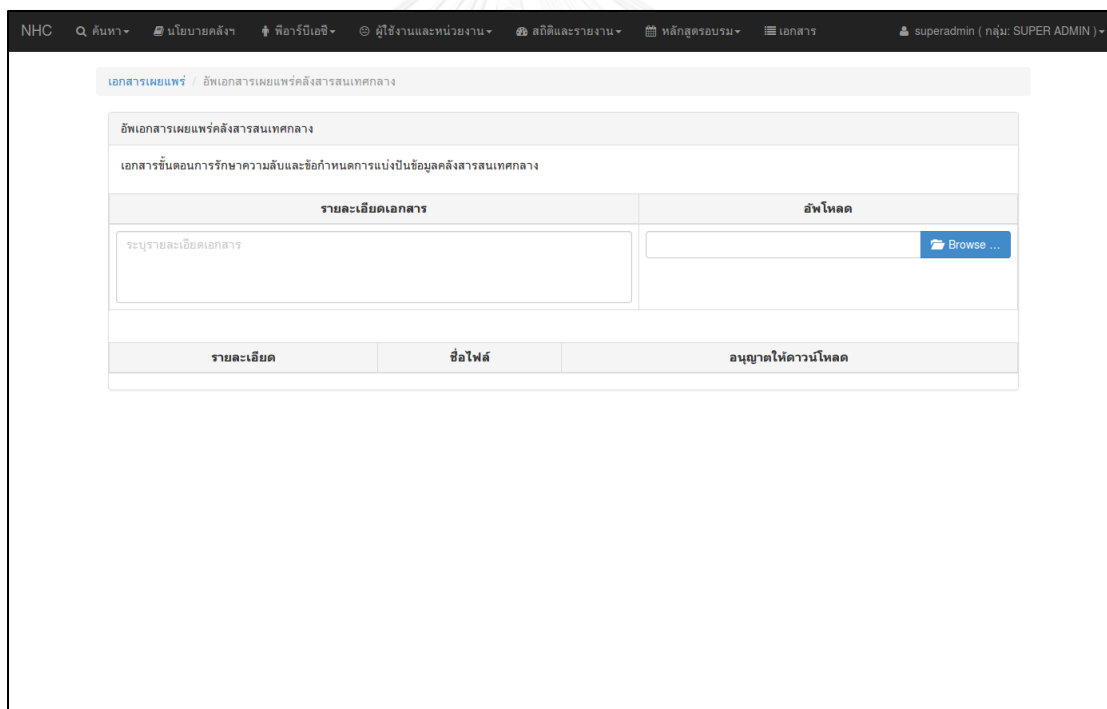
แสดง 1 ถึง 1 จากทั้งหมด 1 แถว

ถอยหลัง 1 | เดินหน้า

รูปที่ ง.23 เจ้าของข้อมูลพิจารณาเพื่อดำเนินการต่อคำร้องขอ



รูปที่ ง.24 ช่องทางการติดต่อกับเจ้าหน้าที่ในองค์กรที่รับผิดชอบด้านนโยบาย



รูปที่ ง.25 อัปเดตเอกสารขั้นตอนการรักษาความลับและข้อกำหนดการแบ่งปันข้อมูลคลังสารสนเทศกลาง

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารชี้แจงช่วงเวลาดำหนดบททวนนโยบายโทรเวชีและความมั่นคงในคลังสารสนเทศกลาง

รายละเอียดเอกสาร	อัปโหลด	
ระบุรายละเอียดเอกสาร	<input type="text"/> Browse ...	
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.26 อีพโหลดเอกสารชี้แจงช่วงเวลาดำหนดบททวนนโยบายโทรเวชีและความมั่นคงในคลังสารสนเทศกลาง

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารแผนงานโครงการการพัฒนา ไรตี้ไซน์เทคโนโลยีของคลังสารสนเทศกลาง

รายละเอียดเอกสาร	อัปโหลด	
ระบุรายละเอียดเอกสาร	<input type="text"/> Browse ...	
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.27 อีพโหลดเอกสารแผนงานโครงการการพัฒนา ไรตี้ไซน์เทคโนโลยีของคลังสารสนเทศกลาง

รูปที่ ง.28 อ็อปโหลดเอกสารมาตรฐานสำหรับการประเมินการออกแบบด้านโทรเวช

รูปที่ ง.29 อ็อปโหลด เอกสารขั้นตอนการดำเนินการประเมินการตรวจสอบการปฏิบัติตามนโยบายโทรเวชและความมั่นคงของคลังสารสนเทศกลาง

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารตรวจสอบด้านโทรเวชและความมั่นคง

รายละเอียดเอกสาร	อัปโหลด	
ระบุรายละเอียดเอกสาร	<input type="text"/> Browse ...	
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.30 อีพโหลดเอกสารตรวจสอบด้านโทรเวชและความมั่นคง

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารการออกแบบและสถาปัตยกรรมเทคโนโลยีสารสนเทศ กระบวนการทางธุรกิจของคลังสารสนเทศกลาง

รายละเอียดเอกสาร	อัปโหลด	
ระบุรายละเอียดเอกสาร	<input type="text"/> Browse ...	
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.31 อีพโหลดเอกสารการออกแบบและสถาปัตยกรรมเทคโนโลยีสารสนเทศ กระบวนการทางธุรกิจของคลังสารสนเทศกลาง

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารชี้แจงวัตถุประสงค์การเก็บข้อมูลในคลังสารสนเทศกลาง

รายละเอียดเอกสาร		อัปโหลด
ระบุรายละเอียดเอกสาร		<input type="text"/> Browse ...
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.32 อีพโหลดเอกสารชี้แจงวัตถุประสงค์การเก็บข้อมูลในคลังสารสนเทศกลาง

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารตรวจสอบการใช้ข้อมูลและวัตถุประสงค์ที่กำหนด

รายละเอียดเอกสาร		อัปโหลด
ระบุรายละเอียดเอกสาร		<input type="text"/> Browse ...
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.33 อีพโหลด เอกสารตรวจสอบการใช้ข้อมูลและวัตถุประสงค์ที่กำหนด

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารข้อกำหนดการใช้งานข้อมูลในคลังสารสนเทศกลางสำหรับบุคคลภายนอก

รายละเอียดเอกสาร		อัปโหลด
ระบุรายละเอียดเอกสาร		<input type="text"/> Browse ...
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.34 อีพโหลดเอกสารข้อกำหนดการใช้งานข้อมูลในคลังสารสนเทศกลางสำหรับบุคคลภายนอก

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารตัวชี้วัดประสิทธิภาพการใช้งานข้อมูลและวัตถุประสงค์ของคลังสารสนเทศกลาง

รายละเอียดเอกสาร		อัปโหลด
ระบุรายละเอียดเอกสาร		<input type="text"/> Browse ...
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.35 อีพโหลด เอกสารตัวชี้วัดประสิทธิภาพการใช้งานข้อมูลและวัตถุประสงค์ของคลังสารสนเทศกลาง

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารประเมินความเสี่ยง

รายละเอียดเอกสาร		อัปโหลด
ระบุรายละเอียดเอกสาร		<input type="text"/> Browse ...
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.36 อีพโหลดเอกสารประเมินความเสี่ยง

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารชี้แจงสิทธิเพื่อทำการเพิกถอน ระเบียบการใช้งานและเปิดเผยข้อมูลในคลังสารสนเทศกลาง และขั้นตอนการร้องเรียนด้านไพรเวซี

รายละเอียดเอกสาร		อัปโหลด
ระบุรายละเอียดเอกสาร		<input type="text"/> Browse ...
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.37 อีพโหลดเอกสารชี้แจงสิทธิเพื่อทำการเพิกถอน ระเบียบการใช้งานและเปิดเผยข้อมูลในคลังสารสนเทศกลาง และขั้นตอนการร้องเรียนด้านไพรเวซี

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารประเมินความถูกต้องข้อมูล

รายละเอียดเอกสาร	อัปโหลด	
ระบุรายละเอียดเอกสาร	<input type="text"/> Browse ...	
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

รูปที่ ง.38 อีพโหลดเอกสารประเมินความถูกต้องของข้อมูล

เอกสารเผยแพร่ / อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

อีพเอกสารเผยแพร่คลังสารสนเทศกลาง

เอกสารผลการประเมินความคาดหวังของผู้ให้ข้อมูลแก่คลังสารสนเทศกลาง

รายละเอียดเอกสาร	อัปโหลด	
ระบุรายละเอียดเอกสาร	<input type="text"/> Browse ...	
รายละเอียด	ชื่อไฟล์	อนุญาตให้ดาวน์โหลด

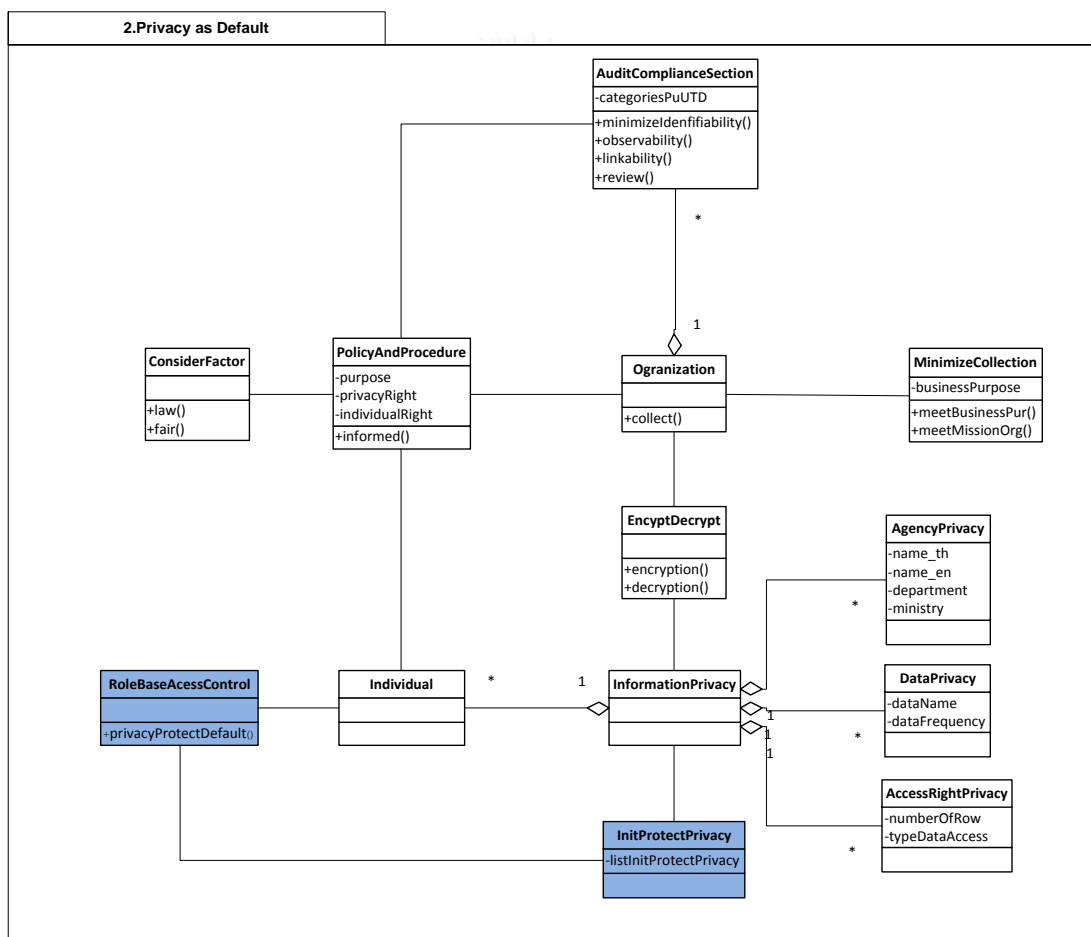
รูปที่ ง.39 อีพโหลดเอกสารผลการประเมินความคาดหวังของผู้ให้ข้อมูลแก่คลังสารสนเทศกลาง

ตารางที่ ง.3 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.40 ด้าน Proactive not Reactive (ต่อ)

ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
4.	Eexecutive	คลาสเกี่ยวข้องกับ ผู้บริหารระดับสูง	c,e,f
5.	Stakeholders	คลาสเกี่ยวข้องกับผู้มีส่วน ได้เสีย	d
6.	Training	คลาสเกี่ยวข้องกับการจัด อบรม	s
7.	RoleBaseCourse	คลาสเกี่ยวข้องกับ หลักสูตรการอบรมด้าน การเข้าถึงตามบทบาท	u
8.	Organization	คลาสเกี่ยวข้องกับองค์กร	a
9.	PrivacySecurityProgram	คลาสเกี่ยวข้องกับ โปรแกรมด้านความเป็นส่วนตัว และความมั่นคง	a,b
10.	PrivacySecuritySection	คลาสเกี่ยวข้องกับ หน่วยงานด้านความเป็นส่วนตัว และความมั่นคง	i,j,k
11.	AuditComplianceSection	คลาสเกี่ยวข้องกับ หน่วยงานตรวจสอบการ ปฏิบัติตาม	z
12.	Agreement	คลาสเกี่ยวข้องกับการ ยอมรับ ข้อตกลงการ ให้บริการ	h

ตารางที่ ง.3 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.40 ด้าน Proactive not Reactive (ต่อ)

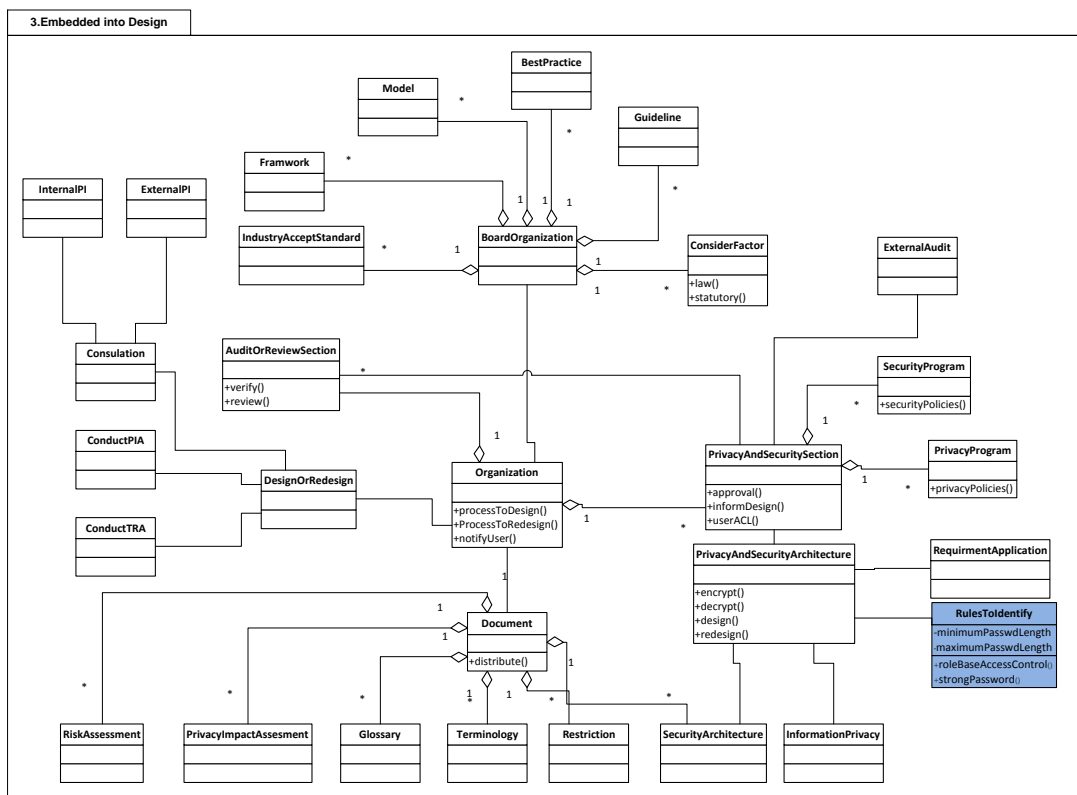
ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
13.	ExternalAudit	คลาสเกี่ยวข้องกับ การตรวจสอบจากบุคคลภายนอก	aa



รูปที่ ง.41 แผนภาพคลาสหลักการที่ 2 Privacy as Default

ตารางที่ ง.4 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.41 ด้าน Privacy as Default

ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
1.	AuditComplianceSection	คลาสเกี่ยวข้องกับ หน่วยงานด้านการ ตรวจสอบการปฏิบัติตาม	a-c,g
2.	ConsiderFactor	คลาสเกี่ยวข้องกับปัจจัย ที่จำเป็นต้องพิจารณา	i
3.	MinimizeCollection	คลาสเกี่ยวข้องกับการ จัดเก็บตามหลักการเก็บ ให้น้อยที่สุด	g
4.	EncryptDecrypt	คลาสเกี่ยวข้องกับการ เข้ารหัสและถอดรหัส	e,f
5.	InitProtectPrivacy	คลาสเกี่ยวข้องกับการ กำหนดค่าเริ่มต้นการ ป้องกันไพรเวซี	l
6.	RoleBaseAccessControl	คลาสเกี่ยวข้องการเข้าถึง ตามบทบาทที่ได้รับ	k



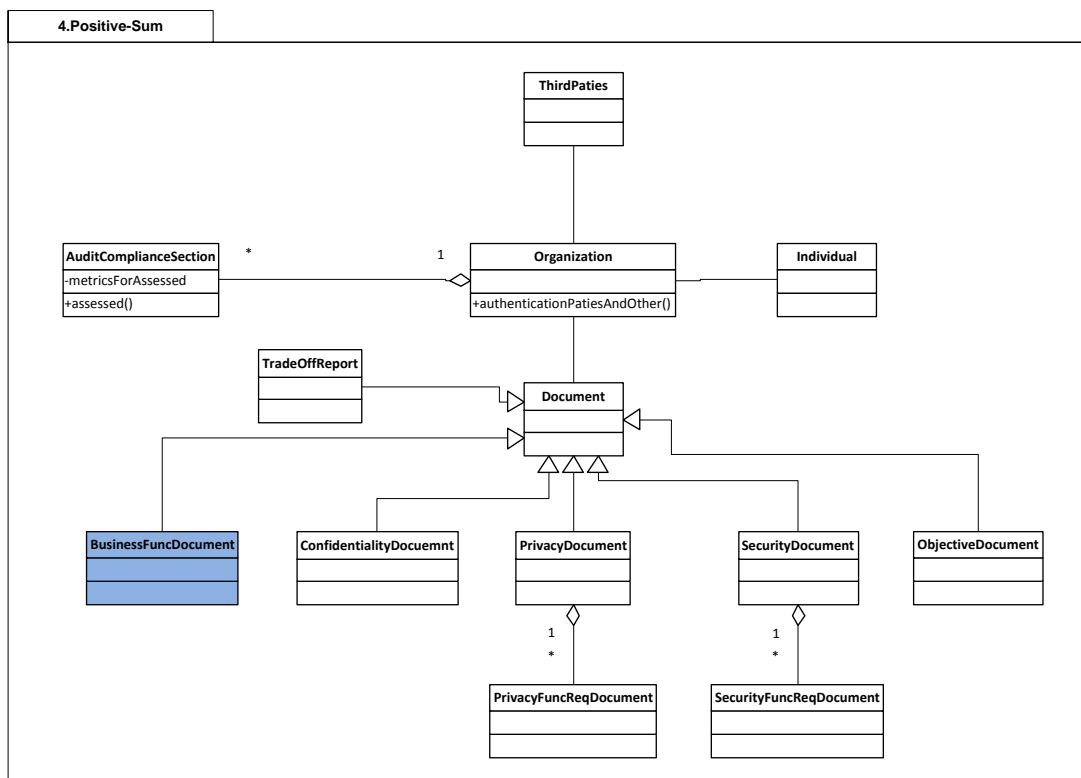
รูปที่ ง.42 แผนภาพคลาสหลักการที่ 3 Embedded into Design

ตารางที่ ง.5 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.42 ด้าน Embedded into Design

ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
1.	BoardOrganization	คลาสเกี่ยวข้องกับ กรรมการบริหารองค์กร	a
2.	AuditOrReviewSection	คลาสเกี่ยวข้องกับ หน่วยงานตรวจสอบหรือ การทบทวน	f,j
3.	DesignOrRedesign	คลาสเกี่ยวข้องกับการ ออกแบบและการรีดีไซน์	k1-k4
4.	Organization	คลาสเกี่ยวข้องกับองค์กร	h

ตารางที่ ง.5 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.42 ด้าน Embedded into Design (ต่อ)

ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
5.	Document	คลาสเกี่ยวข้องกับเอกสารในองค์กร	d,i
6.	SecurityArchitecture	คลาสเกี่ยวข้องกับเอกสารสถาปัตยกรรมด้านความมั่นคง	e
7.	ExternalAudit	คลาสเกี่ยวข้องกับผู้ตรวจสอบภายนอกองค์กร	c
8.	PrivacyAndSecurityArchitecture	คลาสเกี่ยวข้องกับสถาปัตยกรรมด้านความเป็นส่วนตัวและความมั่นคง	b
9.	RulesToIdentify	คลาสเกี่ยวข้องกับกฎสำหรับการระบุตัวตน	g,k9-10



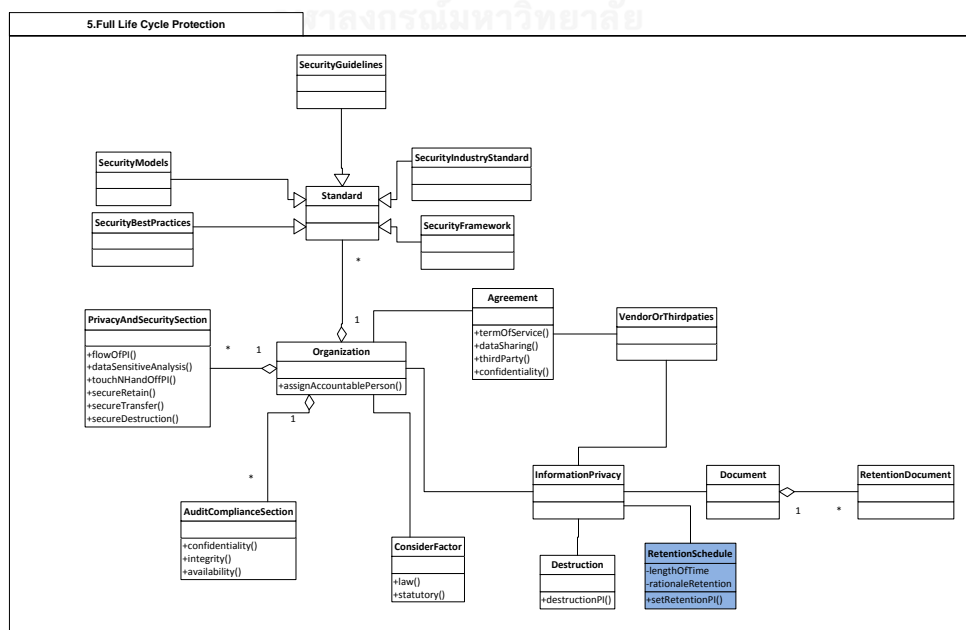
รูปที่ ง.43 แผนภาพคลาสหลักการที่ 4 Positive-Sum

ตารางที่ ง.6 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.43 ด้าน Positive-Sum

ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
1.	AuditComplianceSection	คลาสเกี่ยวข้องกับหน่วยงานตรวจสอบการปฏิบัติตาม	c
2.	Organization	คลาสเกี่ยวข้องกับองค์กร	b
3.	BusinessFuncDocument	คลาสเกี่ยวข้องกับเอกสารการดำเนินงาน	a3
4.	ConfidentialityDocument	คลาสเกี่ยวข้องกับเอกสารด้านความลับ	a1

ตารางที่ ง.6 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.43 ด้าน Positive-Sum (ต่อ)

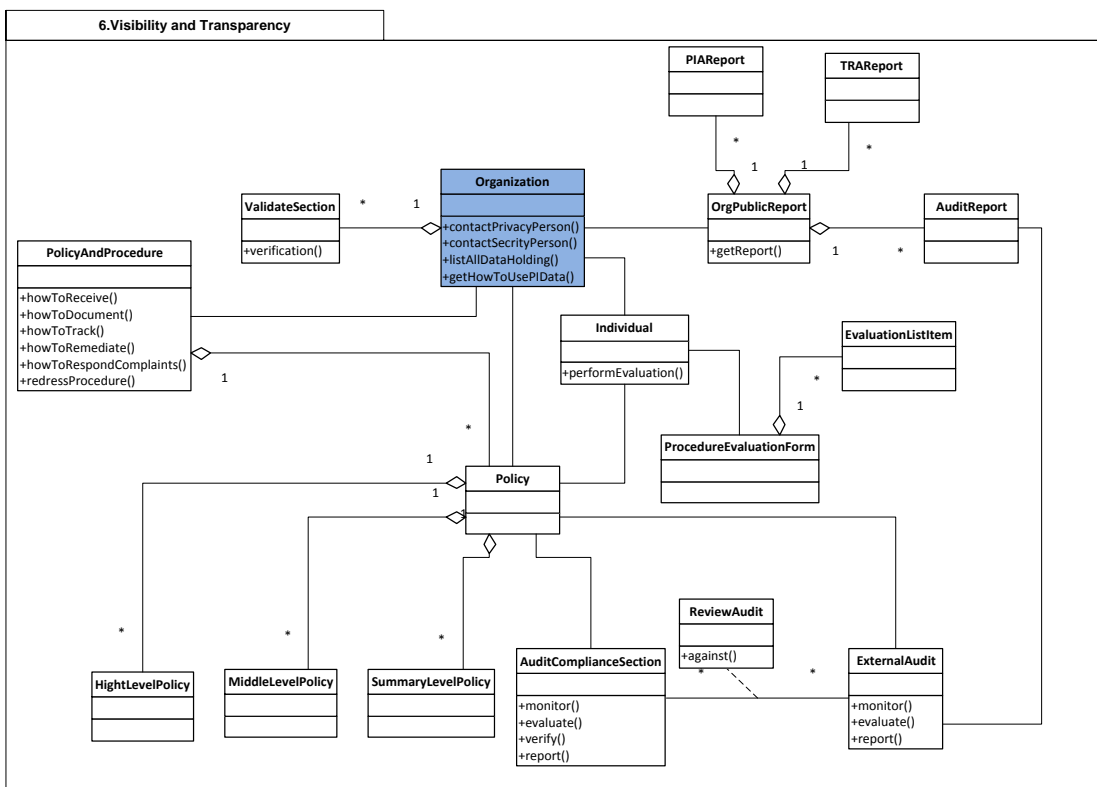
ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
5.	PrivacyDocument	คลาสเกี่ยวข้องกับเอกสารด้านความเป็นส่วนตัว	a1
6.	SecurityDocument	คลาสเกี่ยวกับเอกสารด้านความมั่นคง	a1
7.	ObjectiveDocument	คลาสเกี่ยวข้องกับเอกสารด้านวัตถุประสงค์	a2
8.	PrivacyFuncReqDocument	คลาสเกี่ยวกับเอกสารด้านรายการความต้องการด้านความเป็นส่วนตัว	a4
9.	SecurityFuncReqDocument	คลาสเกี่ยวกับเอกสารด้านรายการความต้องการด้านความมั่นคง	a4



รูปที่ ง.44 แผนภาพคลาสหลักการที่ 5 Full Life Cycle Protection

ตารางที่ ง.7 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.44 ด้าน Full Life Cycle Protection

ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
1.	Standard	คลาสเกี่ยวข้องกับ มาตรฐานที่นำมาใช้งาน	f1
2.	PrivacyAndSecuritySection	คลาสเกี่ยวข้องกับ หน่วยงานด้านโพรเวซี และความมั่นคง	a,b,d,g
3.	Organization	คลาสเกี่ยวข้องกับองค์กร	e
4.	Agreement	คลาสเกี่ยวข้องกับเงื่อนไข การใช้บริการ การ แบ่งปันข้อมูล	h
5.	AuditComplianceSection	คลาสเกี่ยวข้องกับการ ตรวจสอบการปฏิบัติตาม	i
6.	Destruction	คลาสเกี่ยวข้องกับการ ทำลายข้อมูล	l
7.	RetentionSchedule	คลาสเกี่ยวข้องกับ ระยะเวลาในการเก็บ ข้อมูล	j,k



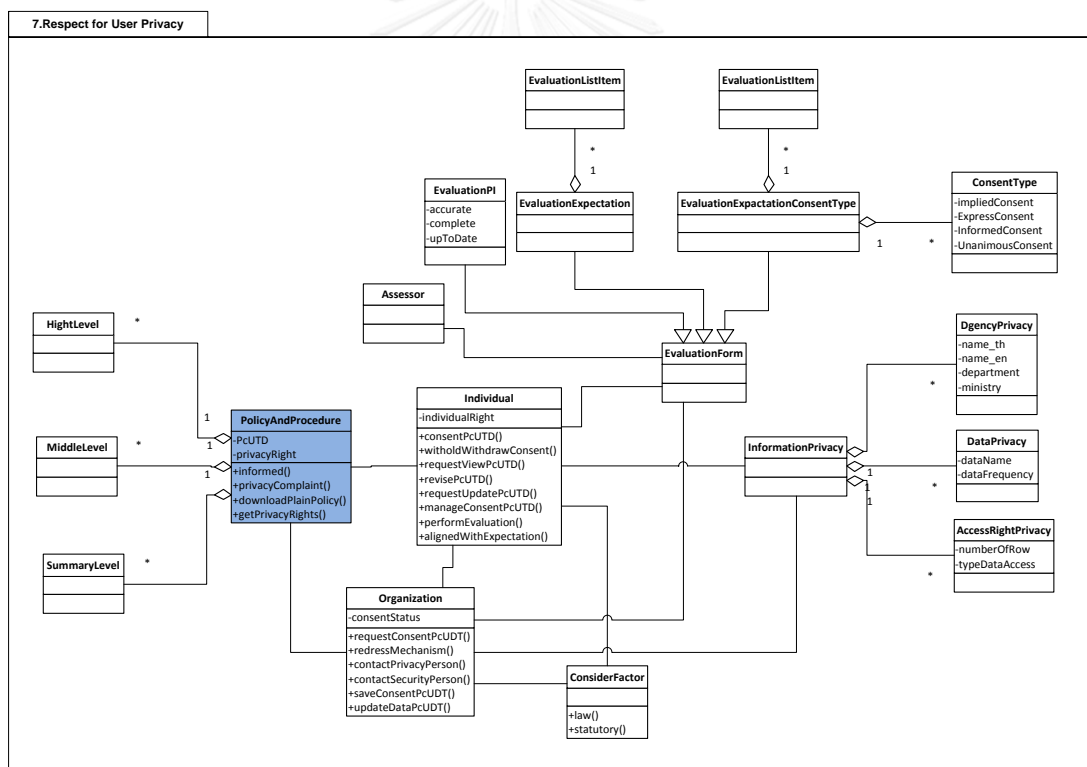
รูปที่ ง.45 แผนภาพคลาสหลักการที่ 6 Visibility and Transparency

ตารางที่ ง.8 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.45 ด้าน Visibility and Transparency

ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
1.	Organization	คลาสเกี่ยวข้องกับองค์กร	a,g,d
2.	PIAResult	คลาสเกี่ยวข้องกับ รายงานการประเมินผล กระทบด้านไพรเวซี	e
3.	TRAResult	คลาสเกี่ยวข้องกับ รายงานการประเมินผล ความเสี่ยงและภัยคุกคาม	e
4.	AuditReport	คลาสเกี่ยวข้องกับ รายงานด้านการตรวจ	f

ตารางที่ ง.8 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.45 ด้าน Visibility and Transparency (ต่อ)

ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
5.	Policy	คลาสเกี่ยวข้องกับนโยบายในองค์กร	b
6.	PolicyAndProcedure	คลาสเกี่ยวข้องกับกระบวนการและนโยบายด้านการติดตาม การชดใช้	h,i



รูปที่ ง.46 แผนภาพคลาสหลักจากรูปที่ 7 Respect for User Privacy

ตารางที่ ง.9 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.46 ด้าน Respect for User Privacy

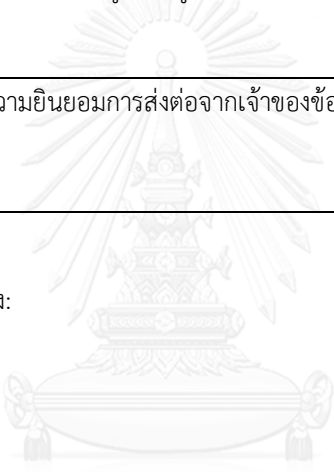
ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
1.	PolicyAndProcedure	คลาสเกี่ยวข้องกับนโยบายและขั้นตอนปฏิบัติในองค์กร	a1,a6,b,f,e
2.	Individual	คลาสเกี่ยวข้องกับข้อมูลส่วนบุคคล	a2,a4-5,k,g,l,h,i,j
3.	Organization	คลาสเกี่ยวข้องกับองค์กร	a7,a8
4.	ConsiderFactor	คลาสเกี่ยวข้องกับปัจจัยที่จำเป็นต้องพิจารณา	a3
5.	EvaluationForm	คลาสเกี่ยวข้องกับแบบฟอร์มการประเมิน	
6.	HightLevel	คลาสเกี่ยวข้องกับนโยบายหรือขั้นตอนการปฏิบัติขององค์กรในมุมมองเชิงกว้าง	d
7.	MiddleLevel	คลาสเกี่ยวข้องกับนโยบายหรือขั้นตอนการปฏิบัติขององค์กรในมุมมองระดับกลาง	d
8.	SummaryLevel	คลาสเกี่ยวข้องกับนโยบายหรือขั้นตอนปฏิบัติขององค์กรในมุมมองสรุป	d
9.	Assessor	คลาสเกี่ยวข้องกับผู้ทำการประเมิน	

ตารางที่ ง.9 แสดงคำอธิบายแผนภาพคลาสจากรูปที่ ง.46 ด้าน Respect for User Privacy (ต่อ)

ลำดับ	ชื่อคลาส	คำอธิบาย	คำถามในตาราง ง.1 ที่เกี่ยวข้อง
10.	EvaluationPI	คลาสเกี่ยวข้องกับการ ประเมินสารสนเทศโพรว ซี่	
11.	EvaluationExpectation	คลาสเกี่ยวข้องกับการ คาดหวังการประเมิน	
12.	EvaluationListItem	คลาสเกี่ยวข้องกั รายการที่ใช้ในการ ประเมิน	
13.	EvaluationExpectationConsentType	คลาสเกี่ยวข้องกับความ คาดหวังของประเภทการ ยินยอม	
14.	ConsentType	คลาสเกี่ยวข้องกั ประเภทของการยินยอม	
15.	AgencyPrivacy	คลาสเกี่ยวข้องกัโพรวเวซี่ ของหน่วยงาน	
16.	DataPrivacy	คลาสเกี่ยวข้องกัโพรวเวซี่ ข้อมูล	
17.	AccessRightPrivacy	คลาสเกี่ยวข้องกัสิทธิ โพรวเวซี่	

ภาคผนวก จ ตัวอย่างคำอธิบายแผนภาพยูสเคส

ตารางที่ จ.1 คำอธิบายแผนภาพยูสเคสบันทึกคำร้องขอส่งต่อข้อมูล

ชื่อยูสเคส: บันทึกคำร้องขอส่งต่อข้อมูล	รหัส: UCNHC-01	ระดับความสำคัญ: มาก
ผู้กระทำหลัก: ผู้ใช้งานเครื่องมือสนับสนุน		ประเภทยูสเคส: เชิงละเอียด
ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์: - ตัวแทนหน่วยงานผู้ส่งคำร้อง, ตัวแทนหน่วยงานพิจารณาคำร้อง		
คำอธิบาย: เป็นยูสเคสทำหน้าที่ส่งคำร้องขอข้อมูลจากผู้ใช้งานที่ไม่ได้เป็นเจ้าของข้อมูลและต้องการนำข้อมูลไปใช้งาน		
สิ่งกระตุ้น: เมื่อผู้ร้องขอต้องการความยินยอมการส่งต่อจากเจ้าของข้อมูล ประเภทสิ่งกระตุ้น:		
ความสัมพันธ์: ความเกี่ยวเนื่อง: การรวม: การขยาย: การรับทอดคุณสมบัติ: 		
ขั้นตอนทำงานปกติ: 1. ตัวแทนหน่วยงานผู้ส่งคำร้องเข้าสู่ระบบ 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. ตัวแทนหน่วยงานผู้ส่งคำร้องเลือกเมนูร้องขอข้อมูล 4. ตัวแทนหน่วยงานผู้ส่งคำร้องเลือกหน่วยงานเจ้าของข้อมูล 5. ตัวแทนหน่วยงานผู้ส่งคำร้องเลือกช่วงเวลาข้อมูล 6. ตัวแทนหน่วยงานผู้ส่งคำร้องเลือกประเภทคำร้องขอข้อมูล 7. ตัวแทนหน่วยงานผู้ส่งคำร้องบันทึกคำร้องขอข้อมูล		
ขั้นตอนการทำงานย่อย: 7.1 ระบบตรวจสอบคำร้อง ถ้ามีการบันทึกคำร้องนี้แล้วหรือไม่		

7.1.1	ถ้ามีคำร้องนี้ในระบบแล้ว ระบบแสดงข้อความให้ผู้ใช้งานทราบว่ามีการบันทึกคำร้องนี้แล้ว
7.1.2	ถ้ายังไม่มีคำร้องนี้ในระบบ ระบบบันทึกคำร้องในฐานะข้อมูลและแจ้งให้ผู้ใช้งานทราบว่าบันทึกสำเร็จ
ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):	

ตารางที่ จ.2 คำอธิบายแผนภาพยูสเคสสกัดเอนทิตินโยบายการใช้งานคลังสารสนเทศกลาง

ชื่อยูสเคส: สกัดเอนทิตินโยบายการใช้งานคลังสารสนเทศกลาง	รหัส: UCNHC-02	ระดับความสำคัญ: มาก
ผู้กระทำหลัก: เจ้าหน้าที่คลังสารสนเทศกลาง	ประเภทยูสเคส: เชิงละเอียด	
ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์: - เจ้าหน้าที่คลังสารสนเทศกลาง		
คำอธิบาย: เป็นยูสเคสทำหน้าที่สกัดเอนทิตินโยบายการใช้งานคลังสารสนเทศกลางเพื่อใช้ในการกำหนดสิทธิและบทบาทผู้ใช้งานในคลังสารสนเทศกลางต่อไป		
สิ่งกระตุ้น: ประเภทสิ่งกระตุ้น:		
ความสัมพันธ์: ความเกี่ยวเนื่อง: การรวม: การขยาย: การรับทอดคุณสมบัติ:		
ขั้นตอนทำงานปกติ: 1. เจ้าหน้าที่คลังสารสนเทศเข้าสู่ระบบ 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. เจ้าหน้าที่คลังสารสนเทศเลือกเมนูนโยบาย เพื่อแสดงนโยบายทั้งหมด 4. เจ้าหน้าที่คลังสารสนเทศกดปุ่มฟิวส์ไอคอน 5. เจ้าหน้าที่คลังสารสนเทศพิจารณานโยบายการใช้งาน 6. เจ้าหน้าที่คลังสารสนเทศเลือกเอนทิตินโยบายให้เหมาะสมกับนโยบาย		

7. เจ้าหน้าที่คลังสารสนเทศคอมพิวเตอร์ เพื่อบันทึกเอนทิตีนโยบายลงในฐานข้อมูล
ขั้นตอนการทำงานย่อย:
ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):

ตารางที่ จ.3 คำอธิบายแผนภาพยูสเคสการเรียกดูข้อมูล

ชื่อยูสเคส: เรียกดูข้อมูล	รหัส: UCNHC-03	ระดับความสำคัญ: มาก
ผู้กระทำหลัก: ผู้ใช้งานเครื่องมือสนับสนุน		ประเภทยูสเคส: เชิงละเอียด
ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์: <ul style="list-style-type: none"> - เจ้าหน้าที่คลังสารสนเทศกลาง - นักวิจัย - นักพัฒนาระบบ - ผู้ดูแลฐานข้อมูล - ตัวแทนหน่วยงาน - ผู้บริหารระดับสูง 		
คำอธิบาย: เป็นยูสเคสทำหน้าที่เรียกดูข้อมูลตามสิทธิบทบาทที่กำหนดไว้ในนโยบายการใช้งาน		
สิ่งกระตุ้น: ประเภทสิ่งกระตุ้น:		
ความสัมพันธ์: ความเกี่ยวเนื่อง: การรวม: การขยาย: การรับทอดคุณสมบัติ:		
ขั้นตอนทำงานปกติ: <ol style="list-style-type: none"> 1. ผู้ใช้งานเครื่องมือสนับสนุนเข้าสู่ระบบ 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. ผู้ใช้งานเครื่องมือสนับสนุนเลือกข้อมูลที่ต้องการเรียกดู 4. ผู้ใช้งานเครื่องมือสนับสนุนเลือกช่วงเวลาข้อมูล 		

5. ผู้ใช้งานเครื่องมือสนับสนุนกดปุ่มค้นหา
ขั้นตอนการทำงานย่อย: 5.1 ระบบตรวจสอบชื่อผู้ใช้งานว่าอยู่ในบทบาทไหนเพื่อกำหนดรายการข้อมูลที่มีผู้ใช้งานมีสิทธิใช้งานข้อมูล
ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):

ตารางที่ จ.4 คำอธิบายแผนภาพยูสเคสการบันทึกมอบหมายสิทธิบทบาท

ชื่อยูสเคส: บันทึกมอบหมายสิทธิ บทบาท	รหัส: UCNHC-04	ระดับความสำคัญ: มาก
ผู้กระทำหลัก: เจ้าหน้าที่คลังสารสนเทศกลาง		ประเภทยูสเคส: เชิงละเอียด
ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์: <ul style="list-style-type: none"> - นักวิจัย - นักพัฒนาระบบ - ผู้ดูแลฐานข้อมูล - ตัวแทนหน่วยงาน - ผู้บริหารระดับสูง 		
คำอธิบาย: เป็นยูสเคสทำหน้าที่บันทึกการมอบหมายสิทธิบทบาทการใช้งานข้อมูลในคลังสารสนเทศกลาง		
สิ่งกระตุ้น: ประเภทสิ่งกระตุ้น: <p style="text-align: center;">จุฬาลงกรณ์มหาวิทยาลัย CHULALONGKORN UNIVERSITY</p>		
ความสัมพันธ์: ความเกี่ยวเนื่อง: การรวม: การขยาย: การรับทอดคุณสมบัติ:		
ขั้นตอนทำงานปกติ: <ol style="list-style-type: none"> 1. เจ้าหน้าที่คลังสารสนเทศกลางเข้าสู่ระบบ 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. เจ้าหน้าที่คลังสารสนเทศกลางเลือกเมนูผู้ใช้และหน่วยงาน 		

4. เจ้าหน้าที่คลังสารสนเทศกลางเลือกเมนูย่อยผู้ใช้งานในระบบ
5. เจ้าหน้าที่คลังสารสนเทศกลางเลือกกดปุ่มแก้ไขชื่อผู้ใช้งานที่ต้องการมอบหมายสิทธิ
6. เจ้าหน้าที่คลังสารสนเทศกลางเลือกบทบาทให้กับผู้ใช้งาน
7. เจ้าหน้าที่คลังสารสนเทศกลางบันทึกการมอบหมายสิทธิให้กับผู้ใช้งาน
ขั้นตอนการทำงานย่อย:
ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):

ตารางที่ จ.5 คำอธิบายแผนภาพยูสเคสการบันทึกค่าไพรเวซีข้อมูลเริ่มต้น

ชื่อยูสเคส: บันทึกค่าไพรเวซีข้อมูลเริ่มต้น	รหัส: UCNHC-05	ระดับความสำคัญ: มาก
ผู้กระทำหลัก: เจ้าหน้าที่คลังสารสนเทศกลาง	ประเภทยูสเคส: เชิงละเอียด	
ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์:		
<ul style="list-style-type: none"> - นักวิจัย - นักพัฒนาระบบ - ผู้ดูแลฐานข้อมูล - ตัวแทนหน่วยงาน - ผู้บริหารระดับสูง 		
คำอธิบาย: เป็นยูสเคสทำหน้าที่บันทึกค่าไพรเวซีเริ่มต้นของข้อมูล เพื่อใช้ในการกำหนดค่าไพรเวซีของข้อมูลในกรณีที่เจ้าของข้อมูลไม่ได้กำหนด		
สิ่งกระตุ้น:		
ประเภทสิ่งกระตุ้น:		
ความสัมพันธ์:		
<p>ความเกี่ยวเนื่อง:</p> <p>การรวม:</p> <p>การขยาย:</p> <p>การรับทอดคุณสมบัติ:</p>		
ขั้นตอนทำงานปกติ:		

<ol style="list-style-type: none"> 1. เจ้าหน้าที่คลังสารสนเทศกลางเข้าสู่ระบบ 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. เจ้าหน้าที่คลังสารสนเทศกลางเลือกเมนูตั้งค่าโปรแกรม 4. เจ้าหน้าที่คลังสารสนเทศกลางเลือกแถบโปรแกรมเริ่มต้น 5. เจ้าหน้าที่คลังสารสนเทศกลางเลือกกดปุ่มแก้ไขรายการโปรแกรม 6. เจ้าหน้าที่คลังสารสนเทศกลางเลือกเปลี่ยนสถานะของรายการโปรแกรมและบันทึกโปรแกรมเริ่มต้น
ขั้นตอนการทำงานย่อย:
ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):

ตารางที่ จ.6 คำอธิบายแผนภาพยูสเคสการกำหนดผู้รับผิดชอบนโยบาย

ชื่อยูสเคส: กำหนดผู้รับผิดชอบนโยบาย	รหัส: UCNHC-06	ระดับความสำคัญ: มาก
ผู้กระทำหลัก: เจ้าหน้าที่คลังสารสนเทศกลาง	ประเภทยูสเคส: เชิงละเอียด	
ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์:		
<ul style="list-style-type: none"> - เจ้าหน้าที่คลังสารสนเทศกลาง, นักวิจัย, นักพัฒนาระบบ, ผู้ดูแลฐานข้อมูล, ตัวแทนหน่วยงาน, ผู้บริหารระดับสูง 		
คำอธิบาย: เป็นยูสเคสทำหน้าที่กำหนดผู้รับผิดชอบนโยบายการใช้งานคลังสารสนเทศกลาง เพื่อเป็นข้อมูลสำหรับให้ผู้ใช้งานได้รับทราบข้อมูลการติดต่อสื่อสารกับเจ้าหน้าที่		
<p>สิ่งกระตุ้น:</p> <p>ประเภทสิ่งกระตุ้น:</p>		
<p>ความสัมพันธ์:</p> <p> ความเกี่ยวเนื่อง:</p> <p> การรวม:</p> <p> การขยาย:</p> <p> การรับทอดคุณสมบัติ:</p>		
<p>ขั้นตอนทำงานปกติ:</p> <ol style="list-style-type: none"> 1. เจ้าหน้าที่คลังสารสนเทศเข้าสู่ระบบ 		

<ol style="list-style-type: none"> 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. เจ้าหน้าที่คลังสารสนเทศกลางเลือกเมนูนโยบาย 4. เจ้าหน้าที่เลือกกดปุ่มแก้ไขนโยบายที่ต้องการมอบหมายผู้รับผิดชอบ 5. เจ้าหน้าที่คลังสารสนเทศกลางเลือกชื่อผู้รับผิดชอบ 6. เจ้าหน้าที่คลังสารสนเทศกลางกดปุ่มบันทึกการเปลี่ยนแปลง 7. เครื่องมือสนับสนุนนำเจ้าหน้าที่คลังสารสนเทศกลางกลับมายังหน้านโยบายการใช้งาน
ขั้นตอนการทำงานย่อ:
ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):

ตารางที่ จ.7 คำอธิบายแผนภาพยูสเคสการสร้างหลักสูตรอบรม

ชื่อยูสเคส: การสร้างหลักสูตรอบรม	รหัส: UCNHC-07	ระดับความสำคัญ: มาก
ผู้กระทำหลัก: เจ้าหน้าที่คลังสารสนเทศกลาง	ประเภทยูสเคส: เชิงละเอียด	
ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์: <ul style="list-style-type: none"> - เจ้าหน้าที่คลังสารสนเทศกลาง, นักวิจัย, นักพัฒนาระบบ, ผู้ดูแลฐานข้อมูล, ตัวแทนหน่วยงาน, ผู้บริหารระดับสูง 		
คำอธิบาย: เป็นยูสเคสทำหน้าที่กำหนดค่าเริ่มต้นสำหรับผู้ใช้งานที่ลงทะเบียนเข้าใช้งาน		
สิ่งกระตุ้น: ประเภทสิ่งกระตุ้น:		
ความสัมพันธ์: ความเกี่ยวเนื่อง: การรวม: การขยาย: การรับทอดคุณสมบัติ:		
ขั้นตอนทำงานปกติ: <ol style="list-style-type: none"> 1. เจ้าหน้าที่คลังสารสนเทศเข้าสู่ระบบ 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. เจ้าหน้าที่คลังสารสนเทศกลางกดปุ่มหลักสูตรอบรม 		

<p>4. เจ้าหน้าที่คลังสารสนเทศกลางกดปุ่มเพิ่มหลักสูตรอบรม</p> <p>5. เจ้าหน้าที่กรอกรายละเอียดหลักสูตรอบรม</p> <p>6. เจ้าหน้าที่กำหนดกลุ่มเป้าหมายในการอบรม</p> <p>7. เจ้าหน้าที่ช่วงเวลาให้ผู้ใช้งานได้เข้าร่วมอบรม</p> <p>8. เจ้าหน้าที่บันทึกหลักสูตรอบรม</p>
<p>ขั้นตอนการทำงานย่อย:</p> <p>8.1 ระบบตรวจสอบชื่อหลักสูตรว่ามีอยู่ในระบบหรือไม่</p> <p>8.1.1 ถ้ามีระบบแจ้งเตือนเจ้าหน้าที่คลังสารสนเทศกลางว่ามีหลักสูตรนี้อยู่ในระบบแล้ว</p> <p>8.1.2 ถ้าไม่มีระบบบันทึกหลักสูตรในฐานข้อมูลและแจ้งเตือนเจ้าหน้าที่คลังสารสนเทศกลางว่าบันทึกสำเร็จ</p>
<p>ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):</p>

ตารางที่ จ.8 คำอธิบายแผนภาพยูสเคสบันทึกเข้ารับการอบรม

ชื่อยูสเคส: บันทึกเข้ารับการอบรม	รหัส: UCNHC-08	ระดับความสำคัญ: มาก
ผู้กระทำหลัก: ผู้ใช้งานเครื่องมือสนับสนุน	ประเภทยูสเคส: เชิงละเอียด	
ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์:		
- นักวิจัย, นักพัฒนาระบบ, ผู้ดูแลฐานข้อมูล, ตัวแทนหน่วยงาน, ผู้บริหารระดับสูง		
คำอธิบาย: เป็นยูสเคสทำหน้าที่กำหนดโปรเวซีข้อมูลในแต่ละหน่วยงาน		
สิ่งกระตุ้น:		
ประเภทสิ่งกระตุ้น:		
ความสัมพันธ์:		
<p>ความเกี่ยวเนื่อง:</p> <p>การรวม:</p> <p>การขยาย:</p> <p>การรับทอดคุณสมบัติ:</p>		
ขั้นตอนทำงานปกติ:		

<ol style="list-style-type: none"> 1. ผู้ใช้งานเครื่องมือสนับสนุนเข้าสู่ระบบ 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. ผู้ใช้งานเครื่องมือสนับสนุนกดปุ่มเมนูหลักสูตรอบรม 4. ผู้ใช้งานเครื่องมือสนับสนุนเลือกหลักสูตรอบรมที่ต้องการเข้ารับการอบรม 5. ผู้ใช้งานเครื่องมือสนับสนุนบันทึกการเข้ารับการอบรม
<p>ขั้นตอนการทำงานย่อย:</p> <p>5.1 ระบบแสดงข้อความให้ผู้ใช้งานทราบว่าได้บันทึกการเข้ารับการอบรมสำเร็จ</p>
<p>ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):</p>

ตารางที่ จ.9 คำอธิบายแผนภาพยูสเคสการบันทึกการเก็บรักษาและทำลายข้อมูล

<p>ชื่อยูสเคส: การเก็บรักษาและทำลายข้อมูล</p>	<p>รหัส: UCNHC-09</p>	<p>ระดับความสำคัญ: มาก</p>
<p>ผู้กระทำหลัก: ผู้ใช้งานคลังสารสนเทศกลาง</p>	<p>ประเภทยูสเคส: เจิงละเอียด</p>	
<p>ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์:</p> <p>- ผู้ใช้งานคลังสารสนเทศกลาง</p>		
<p>คำอธิบาย: เป็นยูสเคสทำหน้าที่จัดการกับไพรเวซีของผู้ใช้งานโดยสามารถกำหนดหรือแก้ไขไพรเวซีของผู้ใช้งาน</p>		
<p>สิ่งกระตุ้น:</p> <p>ประเภทสิ่งกระตุ้น:</p>		
<p>ความสัมพันธ์:</p> <p> ความเกี่ยวเนื่อง:</p> <p> การรวม:</p> <p> การขยาย:</p> <p> การรับทอดคุณสมบัติ:</p>		
<p>ขั้นตอนทำงานปกติ:</p> <ol style="list-style-type: none"> 1. เจ้าหน้าที่คลังสารสนเทศกลางเข้าสู่ระบบ 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. เจ้าหน้าที่คลังสารสนเทศกลางเลือกการตั้งค่าไพรเวซี 		

<ol style="list-style-type: none"> 4. เจ้าหน้าที่คลังสารสนเทศกลางเลือกแถบการรักษาและทำลายข้อมูล 5. เจ้าหน้าที่คลังสารสนเทศกลางเลือกข้อมูลที่ต้องการกำหนด 6. เจ้าหน้าที่คลังสารสนเทศกลางเลือกระยะเวลาในการเก็บรักษาและทำลาย 7. เจ้าหน้าที่คลังสารสนเทศกลางกดปุ่มบันทึก
ขั้นตอนการทำงานย่อย:
ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):

ตารางที่ จ.10 คำอธิบายแผนภาพยูสเคสการบันทึกนโยบายการใช้งาน

ชื่อยูสเคส: บันทึกนโยบายการใช้งาน	รหัส: UCNHC-10	ระดับความสำคัญ: มาก
ผู้กระทำหลัก: เจ้าหน้าที่คลังสารสนเทศกลาง	ประเภทยูสเคส: เชิงละเอียด	
ผู้มีส่วนเกี่ยวข้องและการได้ประโยชน์:		
- เจ้าหน้าที่คลังสารสนเทศกลาง		
คำอธิบาย: เป็นยูสเคสทำหน้าที่บันทึกนโยบายการใช้งานของคลังสารสนเทศกลางที่ตระหนักถึงโพรวเวซี ที่ได้รับความเห็นชอบจากผู้บริหาร		
สิ่งกระตุ้น:		
ประเภทสิ่งกระตุ้น:		
ความสัมพันธ์:		
<p>ความเกี่ยวเนื่อง:</p> <p>การรวม:</p> <p>การขยาย:</p> <p>การรับทอดคุณสมบัติ:</p>		
ขั้นตอนทำงานปกติ:		
<ol style="list-style-type: none"> 1. เจ้าหน้าที่คลังสารสนเทศกลางเข้าสู่ระบบ 2. ระบบตรวจสอบสิทธิบทบาทผู้ใช้งาน 3. เจ้าหน้าที่คลังสารสนเทศกลางกดปุ่มนโยบายการใช้งาน 4. เจ้าหน้าที่คลังสารสนเทศกลางกดปุ่มเพิ่ม 5. เจ้าหน้าที่คลังสารสนเทศกลางระบุรายละเอียดเนื้อหาของนโยบายการใช้งาน 		

<p>6. เจ้าหน้าที่คลังสารสนเทศกลางกำหนดผู้รับผิดชอบนโยบายการใช้งาน</p> <p>7. เจ้าหน้าที่คลังสารสนเทศกลางกวดปุ่มบันทึกนโยบายการใช้งาน</p>
<p>ขั้นตอนการทำงานย่อย:</p> <p>7.1 ระบบตรวจสอบเนื้อหา นโยบายว่ามีอยู่ในระบบหรือไม่</p> <p>7.1.1 ถ้ามีระบบแสดงข้อความแจ้งเตือนให้เจ้าหน้าที่คลังสารสนเทศกลางทราบ</p> <p>7.1.2 ถ้าไม่มีระบบบันทึกนโยบายการใช้งานและแสดงข้อความว่าบันทึกสำเร็จให้เจ้าหน้าที่คลังสารสนเทศกลางทราบ</p>
<p>ขั้นตอนการทำงานทางเลือก/พิเศษ (ถ้ามี):</p>



รายการอ้างอิง

1. กรมประชาสัมพันธ์, ส. แกลงข่าวแผนแม่บทการบริหารจัดการทรัพยากรน้ำ. 2012; Available from: http://region6.prd.go.th/ewt_dl_link.php?nid=616.
2. Tavani, H.T., *Informational Privacy: Concepts, Theories, and Controversies*, in *The Handbook of Information and Computer Ethics*. 2009, John Wiley & Sons, Inc. p. 131-164.
3. Clarke, R. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. 2006; Available from: <http://www.rogerclarke.com/DV/Intro.html>.
4. Westin, A.F., *Privacy and Freedom*. 1967, New York: Atheneum. p. 487.
5. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550. Available from: http://www.mict.go.th/ewt_news.php?nid=333.
6. Budget, N.I.o.S.a.T.O.o.M.a. *Federal Enterprise Architecture Security and Privacy Profile Version 3.0*. 2010; Available from: <http://www.cio.gov/documents/fea-security-privacy-profile-v3-09-30-2010.pdf>.
7. Cavoukian, A., *Privacy by Design: The 7 Foundational Principles*. 2010.
8. Covoukian, A. *A Foundational Framework for a Pbd-PIA*. 2011; Available from: <http://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf>.
9. Ann Cavoukian, P.D., *Creation of a Global Privacy Standard*. 2006.
10. Sandhu, R.S., et al., *Role-Based Access Control Models*. Computer, 1996. **29**(2): p. 38-47.
11. Ni, Q., et al., *Privacy-aware role based access control*, in *Proceedings of the 12th ACM symposium on Access control models and technologies*. 2007, ACM: Sophia Antipolis, France. p. 41-50.

12. Yau, S.S. and Y. Yin, *A Privacy Preserving Repository for Data Integration across Data Sharing Services*. *Services Computing, IEEE Transactions on*, 2008. **1**(3): p. 130-140.



ประวัติผู้เขียนวิทยานิพนธ์

ชื่อ ชื่อสกุล ยศพนธ์ เลิศห้ำาเดชานนท์

วัน เดือน ปี เกิด 1 สิงหาคม พ.ศ.2526

ที่อยู่ปัจจุบัน 27 หมู่ 8 ตำบลแม่เปา อำเภอพญาเม็งราย จังหวัดเชียงราย

ที่ทำงาน สถาบันสารสนเทศทรัพยากรน้ำและการเกษตร (องค์การ
มหาชน)

เลขที่ 108 ชั้น 8 อาคารบางกอกไทยเวอร์ ถนนรางน้ำ แขวงถนนพญาไท

เขตราชเทวี กรุงเทพมหานคร

ตำแหน่งหน้าที่ปัจจุบัน เจ้าหน้าที่พัฒนาระบบ

ประวัติการศึกษา พ.ศ.2549 ทล.บ (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยบูรพา