สถาบันนวัตกรรมการเรียนรู้
มหาวิทยาลัยพะเยา

เอกสารความปลอดภัยด้านเทคโนโลยี
สถาบันนวัตกรรมการเรียนรู้ มหาวิทยาลัยพะเยา
พ.ศ. 2566

งานเทคโนโลยีสารสนเทศ สถาบันนวัตกรรมการเรียนรู้ มหาวิทยาลัยพะเยา

คำนำ

สถาบันนวัตกรรมการเรียนรู้ มหาวิทยาลัยพะเยา เป็นหน่วยงานสนับสนุนภารกิจด้านการเรียนการสอนและกิจกรรมอื่นๆ ของมหาวิทยาลัย ที่มีการให้บริการด้านระบบคอมพิวเตอร์และระบบสารสนเทศแก่ผู้ใช้บริการ เช่น ระบบสารสนเทศต่างๆ ระบบห้องสมุดอัตโนมัติ (ALIST) บริการสืบค้นสารสนเทศ (OPAC) ระบบ UP Academy ระบบ UP e-Learning ระบบ UP Podcasts ระบบ UP Digital Collections และเตรียมเอกสารเป็นต้น ซึ่งการให้บริการด้านระบบคอมพิวเตอร์และระบบสารสนเทศนั้น ผู้ให้บริการและผู้ใช้บริการจะต้องดำเนินการในกิจกรรมตามวัตถุประสงค์ของตนเองให้สอดคล้องและไม่ขัดต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมทั้ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์

สถาบันนวัตกรรมการเรียนรู้ จึงกำหนดนโยบายการปฏิบัติงานด้านระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งเป็นสิ่งสำคัญที่จะขับเคลื่อนพันธกิจและการให้บริการของสถาบันนวัตกรรมการเรียนรู้ เป็นไปตามวัตถุประสงค์ไม่ขัดต่อกฎหมายหรือพระราชบัญญัติในส่วนที่เกี่ยวข้อง อีกทั้งยังเป็นการสร้างความเชื่อมั่นให้กับผู้ใช้บริการและผู้มีส่วนเกี่ยวข้องในทุกภาคส่วนรวมถึงเพื่อสร้างความนำเชื่อถือให้กับการดำเนินการปฏิบัติงานด้านคอมพิวเตอร์และสารสนเทศของสถาบันนวัตกรรมการเรียนรู้ มหาวิทยาลัยพะเยา

การกำหนดนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานทราบหน้าที่ความรับผิดชอบ แนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบายและการปฏิบัติตามนโยบาย

สถาบันนวัตกรรมการเรียนรู้ ตระหนักดีถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้จัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติให้ผู้ใช้งานมีความตระหนักถึงความปลอดภัยของเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยของระบบข้อมูลสารสนเทศ และเป็นมาตรการป้องกันความเสี่ยงต่อการเกิดปัญหา รวมทั้งเพื่อให้สอดคล้องกับนโยบายความปลอดภัยด้านอื่นๆ ที่มุ่งเน้นการปฏิบัติงานภายในสถาบันนวัตกรรมการเรียนรู้ ให้มีความมั่นคงปลอดภัย

งานเทคโนโลยีสารสนเทศ
สถาบันนวัตกรรมการเรียนรู้

สารบัญ

	หน้า
คำนำ	ก
สารบัญ	ข
ขอบเขตของงาน	
การแบ่งแยกอำนาจหน้าที่	1
การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย	7
แบบฟอร์มการขอบัญชีผู้ใช้เพื่อใช้งานระบบสารสนเทศ	16
แบบฟอร์มการขอติดตั้งซอฟท์แวร์	17
แบบฟอร์มการตรวจสอบระบบและอุปกรณ์ต่อพ่วง	18
แบบคำร้องขอดูข้อมูลย้อนหลังระบบกล้องวงจรปิด	19
ขั้นตอนการขอบัญชีผู้ใช้	20
การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์	21
รายละเอียดขั้นตอนการดำเนินงานพัฒนาระบบสารสนเทศ	23
เอกสารขั้นตอนการขอพัฒนาโปรแกรม	40
เอกสารขอพัฒนาโปรแกรม	41
ฟอร์มบันทึกข้อผิดพลาดของระบบ	42
ฟอร์มบันทึกขอโอนย้ายระบบ	43
แบบฟอร์มบันทึกระบบการทำงานอัตโนมัติ	44
รายงานการทบทวนสิทธิ์การเข้าใช้งานระบบสารสนเทศ	45
ทะเบียนบันทึกการขออนุมัติระบบ	46
การสำรองข้อมูลและระบบคอมพิวเตอร์และการเตรียมพร้อมกรณีฉุกเฉิน	47
แบบฟอร์มบันทึกการสำรองข้อมูล	59
แบบฟอร์มบันทึกเก็บข้อมูลสำรอง	60
การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์	61

การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

วัตถุประสงค์

การแบ่งแยกอำนาจหน้าที่มีวัตถุประสงค์เพื่อมีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในสถาบันนวัตกรรมการเรียนรู้ ฝ่ายเทคโนโลยีสารสนเทศ และลดความเสี่ยงด้านบริหารจัดการเทคโนโลยีสารสนเทศ (infrastructure risk)

แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control)

การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล

1. ผู้รับผิดชอบระบบสารสนเทศ ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศดังนี้

1.1 ผู้ดูแลระบบ อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ตนต้องใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบข้อมูล และ/หรือ ผู้รับผิดชอบระบบสารสนเทศตามความจำเป็นต่อการใช้งานแล้วเท่านั้น

1.2 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ หมายถึงการขออนุญาตเข้าระบบสารสนเทศนั้น ผู้ใช้จะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารเพื่อขออนุญาตเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจาผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน จากนั้น ผู้ดูแลระบบสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็น และโดยคำนึงถึงประเภทข้อมูล และชั้นความลับ

1.3 ผู้ดูแลระบบ ต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่านเข้าระบบผิด 3 ครั้ง จนกว่าจะยื่นเรื่องพร้อมหลักฐานแสดงความเป็นตัวตนต่อเจ้าหน้าที่ดูแลระบบ เพื่อขอรหัสใหม่อีกครั้ง

1.4 ผู้ดูแลระบบ ต้องกำหนดให้การ Log-in เพื่อเข้าใช้ระบบสารสนเทศใดๆ จะต้องมีการตรวจจับการเปิดระบบสารสนเทศไว้ เมื่อไม่มีการใช้งาน จะทำการ Log-out ระบบให้อัตโนมัติ ในระยะเวลาที่เหมาะสม

1.5 ผู้รับผิดชอบข้อมูลและผู้รับผิดชอบระบบสารสนเทศต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

2. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงาน ต้องกำหนดระบบและอุปกรณ์สนับสนุนการทำงานดังนี้

2.1 มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยที่เพียงพอต่อความต้องการใช้งานโดยมีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

2.2 มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

2.3 ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

3. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงาน ต้องควบคุมการนำอุปกรณ์คอมพิวเตอร์ออกนอกหน่วยงานดังนี้

3.1 ให้มีการขออนุญาตก่อนนำสิ่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วยงาน

3.2 บันทึกข้อมูลการนำสิ่งอุปกรณ์ของกรม ออกนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

4. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงาน ต้องควบคุมการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือการนำ

สื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

4.1 ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะแทงจำหน่ายอุปกรณ์ดังกล่าว โดยปฏิบัติตามแนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

4.2 มีมาตรการหรือเทคนิค ในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญ ในอุปกรณ์สำหรับจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

การบริหารจัดการสิทธิการเข้าถึง

1. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภาย ต้องปฏิบัติเพื่อจัดเก็บข้อมูล ดังนี้

1.1 จัดประเภทของข้อมูล มี 3 ประเภท ดังนี้

1.1.1.ข้อมูลสารสนเทศด้านการบริหาร คือ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำร้อง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี

1.1.2.ข้อมูลสารสนเทศด้านการบริการ คือ ข้อมูลสถิติการใช้งานต่างๆ

1.1.3.ข้อมูลสารสนเทศด้านกฎหมาย คือ ระเบียบ ข้อบังคับ นโยบาย แนวปฏิบัติ และกฎหมายต่างๆ

1.2 จัดแบ่งระดับชั้นการเข้าถึง มี 3 ประเภท ดังนี้

1.2.1 ระดับชั้นสำหรับผู้บริหาร

1.2.2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

1.2.3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

1.3 การกำหนดช่องทางที่สามารถเข้าถึงได้ ผู้ดูแลระบบบริหารจัดการให้มีการรักษาความปลอดภัยอย่างเหมาะสม สำหรับการเข้าถึงระบบงานสารสนเทศด้วยช่องทาง 3 ช่องทาง ดังนี้

1.3.1 ทางการเชื่อมต่อด้วยสายสัญญาณ (Wired Access)

1.3.2 ทางการเชื่อมต่อด้วยเครือข่ายไร้สาย (Wireless Access)

1.3.3 ทางการเข้าถึงตรงที่เครื่องแม่ข่าย (Local Access)

2. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User Registration) โดยกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาต

3. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงาน ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

3.1 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานภายจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

3.2 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบสารสนเทศที่ให้บริการต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ 1 ครั้ง

3.3 กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ โดยกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้

3.3.1 อ่านอย่างเดียว

3.3.2 สร้างข้อมูล

3.3.3 ป้อนข้อมูล

3.3.4 แก้ไข

3.3.5 อนุมัติ

3.3.6 ไม่มีสิทธิ

4. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่ดังนี้

4.1 กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานสารสนเทศเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

4.2 จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอใช้ระบบไว้เพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

4.3 ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้งเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ผู้บังคับบัญชาหน่วยงาน ต้องจัดให้มีวิธีการจัดการ การเข้าถึงข้อมูลตามระดับชั้นความลับ ในการกำหนดชั้นความลับของข้อมูล จึงกำหนดให้มีแนวทางปฏิบัติ ดังนี้

1. ประเภทของข้อมูล แบ่งออกเป็น 2 ประเภท ดังนี้

1.1 ข้อมูลประเภทเอกสาร ได้แก่ ข้อมูลที่มีการเขียนหรือพิมพ์ลงบนกระดาษ

1.2 ข้อมูลประเภทอิเล็กทรอนิกส์ ได้แก่ ไฟล์ข้อมูลต่างๆ

2. ลำดับความสำคัญ หรือ ลำดับชั้นความลับของข้อมูล แบ่งออกเป็น ระดับ ดังนี้

2.1 ลับ (Top Secret / Secret / Confidential)

2.2 ใช้ภายในเท่านั้น (Internal Use)

2.3 ส่วนบุคคล (Personal)

2.4 เปิดเผยได้ (Public)

3. ระดับชั้นการเข้าถึง แบ่งออกเป็น 3 ระดับ ดังนี้

3.1 ระดับชั้นสำหรับผู้บริหาร

3.2 ระดับชั้นสำหรับผู้ดูแลระบบ หรือ ผู้ที่ได้รับมอบหมาย

3.3 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

4. ช่องทางการเข้าถึงการกำหนดจำนวนช่องทางในการเข้าถึงระบบสารสนเทศ ต้องกำหนดให้เข้าถึงได้ทั้งภายใน และภายนอก โดยเชื่อมต่อผ่าน เครือข่ายคอมพิวเตอร์ไร้สาย (Wifi), เครือข่ายคอมพิวเตอร์มีสาย (Lan), อินเทอร์เน็ต (Internet) และมีการติดต่อด้วยตนเอง โทรศัพท์ หรือโทรสาร, หนังสือหรือบันทึกข้อความ, จดหมายอิเล็กทรอนิกส์ (E-mail) สำหรับ อินเทอร์เน็ต (Internet) เป็นช่องทาง ให้เข้าถึงได้เฉพาะภายในเท่านั้น

5. ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

5.1 จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและต้องแสดงชั้นความลับบนไฟล์ข้อมูลลับ โดยต้องแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

5.2 การสำเนาข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล

5.3 ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยคำนึงถึงการป้องกันด้วยวิธี ดังนี้

5.3.1 การใช้รหัสผ่านที่มีความมั่นคงปลอดภัย

5.3.2 การอัพเดทข้อมูลในระบบป้องกันไวรัสอย่างสม่ำเสมอ

5.3.3 การติดตั้งโปรแกรมแก้ไขช่องโหว่เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์

5.4 ห้ามแบ่งปัน (Share) ไฟล์ข้อมูลลับบนเครือข่าย เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะ

ได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการแบ่งปัน Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

5.5 ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

5.6 ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดิสก์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

ภาระงานงานเทคโนโลยีสารสนเทศ

หน้าที่ความรับผิดชอบหลักที่เป็นงานประจำ

1. งานควบคุม ดูแล บำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย และ ระบบเครือข่าย

1.1 ดูแลเครื่องคอมพิวเตอร์แม่ข่าย (Server) ต่าง ๆ ภายในสถาบันนวัตกรรมการเรียนรู้

1.2 สำรองฐานข้อมูลและกู้คืนข้อมูลที่สำคัญต่าง ๆ

1.3 ประสานงานกับหน่วยงานอื่นทั้งภายในและภายนอกที่เกี่ยวข้องกับหน่วยระบบเทคโนโลยีสารสนเทศ เมื่อมีปัญหาด้านการใช้งานเครือข่าย

2. งานควบคุม ดูแล บำรุงรักษาครุภัณฑ์คอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ มีหน้าที่ดังนี้

2.1. ดูแลคอมพิวเตอร์สำหรับให้บริการทั้งหมด 121 เครื่อง

2.2. ดูแลการให้บริการอินเทอร์เน็ต (Internet) แก่ผู้ใช้บริการเพื่อค้นหาข้อมูลต่างๆ

2.3. บริการให้กับบุคลากรภายในหน่วยงาน ซึ่งมีปัญหาด้าน Hardware Software เพื่อให้คอมพิวเตอร์ครุภัณฑ์และโปรแกรมคอมพิวเตอร์ทำงานได้เป็นปกติมีประสิทธิภาพในการใช้งานอยู่เสมอและสามารถให้บริการแก่ผู้ใช้บริการได้อย่างต่อเนื่องโดยไม่ติดขัดหรือเกิดปัญหา

2.4. ดูแลเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ภายในสถาบันนวัตกรรมการเรียนรู้ และอุปกรณ์ต่างๆ เช่น เครื่องพิมพ์ (Printer) เครือข่ายอินเทอร์เน็ต (Internet),เครือข่ายคอมพิวเตอร์ไร้สาย (Wi-Fi) เป็นต้น

2.5. จัดหาอุปกรณ์อิเล็กทรอนิกส์ต่างๆ เพื่อใช้ในการส่งเสริมการปฏิบัติงานของเจ้าหน้าที่ภายในสถาบันนวัตกรรมการเรียนรู้

2.6. ดูแลการยืม-คืน ครุภัณฑ์คอมพิวเตอร์และวัสดุอุปกรณ์คอมพิวเตอร์

2.7. ดูแลโปรแกรมคอมพิวเตอร์ต่าง ๆ ที่เกี่ยวข้องกับการบริการของสถาบันนวัตกรรมการเรียนรู้

2.8. บริการให้คำปรึกษาและแก้ปัญหาเบื้องต้นในการใช้เทคโนโลยีสารสนเทศของสถาบันนวัตกรรมการเรียนรู้

3. งานจัดการระบบห้องสมุดอัติโนมัติ

3.1 ดูแลระบบห้องสมุดอัตโนมัติ ALIST ในส่วนของโมดูล Administrator

3.2 ติดตั้งโปรแกรมให้ศูนย์บรรณสาร ฯ และห้องสมุดคณะต่าง ๆ ภายในมหาวิทยาลัยพะเยา

3.3 ดูแลและควบคุมระบบการสืบค้นข้อมูลภายในศูนย์บรรณสารฯ (OPAC)

3.4 ดูแลและควบคุมระบบการสืบค้นข้อมูลภายในศูนย์บรรณสารฯ ผ่านโทรศัพท์มือถือสมาร์ทโฟน Mobile Apps

3.5 แก้ไขปัญหาเบื้องต้นในการใช้ระบบห้องสมุดอัตโนมัติ ALIST

4. งานพัฒนาระบบสารสนเทศและเว็บไซต์ มีหน้าที่ดังนี้

4.1 พัฒนาระบบสารสนเทศและการทดสอบโปรแกรมตามที่ได้รับมอบหมาย

4.2 ดูแลและปรับปรุงเว็บไซต์ศูนย์บรรณสารและการเรียนรู้

4.3 ประยุกต์ใช้ เทคโนโลยีสารสนเทศ ตามหน่วยงานที่ร้องขอมาเพื่อให้ช่วยเพิ่มประสิทธิภาพในการทำงาน

5. งานบริการโสตทัศนูปกรณ์ มีหน้าที่ดังนี้

5.1 ดูแลเครื่องมืออุปกรณ์งานโสตทัศนวัสดุ ของสถาบันนวัตกรรมการเรียนรู้ ดูแลอุปกรณ์โสตทัศนวัสดุในห้องประชุม เช่น เครื่องฉายโปรเจคเตอร์ จอภาพโปรเจคเตอร์ เครื่องเสียง เป็นต้น

5.2 ควบคุมระบบสื่อโสตทัศนูปกรณ์ห้องประชุม

5.3 จัดหา ดูแล รักษา ซ่อมแซม โสตทัศนูปกรณ์

5.4 ให้คำปรึกษา แนะนำในด้านการใช้ โสตทัศนูปกรณ์ มีหน้าที่ดังนี้

6. งานความปลอดภัยด้านเทคโนโลยีสารสนเทศ

6.1 จัดทำเอกสารเกี่ยวกับนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

6.2 ตรวจสอบ ควมคุมการดำเนินงานด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามแผนหรือกำหนดการ

6.3 ควบคุม ดูแลระบบรักษาความปลอดภัยกล้องโทรทัศน์วงจรปิด (closed circuit television :CCTV)

6.4 ควบคุมดูแล ระบบ RFID ศูนย์บรรณสารและการเรียนรู้

ตารางกำหนดผู้รับผิดชอบการแบ่งอำนาจหน้าที่

ลำดับ	เนื้อหา	ผู้รับผิดชอบ	หมายเหตุ
1.	การควบคุมการเข้าถึงระบบ (Access Control Policy) 1.1 กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสาร สนเทศ จะต้องขออนุญาตต่อผู้ดูแลระบบ (System Administrator)	หัวหน้างาเทคโนโลยีสารสนเทศ	
	1.2. จัดกลุ่มบุคลากรที่ปฏิบัติหน้าที่ในส่วนของการพัฒนาระบบ (Developer) ออกจากการทำหน้าบริหารระบบ (System Administrator) ซึ่งปฏิบัติงานในส่วนของระบบที่ใช้งานจริง	หัวหน้างานเทคโนโลยีสารสนเทศ	
	1.3. กำหนดสิทธิ์ในการเข้าถึงข้อมูลและระบบ ให้เหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้รวมถึงต้องมีการตรวจทานสิทธิ์การใช้งานอยู่เสมอ	หัวหน้างานเทคโนโลยีสารสนเทศ	
	1.4. บันทึกรายละเอียดการเข้าถึงระบบ การแก้ไข เปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออก สถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลัก ฐานในการตรวจสอบ	หัวหน้างานเทคโนโลยีสารสนเทศ	
	1.5. กำหนดขั้นตอนในการลงทะเบียนบุคคลากรใหม่ ให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิ์ใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติในการยกเลิกสิทธิ์ เช่น กรณีลาออก หรือเปลี่ยนแปลงตำแหน่งงาน เป็นต้น	หัวหน้างานเทคโนโลยีสารสนเทศ	
	1.6. กำหนดการใช้งานเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ประยุกต์ (Application),จดหมายอิเล็กทรอนิกส์ (E-Mail), ระบบเครือข่ายไร้สาย(Wireless) ,ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ รวมทั้งต้องตรวจสอบสิทธิ์ดังกล่าวอย่างสม่ำเสมอ	หัวหน้างานเทคโนโลยีสารสนเทศ	

ลำดับ	เนื้อหา	ผู้รับผิดชอบ	หมายเหตุ
2.	การบริหารจัดการการเข้าถึงระบบสารสนเทศ 2.1. บริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้		
	2.1.1 การกำหนดสิทธิ์ผู้ใช้ของบุคลากรใหม่ ต้องได้รับการร้องขอเป็นลายลักษณ์อักษร และต้องได้รับการอนุมัติจากผู้ดูแลระบบสูงสุด (Super System Administrator) ก่อนดำเนินการเสมอ	หัวหน้างานเทคโนโลยีสารสนเทศ	
	2.1.2 กำหนดให้ทำการยกเลิกการใช้งานสำหรับทุก User ID ของผู้ใช้งานที่พ้นสภาพจากการจ้างงานแล้ว ซึ่งต้องได้รับการแจ้งจากฝ่ายบุคคลและได้รับการอนุมัติจากผู้ดูแลระบบสูงสุด (Super System Administrator) หลัง จากดำเนินการแล้วเสร็จ ต้องมีเอกสารเป็นลายลักษณ์อักษร	เจ้าหน้าที่งานเทคโนโลยีสารสนเทศ	
	2.1.3 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุดต้องกำหนดระยะเวลาการใช้งานเริ่มต้นและสิ้นสุดเป็นลายลักษณ์อักษรอย่างชัดเจน โดยได้รับการอนุมัติจากผู้มีอำนาจสูงสุดในสายงาน และผู้ดูแลระบบสูงสุดเมื่อครบเวลาที่กำหนดจะถูกระงับการใช้สิทธิ์นั้นทันที	หัวหน้างานเทคโนโลยีสารสนเทศ	
	2.1.4 กำหนดให้มีการทบทวนความมีตัวตนของผู้ใช้งานโดยให้ฝ่ายบุคคลร่วมยืนยันสถานภาพของทุก User ID ของทุกระบบ	หัวหน้างานเทคโนโลยีสารสนเทศ	
	2.3. มีการกำหนดความรับผิดชอบในระบบสารสนเทศ (IT Scope) อย่างชัดเจน	หัวหน้างานเทคโนโลยีสารสนเทศ	

การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย
(Information and Network Security)

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้องเพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious Code ต่าง ๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

แนวทางปฏิบัติการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย

1. การบริหารจัดการข้อมูล

1.1. กำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

1.2. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น

1.3. มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

1.4. มีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

2. การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)

2.1. ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application System) สิทธิการใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

2.2. ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิพิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิพิเศษมีความรัดกุมเพียงพอหรือไม่นั้น สำนักงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

2.2.1. ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่

2.2.2. ควรควบคุมการใช้งาน User ที่มีสิทธิพิเศษอย่างเข้มงวด

2.2.3. ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

2.2.4. ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

2.3. ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่

มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

2.4. ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share Files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

2.5. ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

3.1. มีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ เช่น กำหนดรหัสผ่านที่ยากแก่การคาดเดา และกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง โดยพิจารณาการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมรัดกุมโดยมีรายละเอียดดังนี้

3.1.1. ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 6 ตัวอักษร

3.1.2.ควรใช้อักขระพิเศษประกอบ เช่น : ; < > * _ - เป็นต้น

3.1.3.สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 6 เดือน ส่วนผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริหารระบบ (System Administrator) และผู้ใช้งานที่ติดมากับระบบ (Default user) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 3 เดือน

3.1.4.ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้ายในการเปลี่ยนรหัสผ่านแต่ละครั้ง

3.1.5.การกำหนดรหัสผ่านควร ประกอบด้วย ตัวพิมพ์ใหญ่ พิมพ์เล็ก อักขระพิเศษ

3.1.6.ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “123456” เป็นต้น

3.1.7.ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น

3.1.8.ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

3.1.9.ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 5 ครั้ง

3.1.10. ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น

3.1.11. ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

3.1.12. ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

3.2. ตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญ อย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว หรือ บัญชีรายชื่อของเจ้าหน้าที่ที่ลาออกแล้ว พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือ เปลี่ยน Password เป็นต้น

4. การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

4.1. มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่

พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

4.2. เปิดใช้บริการ (Service) เท่าที่จำเป็น หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

4.3. ดำเนินการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS และ Web Server เป็นต้น อย่างสม่ำเสมอ

4.4. ทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

4.5. มีแนวทางปฏิบัติในการใช้งาน Software Utility เช่น Personal Firewall Password Cracker เป็นต้น และตรวจสอบการใช้งาน Software Utility อย่างสม่ำเสมอ

4.6. กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน

5. การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)

5.1. แบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก เป็นต้น

5.2. มีระบบป้องกันการบุกรุก เช่น firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก

5.3. มีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

5.3.1.ความพยายามในการบุกรุกผ่านระบบเครือข่าย

5.3.2.การใช้งานในลักษณะที่ผิดปกติ

5.3.3.การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

5.4. จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.5. ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า Parameter ต่างๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physical Disconnect) และจุดเชื่อมต่อ (Disable Port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง

5.6. ในกรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ Remote Access หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้ Modem (Dial Out) ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และมีการควบคุมอย่างเข้มงวด เช่น การใช้ระบบ Call Back การควบคุมการเปิดปิด Modem การตรวจสอบตัวตนจริงและสิทธิของผู้ใช้งานการบันทึกราย ละเอียดการใช้งาน และในกรณี Dial Out ก็ควรตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อออกจากระบบเครือข่ายภายใน เป็นต้น รวมทั้งต้องตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว

5.7. กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ก็ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

5.8. การใช้เครื่องมือต่างๆ (Tools) เพื่อตรวจเช็คระบบเครือข่าย ควรได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และ

จำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6. การบริหารการเปลี่ยนแปลงระบบคอมพิวเตอร์ (configuration management)

6.1. ก่อนการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์ ควรมีการประเมินผลกระทบที่เกี่ยวข้อง และบันทึกการเปลี่ยนแปลงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ

6.2. ควรติดตั้งซอฟต์แวร์เท่าที่จำเป็นแก่การใช้งาน และถูกต้องตามลิขสิทธิ์

7. การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (capacity planning)

มีการประเมินการใช้งานระบบคอมพิวเตอร์สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต

8. การป้องกันไวรัส และ malicious code

8.1. มีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น

8.2. ฝ่ายคอมพิวเตอร์จัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งานเพื่อใช้เป็นแนวทางปฏิบัติ รวมทั้งแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ๆ อย่างสม่ำเสมอ

8.3. ควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (Disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้ และควรแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีไวรัส

9. บันทึกเพื่อการตรวจสอบ (Audit Logs)

9.1. ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (Login-logout Logs) บันทึกการพยายามเข้าสู่ระบบ (login Attempts) บันทึกการใช้ Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน

9.2. ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

9.3. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

กระบวนการการทำงาน (Work Flow) การขอติดตั้งซอฟท์แวร์

ขั้นตอนการปฏิบัติงาน

รายละเอียดในการดำเนินการตามขั้นตอน ดังนี้

1.ผู้ขอใช้งานกรอกแบบฟอร์มขอติดตั้งซอฟท์แวร์งานเทคโนโลยีสารสนเทศให้ถูกต้องและครบถ้วน และยื่นแบบฟอร์มแก่เจ้าหน้าที่

2.เจ้าหน้าที่ทำการตรวจสอบความถูกต้องของข้อมูลที่กรอกในฟอร์ม และสิทธิ์การใช้งาน

3.เจ้าหน้าที่ดำเนินการติดตั้งซอฟท์แวร์

4.เจ้าหน้าที่แจ้งผลการดำเนินการและรายละเอียดต่างๆ ให้แก่ผู้ขอใช้งาน

ลำดับ	ผังกระบวนการ	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา	แบบฟอร์ม	เอกสารอ้างอิง
	เริ่มต้น					
1	กรอกแบบฟอร์ม หรือ แก้ไขแบบฟอร์ม	ผู้ขอใช้งานกรอกแบบฟอร์มฯ หรือ แก้ไขแบบฟอร์ม	ผู้ขอใช้บริการ	15 นาที	แบบฟอร์มขอติดตั้งซอฟท์แวร์งานเทคโนโลยีสารสนเทศ	
2	ตรวจสอบ (ไม่ใช่ / ใช่)	เจ้าหน้าที่ตรวจสอบความถูกต้องข้อมูลในแบบฟอร์มและสิทธิ์การใช้งาน	เจ้าหน้าที่	1 ชั่วโมง		
3	ดำเนินการติดตั้งซอฟท์แวร์	เจ้าหน้าที่ดำเนินการติดตั้งซอฟท์แวร์	เจ้าหน้าที่	1 ชั่วโมง		
4	แจ้งผลการดำเนินการ	เจ้าหน้าที่แจ้งผลการตรวจสอบแก่ผู้ขอใช้บริการ	เจ้าหน้าที่	15 นาที		
	สิ้นสุด					

กระบวนการการทำงาน (Work Flow) การตรวจสอบระบบและอุปกรณ์ต่อพ่วง

ขั้นตอนการปฏิบัติงาน

รายละเอียดในการดำเนินการตามขั้นตอน ดังนี้

1.เจ้าหน้าที่เจ้าหน้าที่ดำเนินการตรวจสอบระบบและการทำงานของอุปกรณ์ พร้อมทั้งกรอกข้อมูลในแบบฟอร์ม

2.หัวหน้างานตรวจสอบและประเมินความถูกต้องของข้อมูลในแบบฟอร์มกับการทำงานของระบบและอุปกรณ์ต่อพ่วงที่มีการใช้งานอยู่ในปัจจุบัน

3.เจ้าหน้าที่แจ้งผลการดำเนินการและรายละเอียดต่างๆ ให้แก่ผู้บริหารที่เกี่ยวข้องรับทราบ

ลำดับ	ผังกระบวนการ	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา	แบบฟอร์ม	เอกสารอ้างอิง
	เริ่มต้น					
1	ตรวจสอบระบบและอุปกรณ์ และกรอกแบบฟอร์ม	เจ้าหน้าที่ดำเนินการตรวจสอบระบบและการทำงานของอุปกรณ์ พร้อมทั้งกรอกข้อมูลในแบบฟอร์	เจ้าหน้าที่	1 วัน	แบบฟอร์มการตรวจสอบระบบและอุปกรณ์ต่อพ่วง	
2	ตรวจสอบ (ไม่ใช่ / ใช่)	หัวหน้างานตรวจสอบความถูกต้องของข้อมูลและการทำงานปัจจุบัน	หัวหน้างาน	1 ชั่วโมง		
3	แจ้งผลการดำเนินการ	หัวหน้างานแจ้งผู้บริหารระบบสูงที่เกี่ยวข้อง	หัวหน้างาน	1 วัน		
	สิ้นสุด					

กระบวนการการทำงาน (Work Flow) การขอบัญชีผู้ใช้เพื่อใช้งานระบบสารสนเทศ

ขั้นตอนการปฏิบัติงาน

รายละเอียดในการดำเนินการตามขั้นตอน ดังนี้

1.ผู้ขอใช้งานกรอกแบบฟอร์มขอบัญชีผู้ใช้เพื่อใช้งานระบบสารสนเทศให้ถูกต้องและครบถ้วน และยื่นแบบฟอร์มแก่เจ้าหน้าที่

2.เจ้าหน้าที่ทำการตรวจสอบความถูกต้องของข้อมูลที่กรอกในฟอร์ม และตรวจสอบความพร้อมการให้บริการของระบบ แล้วส่งแบบฟอร์มและแจ้งรายละเอียดให้หัวหน้างาน

3.หัวหน้างานทำการตรวจสอบความถูกต้องและเหมาะสมของสิทธิ์การใช้งาน พร้อมให้ความเห็น และนำเสนอต่อผู้อำนวยการ

4.ผู้อำนวยการตรวจสอบความถูกต้อง และพิจารณาอนุมัติ

5.เจ้าหน้าที่ดำเนินการเพิ่มบัญชีผู้ใช้ในระบบสารสนเทศที่ขอใช้งาน

6.เจ้าหน้าที่แจ้งผลการดำเนินการและรายละเอียดต่างๆ ให้แก่ผู้ขอใช้งาน

ลำดับ	ผังกระบวนการ	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา	แบบฟอร์ม	เอกสารอ้างอิง
	เริ่มต้น					
1	กรอกแบบฟอร์ม หรือ แก้ไขแบบฟอร์ม	ผู้ขอใช้งานกรอกแบบฟอร์มฯ หรือ แก้ไขแบบฟอร์ม	ผู้ขอใช้บริการ	15 นาที	แบบฟอร์มขอบัญชีผู้ใช้เพื่อใช้งานระบบสารสนเทศ	
2	ตรวจสอบ ไม่ใช่	เจ้าหน้าที่ตรวจสอบความถูกต้องข้อมูลในแบบฟอร์มและการทำงานของระบบ	เจ้าหน้าที่	1 ชั่วโมง		
3	ใช่ ตรวจสอบ ไม่ใช่	หัวหน้างานตรวจสอบสิทธิ์และความถูกต้อง	หัวหน้างาน	1 ชั่วโมง		
4	อนุมัติ ไม่ใช่	ผู้อำนวยการตรวจสอบและพิจารณาอนุมัติ	ผู้อำนวยการ	1 วัน		

5	ดำเนินการเพิ่มบัญชีผู้ใช้	เจ้าหน้าที่ดำเนินการเพิ่มบัญชีผู้ใช้	เจ้าหน้าที่	1 ชั่วโมง		
6	แจ้งผลการดำเนินการ	เจ้าหน้าที่แจ้งผลการตรวจสอบแก่ผู้ขอใช้บริการ	เจ้าหน้าที่	15 นาที		
	สิ้นสุด					

กระบวนการการทำงาน (Work Flow) การขอดูข้อมูลย้อนหลังระบบกล้องวงจรปิด

ขั้นตอนการปฏิบัติงาน

รายละเอียดในการดำเนินการตามขั้นตอน ดังนี้

1. ผู้ร้องขอกรอกแบบคำร้องขอดูข้อมูลย้อนหลังระบบกล้องวงจรปิด สถาบันนวัตกรรมการเรียนรู้ให้ถูกต้องและครบถ้วน และยื่นแบบคำร้องแก่เจ้าหน้าที่
2. เจ้าหน้าที่ทำการตรวจสอบความถูกต้องของข้อมูลที่กรอกในแบบคำร้องขอ และการทำงานของระบบกล้องวงจรปิดในบริเวณที่ผู้ร้องขอแจ้ง
3. หัวหน้างานตรวจสอบความถูกต้องและประเมินความเหมาะสม แล้วนำเสนอต่อผู้อำนวยการเพื่อพิจารณาอนุญาต
4. ผู้อำนวยการตรวจสอบความถูกต้อง แล้วพิจารณาอนุญาต
5. เจ้าหน้าที่ดำเนินการตรวจสอบข้อมูลกล้องวงจรปิดย้อนหลังให้กับผู้ร้องขอ
6. เจ้าหน้าที่แจ้งผลการตรวจสอบแก่ผู้ขอใช้ร้องขอ

ลำดับ	ผังกระบวนการ	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา	แบบฟอร์ม	เอกสารอ้างอิง
	เริ่มต้น					
1	กรอกแบบฟอร์ม หรือ แก้ไขแบบฟอร์ม	ผู้ร้องขอกรอแบบคำร้องขอฯ หรือ แก้ไขแบบคำร้อง	ผู้ขอใช้บริการ	15 นาที	แบบคำร้องขอดูข้อมูลย้อนหลังระบบกล้องวงจรปิด	
2	ตรวจสอบ (ไม่ใช่)	เจ้าหน้าที่ตรวจสอบความถูกต้องข้อมูลในแบบคำร้องขอและการทำงานของระบบกล้อง	เจ้าหน้าที่	10 นาที		
3	ใช่ ตรวจสอบ (ไม่ใช่)	หัวหน้างานตรวจสอบและความถูกต้องและเสนอผู้อำนวยการ	หัวหน้างาน	10 นาที		
4	อนุญาต (ไม่ใช่)	ผู้อำนวยการตรวจสอบและพิจารณาอนุญาต	ผู้อำนวยการ	1 วัน		
5	ดำเนินการตรวจสอบข้อมูลกล้องวงจรปิดย้อนหลัง	เจ้าหน้าที่ดำเนินการตรวจสอบข้อมูลกล้องวงจรปิดย้อนหลัง	เจ้าหน้าที่	1 ชั่วโมง		
6	แจ้งผลการดำเนินการ	เจ้าหน้าที่แจ้งผลการตรวจสอบแก่ผู้ขอใช้ร้องขอ	เจ้าหน้าที่	15 นาที		
	สิ้นสุด					

Upili-it02.01

แบบฟอร์มการขอบัญชีผู้ใช้ (User Account)
เพื่อใช้งานระบบสารสนเทศ สถาบันนวัตกรรมการเรียนรู้

วันที่ .....

ประเภทของผู้ใช้บริการ

☐ สายวิชาการ (Academic) ☐ สายสนับสนุน (Official)

ประเภทพนักงาน

☐ พนักงานมหาวิทยาลัย (UP Personnel)

☐ ลูกจ้างชั่วคราวของมหาวิทยาลัยหรือหน่วยงาน (Temporary Employee)

☐ อื่นๆ (ผู้ทรงคุณวุฒิ/อาจารย์พิเศษ) (Other).....

เลขบัตรประชาชน/PassportID.....

ชื่อ-นามสกุล (ภาษาไทย).....

ชื่อ-นามสกุล (ภาษาอังกฤษ : English).....

ตำแหน่ง (Position).....

สังกัด คณะ/กอง/ศูนย์/วิทยาลัย (Division).....

งาน/ภาควิชา (Department).....

เบอร์โทรศัพท์ (Phone No.).....โทรศัพท์มือถือ (Mobile No.).....

อีเมล์ส่วนตัว (e-Mail).....

ข้าพเจ้าขอยืนยันว่าจะใช้บริการ User Account เพื่องานด้านการศึกษาและการปฏิบัติงานเท่านั้น ข้าพเจ้า ทราบดีว่า การใช้งาน User Account เป็นสิทธิ์ส่วนบุคคล ไม่สามารถให้บุคคลอื่นใช้งานได้

หากข้าพเจ้าใช้งานนอกเหนือไปจากข้อกำหนดของมหาวิทยาลัยข้าพเจ้ายินดีปฏิบัติตามเงื่อนไขของมหาวิทยาลัยทุกประการ

ลงชื่อ.....

(.....)

วันที่.....

การพิจารณาของงานเทคโนโลยีสารสนเทศ	การพิจารณาของผู้อำนวยการ
เรียน ผู้อำนวยการ	☐ อนุมัติ ☐ ไม่อนุมัติ ลงชื่อ..... (ผู้อำนวยการสถาบันนวัตกรรมการเรียนรู้)

แบบฟอร์มการขอติดตั้งซอฟท์แวร์
งานเทคโนโลยีสารสนเทศ สถาบันนวัตกรรมการเรียนรู้

วันที่ .....

ประเภทของผู้ใช้บริการ

☐ สายวิชาการ (Academic) ☐ สายสนับสนุน (Official)

ประเภทพนักงาน

☐ พนักงานมหาวิทยาลัย ☐ ลูกจ้างชั่วคราว ☐ อื่นๆ.....

ชื่อ-นามสกุล.....ตำแหน่ง.....

สังกัด สังกัด คณะ/วิทยาลัย/กอง/ศูนย์.....งาน/ภาควิชา.....

เบอร์โทรศัพท์ (Phone No.).....โทรศัพท์มือถือ (Mobile No.).....

อีเมล์มหาวิทยาลัย (UP-Mail).....อีเมล์ส่วนตัว.....

มีความประสงค์ขอติดตั้งซอฟท์แวร์ สำหรับเครื่องคอมพิวเตอร์ จำนวน.....เครื่อง

หมายเลขเครื่อง (SN).....หมายเลขครุภัณฑ์.....

ซอฟท์แวร์ที่ต้องการติดตั้ง

☐ ระบบปฏิบัติการ Windows ☐ โปรแกรม Microsoft Office ☐ โปรแกรม Endnote

☐ โปรแกรม ALIST ☐ โปรแกรมอื่นๆ ระบุ.....

.....

ลงชื่อ.....

(.....)

วันที่.....

ผลการดำเนินการ	ความเห็นของผู้ขอใช้บริการ
☐ ติดตั้งและทำงานได้ปกติ ☐ ไม่สามารถติดตั้งได้ เนื่องจาก	☐ สามารถใช้งานได้ปกติ ☐ อุปกรณ์ครบถ้วน ลงชื่อ..... (ผู้ขอใช้บริการ)

แบบฟอร์มการตรวจสอบระบบและอุปกรณ์ต่อพ่วง ปีงบประมาณ.....

งานเทคโนโลยีสารสนเทศ สถาบันนวัตกรรมการเรียนรู้

ลำดับที่	รายการตรวจสอบ	เดือน												หมายเหตุ
		ต.ค	พ.ย	ธ.ค	ม.ค	ก.พ	มี.ค	เม.ย	พ.ค	มิ.ย	ก.ค	ส.ค	ก.ย	
1	ระบบเครือข่ายคอมพิวเตอร์ (Intranet & Internet)													
	- สถานะและประสิทธิภาพการทำงาน													
2	เครื่องแม่ข่าย (Server) ที่ให้บริการระบบสารสนเทศ													
	- สถานะและประสิทธิภาพการทำงาน													
	- การปรับปรุง Update Patch													
	- การสำรองข้อมูล (Backup)													
	- การสำรองข้อมูลการทำงาน Log file													
3	ระบบกล้องวงจรปิด (CCTV)													
	- เครื่องบันทึก DVR													
	- กล้อง CCTV													
4	ระบบการให้บริการในหอสมุด													
	- RFID Security Gate													
	- Flap Gate Barrier													
	- เครื่องคอมพิวเตอร์													

ลงชื่อผู้ตรวจสอบ .....

(.....)

วันที่...../...../.....

ลงชื่อหัวหน้างาน .....

(.....)

วันที่...../...../.....

แบบคำร้องขอดูข้อมูลย้อนหลังระบบกล้องวงจรปิด
สถาบันนวัตกรรมการเรียนรู้

วันที่ .....

เรียน ผู้อำนวยการสถาบันนวัตกรรมการเรียนรู้

ข้าพเจ้า (นาย/นาง/นางสาว).....เลขบัตรประชาชน.....

ที่อยู่ตามทะเบียนบ้านเลขที่.....หมู่ที่.....ตำบล/แขวง.....อำเภอ.....

จังหวัด.....รหัสไปรษณีย์.....หมายเลขโทรศัพท์.....

มีความประสงค์ขอดูข้อมูลย้อนหลังจากระบบกล้องวงจรปิด ในวันที่.....

ช่วงเวลา..... อาคาร.....

บริเวณ.....

เนื่องจาก.....

ข้าพเจ้าขอยืนยันว่า จะไม่นำข้อมูลที่ได้รับไปเผยแพร่หรือแสวงหาประโยชน์ในทางที่ไม่ชอบด้วยกฎหมาย และในกรณีที่เกิดความเสียหายแก่สถาบันนวัตกรรมการเรียนรู้ มหาวิทยาลัยพะเยา จากข้อมูลดังกล่าว ข้าพเจ้าขอยินยอมรับผิดชอบความเสียหายที่เกิดขึ้นในทุกกรณี

จึงเรียนมาเพื่อโปรดพิจารณา

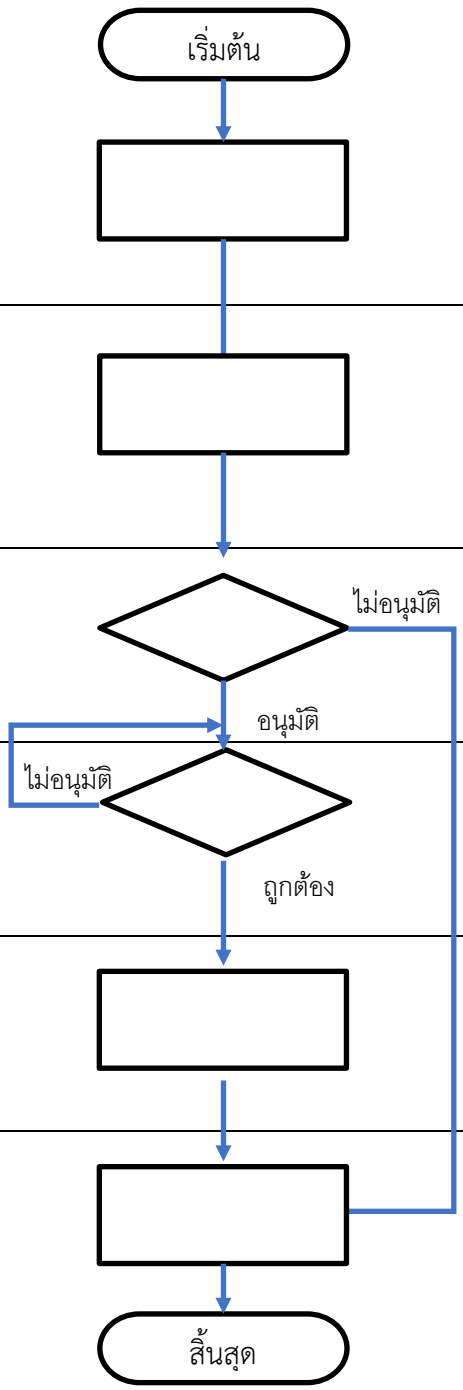
ลงชื่อ.....ผู้ยื่นคำร้อง

(.....)

วันที่.....

การพิจารณาของงานเทคโนโลยีสารสนเทศ	การพิจารณาของผู้อำนวยการ
เรียน ผู้อำนวยการ	☐ อนุมัติ ☐ ไม่อนุมัติ ลงชื่อ..... (ผู้อำนวยการสถาบันนวัตกรรมการเรียนรู้)

ขั้นตอนการขอบัญชีผู้ใช้ (User Account) เพื่อใช้งานระบบสารสนเทศ สถาบันนวัตกรรมการเรียนรู้

รายละเอียด	ขั้นตอน	ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
กรอกแบบฟอร์มการขอใช้บริการ		ผู้ขอใช้บริการ	แบบฟอร์มการขอบัญชีผู้ใช้ (User Account) เพื่อใช้งานระบบสารสนเทศ
ทำเรื่องขอบัญชีผู้ (User Account) ในระบบ DMS พร้อมแนบเอกสารที่กรอก		ผู้ใช้ขอใช้บริการ	
อนุมัติการขอใช้งานในระบบ DMS		ผู้อำนวยการสถาบันฯ	
กำหนดสิทธิ์การใช้งานและตรวจสอบความถูกต้อง		หัวหน้างานเทคโนโลยีสารสนเทศ	
ดำเนินการสร้างบัญชีผู้ใช้		เจ้าหน้าที่งานเทคโนโลยีสารสนเทศ	
แจ้งข้อมูลให้ผู้ขอใช้บริการ		เจ้าหน้าที่งานเทคโนโลยีสารสนเทศ	

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

วัตถุประสงค์

การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

แนวทางปฏิบัติการควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

1. การกำหนดขั้นตอนการปฏิบัติงาน

1.1. กำหนดมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบและขั้นตอนในการโอนย้ายระบบงาน

1.2. กำหนดขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) ควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

1.3. สื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

2. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

2.1 การร้องขอ

2.1.1 การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (อาจเป็น Electronic Transaction เช่น Email เป็นต้น) และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หัวหน้าฝ่ายคอมพิวเตอร์ เป็นต้น

2.1.2 ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง

2.1.3 ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ

2.2 การปฏิบัติงานพัฒนาระบบงาน

2.2.1 ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

2.2.2 ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

2.2.3 ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

2.3 การทดสอบ

2.3.1 ผู้ที่ร้องขอและฝ่ายคอมพิวเตอร์ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

2.3.2 ในระบบงานสำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง

2.4 การโอนย้ายระบบงานเพื่อใช้งานจริง

2.4.1 ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

2.4.2 แบ่งแยกหน้าที่ระหว่างผู้แก้ไขโปรแกรมและผู้โอนย้ายโปรแกรมให้ชัดเจน

2.5 การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บเวอร์ชันของระบบงานที่ได้รับการพัฒนา

2.5.1 ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา

2.5.2 ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

2.5.3 ต้องจัดเก็บโปรแกรม version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

2.6 การทดสอบหลังการใช้งาน (Post- implementation Test)

2.6.1 ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

2.7 การสื่อสารการเปลี่ยนแปลง

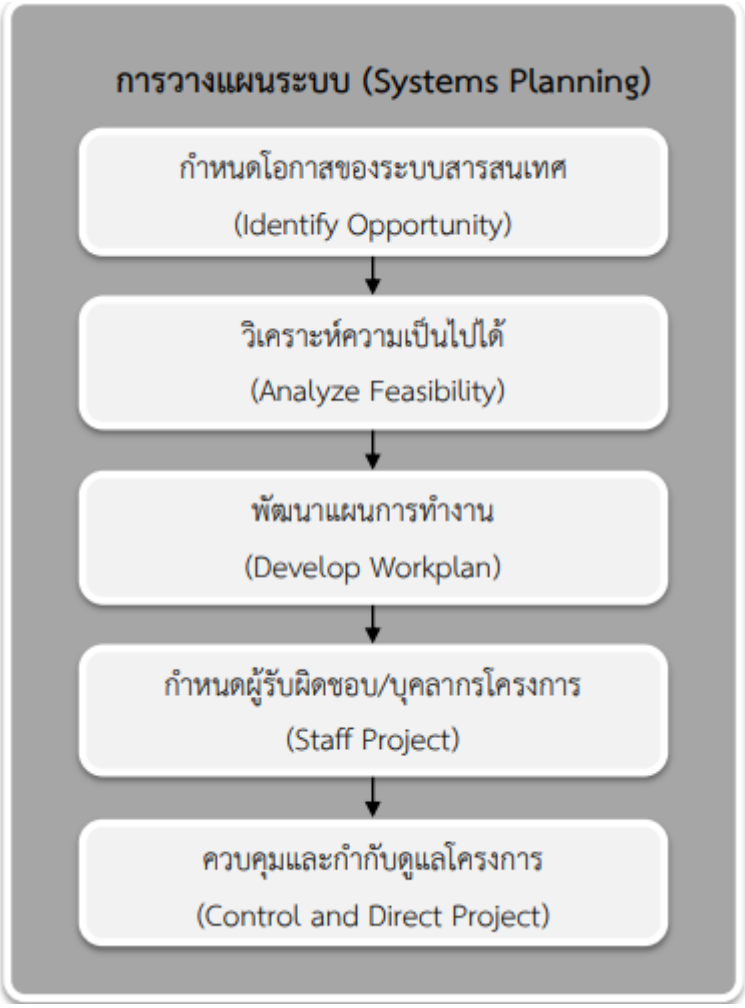
2.7.1 ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

รายละเอียดขั้นตอนการดำเนินงานพัฒนาระบบสารสนเทศ

1. การวางแผนระบบ (Systems Planning)

การวางแผนระบบ (Systems Planning) เป็นขั้นตอนแรกที่สำคัญในการพัฒนาระบบสารสนเทศ

กระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ : กระบวนการย่อยการวางแผนระบบ (Systems Planning)



รูปที่ 1 แสดงขั้นตอนการวางแผนระบบ (Systems Planning)

ขั้นตอนการวางแผนระบบประกอบไปด้วย

1.1 กำหนดโอกาสของระบบสารสนเทศในการใช้งาน (Identify Opportunity) เพื่อ พิจารณาว่าจะพัฒนาระบบสารสนเทศเพื่อใช้กับงานใด เพื่อให้สอดคล้องกับความต้องการจำเป็นของ ผู้ใช้ (User Requirement)

สิ่งที่ต้องดำเนินการ

1. ศึกษาระบบงานปัจจุบัน เป็นการศึกษาปัญหาที่เกิดขึ้น จากการทำงานหรือจาก ระบบเดิมที่ใช้งานอยู่
2. จดบันทึกความต้องการที่จะปรับปรุงเพิ่มเติม

1.2 วิเคราะห์ความเป็นไปได้ (Analyze Feasibility) เพื่อกำหนดขอบเขตของการ พัฒนาระบบ กำหนดรายละเอียดและขั้นตอนของการดำเนินงานและ ระยะเวลาที่ใช้

สิ่งที่ต้องดำเนินการ

1. ศึกษาความเป็นไปได้ในทางเทคนิค เทคโนโลยี อุปกรณ์
2. ศึกษาความเป็นไปได้เกี่ยวกับการนำระบบสารสนเทศที่พัฒนาขึ้นมาใช้ สอดคล้อง ตามความต้องการของผู้ใช้หรือไม่
3. ศึกษาความเป็นไปได้ทางด้านการเงิน

1.3 พัฒนาแผนการทำงาน (Develop Workplan) การจัดทำข้อเสนอโครงการ สำหรับพัฒนาระบบสารสนเทศ การเก็บรวบรวมข้อมูลตามความต้องการของผู้บริหารทุกระดับ และ บุคลากรระดับปฏิบัติการ มาวิเคราะห์เพื่อวางแผนพัฒนาขึ้น พร้อมทั้งสรุปผล และนำเสนอแนวทาง ที่หมาะสมที่สุด เพื่อนำไปวิเคราะห์และออกแบบระบบต่อไป

สิ่งที่ต้องดำเนินการ

1. จัดทำเอกสารข้อเสนอโครงการ และกรอบงาน
2. จัดทำแผนการทำงาน

1.4 กำหนดผู้รับผิดชอบ/ บุคลากรโครงการ (Staff Project) มีการมอบหมาย ผู้รับผิดชอบในงานตามแผนการทำงาน

สิ่งที่ต้องดำเนินการ

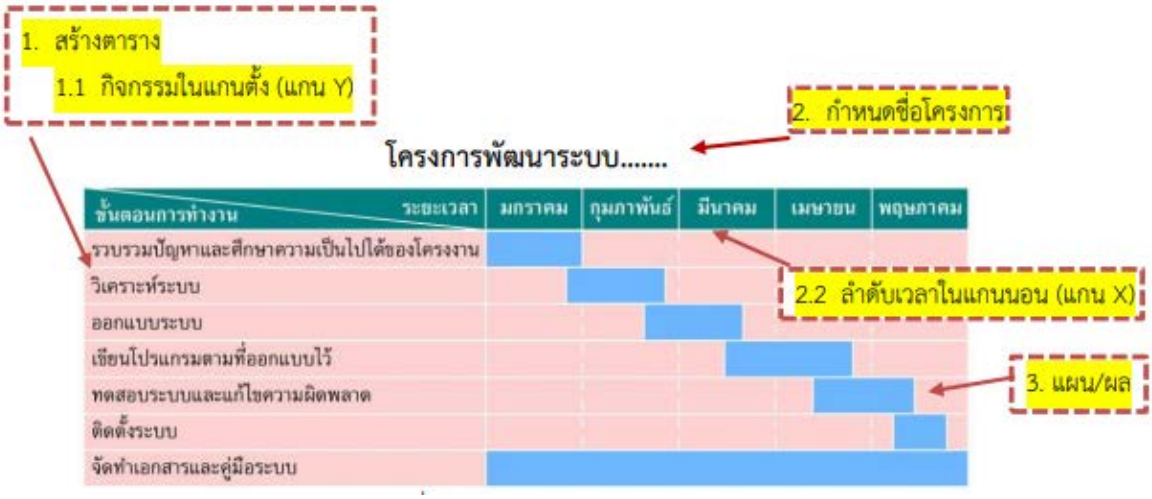
1. กำหนดผู้รับผิดชอบในการดำเนินงานตามแผนการทำงานการพัฒนาระบบสารสนเทศ

1.5 ควบคุมและกำกับดูแลโครงการ (Control and Direct Project)

สิ่งที่ต้องดำเนินการ

1. จัดทำ Gantt Chart เพื่อใช้กำหนดระยะเวลาในการพัฒนาระบบสารสนเทศในแต่ละขั้นตอน

ตัวอย่างแผนภูมิแกนต์ขั้นตอนการพัฒนาข้อมูลและระบบสารสนเทศ



รูปที่ 2 ตัวอย่างแผนภูมิแกนต์

ขั้นตอนการสร้างแผนภูมิแกนต์ (Gantt Chart)

1. กำหนดชื่อโครงการ
2. สร้างตาราง ประกอบด้วย

2.1 กิจกรรมหรืองานสำคัญที่ต้องทำเพื่อให้บรรลุเป้าหมายของโครงการ พัฒนาระบบสารสนเทศในแกนตั้ง (แกน y) โดยจัดทำเป็นขั้นตอนที่เรียงตามลำดับก่อนหลังกิจกรรมที่ทำก่อนอยู่ด้านบนไล่ลงมาตามลำดับถึงกิจกรรมสุดท้ายอย่างต่อเนื่อง

3. ลำดับเวลาในแกนนอน (แกน x)

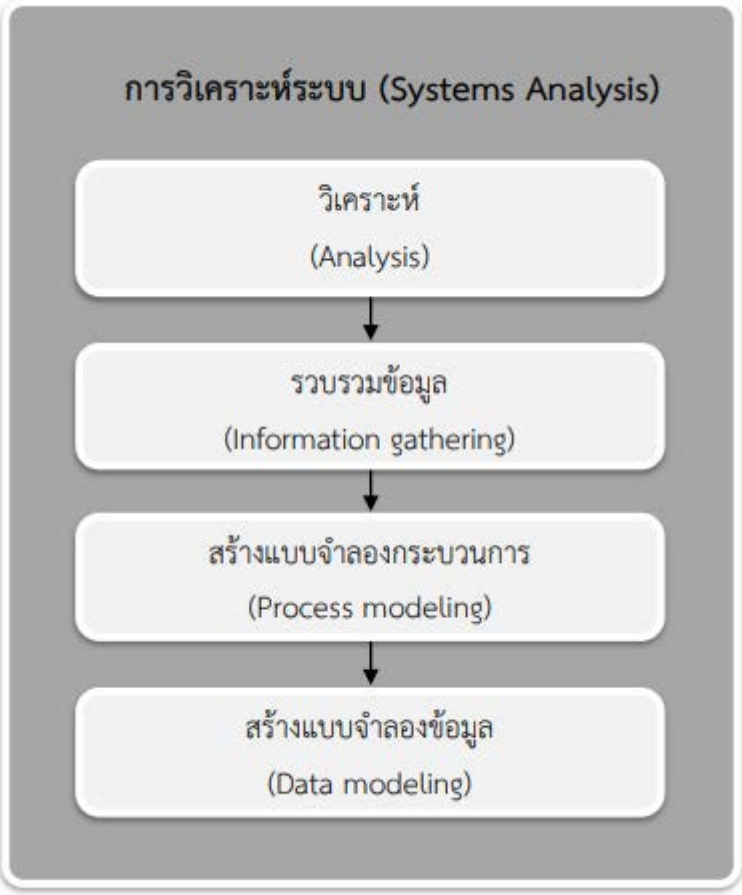
3.1 โดยกำหนดเวลาของระบบสารสนเทศในแต่ละโครงการการแสดงถึงเวลาในการทำกิจกรรมตลอดโครงการ หรืองาน เช่น เดือน สัปดาห์

4. สร้างแผน/ผลโดยตารางแผนมีเพื่อกำหนดระยะเวลาเริ่มต้น – สิ้นสุดของแต่ละกิจกรรมหรืองาน
5. กำหนดผู้รับผิดชอบหลักในแต่ละกิจกรรมกรณีมีผู้รับผิดชอบหลายคนร่วมทำระบบสารสนเทศหรือโครงการนั้น

2. การวิเคราะห์ระบบ (Systems Analysis)

การศึกษาและทำความเข้าใจระบบงานเดิมที่ใช้อยู่ซึ่งอาจเป็นระบบการทำงานด้วยมือหรือเป็นระบบสารสนเทศเดิมที่ใช้อยู่ก็ได้การวิเคราะห์ระบบงานเดิมจะทำให้นักวิเคราะห์หรือผู้พัฒนาระบบทราบถึงสภาพปัญหาที่เกิดขึ้นและใช้เป็นข้อมูลในการวิเคราะห์และออกแบบระบบงานใหม่ต่อไป

กระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ : กระบวนการย่อยการวิเคราะห์ระบบ (Systems Analysis)



รูปที่ 3 แสดงขั้นตอนการวิเคราะห์ระบบ (Systems Analysis)

สิ่งที่ต้องดำเนินการ

1. ผังงานในรูปแบบต่าง ๆ เช่น Activity Diagram , Sequence Diagram
2. แบบจำลองขั้นตอนการทำงานของระบบ (Process Model) : Data Flow Diagram
3. แบบจำลองข้อมูล (Data Model) : ER-Diagram
4. รายงานระบบสารสนเทศที่ได้จากระบบ
5. รายงานการวิเคราะห์และออกแบบระบบเบื้องต้น

ขั้นตอนการวิเคราะห์ระบบ

2.1 วิเคราะห์ (Analysis) โดยทำความเข้าใจระบบงานเดิม รวมถึงจุดอ่อน และจุดแข็งของระบบ

2.2 รวบรวมข้อมูล (Information gathering) รวบรวมความต้องการในระบบใหม่จากผู้ใช้ระบบทั้งความต้องการที่เป็นฟังก์ชันการทำงาน (Functional Requirement) และความ ต้องการที่ไม่ได้เป็นฟังก์ชัน (Non-Functional Requirement) โดยใช้วิธีการดังต่อไปนี้

2.2.1 การสัมภาษณ์ผู้ที่เกี่ยวข้องต่อการพัฒนาระบบ

2.2.2 การสังเกตและการปฏิบัติงาน

2.2.3 การตรวจทานจากเอกสาร โดยเฉพาะเอกสารที่เป็นแบบฟอร์มหรือรายงาน

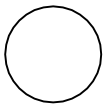
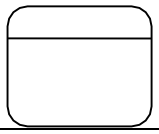
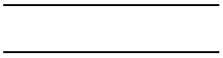
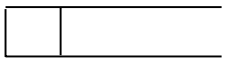
2.2.4 การสร้างแบบสอบถามเพื่อรวบรวมข้อมูลจากกลุ่มผู้ที่เกี่ยวข้อง

2.2.5 การวิเคราะห์จากประสบการณ์ของผู้พัฒนาระบบ ซึ่งเคยออกแบบและพัฒนาระบบลักษณะที่คล้ายคลึงกันมาก่อน

2.3 สร้างแบบจำลองกระบวนการ (Process modeling) เป็นแบบที่ใช้จำลองขั้นตอนการทำงานของระบบจากความต้องการที่รวบรวมได้

2.3.1 สร้างแบบจำลองเชิงตรรกะ (Logical Model) หรือแผนภาพกระแสข้อมูล (Data Flow Diagram) ซึ่งเป็นแผนภาพที่แสดงให้เห็นถึงทิศทางการไหลของข้อมูลที่มีอยู่ในระบบ และการดำเนินงานที่เกิดขึ้นในระบบแผนภาพกระแสข้อมูลจะแสดงภาพรวมของระบบ (Overall picture of a system)

สัญลักษณ์ของแผนภาพกระแสข้อมูล

สัญลักษณ์		คำอธิบาย
DeMarco & Yourdon	Gane & Sarson	
		Process: ขั้นตอนการทำงานภายในระบบ
		Data Store: แหล่งข้อมูลสามารถเป็นได้ทั้งไฟล์ข้อมูลและฐานข้อมูล (File or Database)

		External Agent: ปัจจัยหรือสภาพแวดล้อมที่มีผลกระทบต่อระบบ
		Data Flow: เส้นทางการไหลของข้อมูล แสดงทิศทางของข้อมูลจากขั้นตอนการทำงานหนึ่งไปยังอีกขั้นตอนการทำงานหนึ่ง

รูปที่ 4 สัญลักษณ์ของแผนภาพกระแสข้อมูล

ขั้นตอนของการเขียนแผนภาพกระแสข้อมูล

1. กำหนดรายการกิจกรรมต่าง ๆ ของระบบ และแยกออกมาวาอยู่ในรูปแบบใด (External Entities หรือ Data Flows หรือ Processes หรือ Data Stores)

2. สร้างแผนภาพระดับสูงสุด (Context Diagram) ซึ่งแสดงถึง External Entities และข้อมูลที่ไหลเข้าและออกจากระบบหลักโดยไม่สนใจแหล่งเก็บข้อมูล

3. เขียน Diagram ระดับถัดไป คือแผนภาพระดับล่าง (เรียกวา Diagram 0 หรือ Parent Diagram) ซึ่งแสดงถึง Process ต่าง ๆ ที่มีแต่เขียนให้ อยู่ในรูปแบบทั่วไป พร้อมกันนั้นให้แสดง Data Store ในระดับนี้ด้วย

4. สร้างแผนภาพระดับลูกของแต่ละ Process ใน Diagram 0 เรียกแผนภาพ ในระดับนี้ว่า แผนภาพกระแสข้อมูลระดับ 1 (Level-1 diagram) ถ้าหากมีรายละเอียดของการ ทำงานย่อยจากระดับนี้อีกก็ให้แตกรายละเอียดลงไปจนกระทั่งสิ้นสุด ส่วนชื่อของระดับก็จะเป็น Level-2 diagram, Level-3 diagram ไปเรื่อย ๆ จนกระทั่งหมด

5. ตรวจสอบหาข้อผิดพลาด และดูว่าคำกำกับบนเส้น Data Flow แต่ละเส้น รวมถึง Process แต่ละอันนั้นสื่อความหมายหรือไม่

6. หลังจากเขียนแผนภาพจนครบทุกการทำงานแล้ว ใหทำการตรวจสอบสมดุล ระหว่างข้อมูลเข้าและข้อมูลออกของแผนภาพ DFD กับ Context diagram

7. พัฒนารูปแบบใหม่ จาก Logical Data Flow Diagram ให้ ไปอยู่ ใน รูป Physical Data Flow Diagram เพื่อแยกระหวางระบบที่ทำด้วยมือกับระบบที่ทำงานอัตโนมัติ

8. แบ่งสวนของ Physical Data Flow Diagram โดยการแยกหรือแบ่งกลุ่มของ Diagram ออก เพื่อให้สามารถนำไปเขียนโปรแกรม หรือเพื่อการดำเนินการระบบได้

2.4 สร้างแบบจำลองข้อมูล (Data modeling) เป็นการจำลองข้อมูลที่เกิดขึ้นทั้งหมด ในระบบ พร้อมทั้งจำลองความสัมพันธ์ระหว่างข้อมูลที่เกิดขึ้น โดยใช้แผนภาพแสดงความสัมพันธ์ ระหว่างข้อมูล (Entity Relationship Diagram: ER-Diagram)

สัญลักษณ์ที่ใช้ในการเขียน ER-Diagram

สัญลักษณ์		คำอธิบาย
Chen Model	Crow's Foot Model	
		ใช้แสดง เอนทิตี้ (Entity)
		Relationship line เส้นเชื่อมความสัมพันธ์ระหว่างเอนทิตี้ (Entity)
	-	Entity Relationship แสดงความสัมพันธ์ระหว่างเอนทิตี้ (Entity) ** สำหรับ Crow' s Foot Model ใช้ตัวอักษรเขียนแสดงความสัมพันธ์
	Entity name Attribute 1 Attribute 2	Attribute ใช้แสดงแอททริบิวท์ (Attribute) ของเอนทิตี้ (Entity)

สัญลักษณ์		คำอธิบาย
Chen Model	Crow's Foot Model	
	Entity Name Identifier Attribute	ใช้แสดงคีย์หลัก (Identifier)
		Associative Entity
		Weak Entity

รูปที่ 5 สัญลักษณ์ที่ใช้ในการเขียน ER-Diagram

ขั้นตอนการสร้าง ER-Diagram

1. กำหนดเอนทิตี้ (Entity)

1.1 พิจารณาข้อมูลทั้งหมดที่จะจัดเก็บลงไปในฐานข้อมูล ว่าสามารถแบ่งออก ได้เป็นกี่เอนทิตี้ ภายในฐานข้อมูลหนึ่ง ๆ อาจจะมีจำนวนเอนทิตี้เป็นจำนวนมากซึ่งก็ขึ้นอยู่ที่ผู้ใช้ว่า ต้องการจัดเก็บข้อมูลมากเพียงใด

1.2 การกำหนดเอนทิตี้ จะต้องคำนึงถึง เอนทิตี้ทั้งแบบอ่อนแอและแบบปกติ

2. กำหนดแอททริบิวท์ (Attribute)

2.1 กำหนดคุณสมบัติแอททริบิวท์ให้กับเอนทิตี้ว่าควรจะประกอบไปด้วยแอททริบิวท์ใดบ้าง

2.2 พิจารณาด้วยว่าแอททริบิวท์ใดบ้างที่จะเป็น Composite Attributesหรือ Derived Attributes

2.3 กำหนดแอททริบิวท์ที่เป็นคีย์หลักให้กับแต่ละเอนทิตี้

3. กำหนดความสัมพันธ์ระหว่างเอนทิตี้ (Entity Relationship)

3.1 กำหนดเอนทิตี้ที่มีความสัมพันธ์กันว่าจะสัมพันธ์กันด้วยเงื่อนไขใดและ ชนิดความสัมพันธ์เป็นอย่างไร เช่น 1: 1,1: M และ M: N

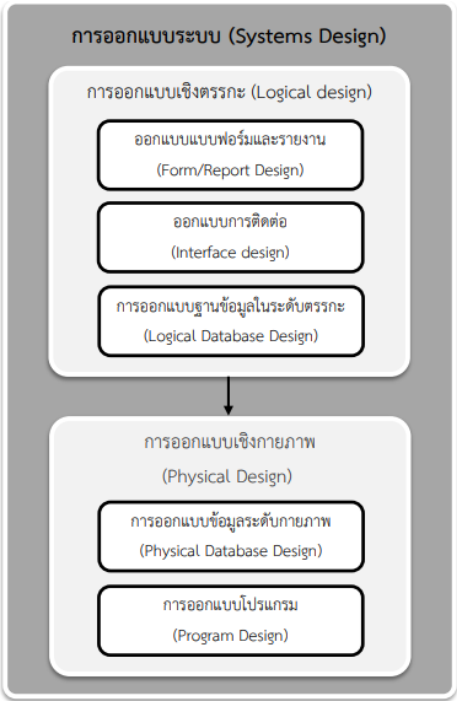
3.2 กำหนดแอททริบิวท์ที่มีคุณสมบัติเป็นคีย์นอกกับเอนทิตี้ที่สัมพันธ์กัน

4. จากนั้นนำเอาความสัมพันธ์ระหว่าง เอนทิตี้ ทั้งหมดมาเขียนรวมกันเป็น แผนภาพ ER-Diagramโดยสามารถเลือกใช้เครื่องมือในการจำลองแบบความต้องการชนิดต่าง ๆ ตามความ เหมาะสมของระบบสารสนเทศที่พัฒนา

3. การออกแบบระบบ (Systems Design)

เป็นการนำข้อมูลจากการวิเคราะห์ระบบที่เป็นแนวคิด (Concept) มาออกแบบให้เห็น รูปร่างของระบบสารสนเทศ โดยนักวิเคราะห์หรือผู้พัฒนาระบบจะออกแบบระบบทีละส่วน โดยเริ่ม จากส่วนที่เป็นผลลัพธ์ (Output) ก่อน เพราะผลลัพธ์นั้นเกิดจากการนำข้อมูลเข้าระบบแล้วไป ประมวลผล ดังนั้น การออกแบบผลลัพธ์หรือส่วนแสดงผลจะทำให้ทราบถึงการออกแบบในส่วนอื่น ๆ ที่เกี่ยวข้อง

กระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ : กระบวนการย่อยการออกแบบระบบ (Systems Design)



รูปที่ 6 แสดงขั้นตอนการออกแบบระบบ (Systems Design)

ขั้นตอนการออกแบบระบบ ประกอบด้วย

3.1 กำหนดข้อมูลเกี่ยวกับ Specification ของ Hardware และ Software

สิ่งที่ต้องดำเนินการ

3.1.1 Specification ของ Hardware และ Software

3.2 ออกแบบฟอร์มข้อมูลและรายงาน (Form/ Report Design) เป็นการกำหนดถึง ลักษณะของรูปแบบรายงานที่เกิดจากการทำงานของระบบ

สิ่งที่ต้องดำเนินการ

3.2.1 รายงานสรุปรายงานสารสนเทศ

3.2.2 รายงานการวิเคราะห์และออกแบบระบบ ลักษณะของรายงานหรือการแสดงผลที่ดี

3.2.3 การแสดงรายงานสารสนเทศต้องมีความชัดเจน ถูกต้อง

3.2.4 เข้าใช้งานง่าย และพร้อมนำข้อมูลในระบบสารสนเทศมาพิมพ์ออกรายงานได้ทันที เช่น มีหัวเรื่อง และรายละเอียดครบถ้วน

3.2.5 การแสดงผลได้อย่างรวดเร็วทันต่อการใช้งาน ไม่เสียเวลารอคอยนานเกินไปและ ควรแสดงผลให้ดูง่าย

3.2.6 การออกรายงานผลที่เหมาะสม และสอดคล้องตรงความต้องการของผู้ใช้

3.3 ออกแบบส่วนต่อประสานกับผู้ใช้ (Screen Design: User Interface) การออกแบบจอภาพ (Screen Design) คือ การปฏิสัมพันธ์ระหว่างผู้ใช้กับระบบ ซึ่งมีหลักการทำงาน พื้นฐาน 3 ส่วนได้แก่ ส่วนนำเข้าข้อมูล ส่วนประมวลผล และส่วนข้อมูลส่งออก

สิ่งที่ต้องดำเนินการ

3.3.1 รายงานการออกแบบหน้าจอ

3.3.2 จัดหาและเลือกเครื่องมือที่ใช้ในการออกแบบ: โปรแกรมสร้าง Mock Up เช่น Pencil, Adobe XD, Moqups

3.3.3 จัดทำต้นแบบสำหรับการออกแบบส่วนต่อประสานกับผู้ใช้

ขั้นตอนการออกแบบจอภาพ (Screen Design)

1. ทำความเข้าใจการทำงานของระบบสารสนเทศ ฯ
2. พัฒนาระบบเมนูและการนำทาง
3. เลือกเครื่องมือในการควบคุมการใช้งานที่เหมาะสม
4. เลือกเครื่องมือควบคุมการแสดงผลบนหน้าจอที่เหมาะสม
5. เตรียมเนื้อหาหรือข้อความที่ชัดเจน
6. สร้างส่วนตอบรับฟีดแบ็กและแนวทางทางการใช้งาน
7. สร้างกราฟิก ไอคอน และภาพที่สื่อความหมาย
8. เลือกใช้สีที่เหมาะสม
9. จัดการเลย์เอาท์หน้าต่าง และเพจ

3.4 ออกแบบฐานข้อมูล (Database Design) แบ่งออกเป็น 3 ระดับ คือ

3.4.1 การออกแบบข้อมูลในระดับแนวคิด (Conceptual Database Design) เป็นการออกแบบถึงข้อมูลที่ต้องการและความสัมพันธ์ระหว่างข้อมูลในฐานการออกแบบระดับนี้บางครั้งเรียกว่าการออกแบบระดับสูง (High-Level Database Design) การ ออกแบบข้อมูลในระดับนี้สามารถใช้แนวทางแบบ Data Driven ซึ่งสามารถแบ่งออกได้ 2 ลักษณะ ดังนี้

1) แบบล่างไปบน (Bottom-Up) วิธีการนี้เริ่มต้นการพิจารณาจาก รายละเอียดของข้อมูล หรือ แอททริบิวต์แล้วนำมาจัดกลุ่มเป็นเอนติตี้และความสัมพันธ์ (Relationship) วิธีการนี้เหมาะกับฐานข้อมูลที่มีรายละเอียดไม่มากและไม่ซ้ำซ้อน ซึ่งจะทำให้เป็น บรรทัดฐาน (Normalization) ช่วยออกแบบ

2) แบบบนมาล่าง (Top-Down) วิธีการนี้เริ่มจากกำหนดเอนติตี้ว่ามีเอนติตี้ อะไรบ้าง แล้วนำมาพิจารณารายละเอียดของแต่ละเอนติตี้ว่าควรจะมีแอททริบิวต์อะไร รวมถึง ความสัมพันธ์แต่ละเอนติตี้ วิธีการนี้เหมาะกับระบบสารสนเทศที่มีฐานข้อมูลที่ซับซ้อน และมี รายละเอียดมาก โดยใช้ E-R model ช่วยออกแบบ อย่างไรก็ตาม ควรใช้วิธีทั้ง 2 วิธีเสริมกันในการออกแบบทั้งวิธี Top-Down และ ทบทวนด้วย Bottom-Up จึงจะสมบูรณ์

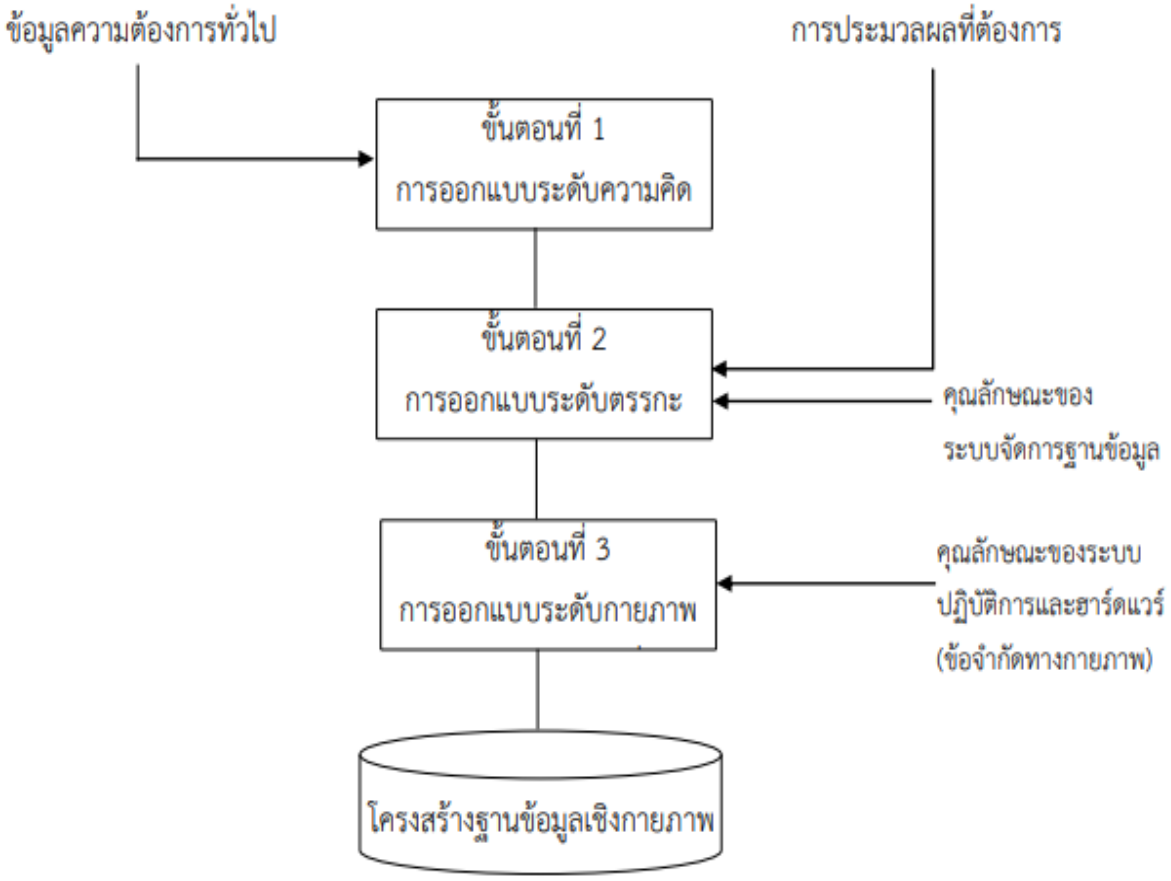
3.4.2 การออกแบบข้อมูลในระดับตรรกะ (Logical Database Design) เป็นการนำผลจากการออกแบบระดับแนวคิดมาวิเคราะห์และออกแบบ โดยในขั้นตอนนี้เป็นการแปลงผลจากการออกแบบระดับแนวคิด (Mapping) ให้อยู่ในรูปแบบของระบบ จัดการฐานข้อมูล (DBMS) ที่เลือกใช้ เช่นรูปแบบเชิงสัมพันธ์ (Relational Model) เป็นต้น ดังนั้นขั้นตอนนี้จะเป็นการแปลงเค้าร่างในระดับแนวคิดให้เป็นรีเลชั่นที่ ประกอบด้วยแอททริบิวต์ รวมถึงระบุข้อกำหนดต่าง ๆ (Constraint) ให้รีเลชั่น เช่น คีย์หลัก คีย์นอก โดเมนของแอททริบิวต์ และมีการใช้การทำให้เป็นบรรทัดฐาน (Normalization) เข้ามาช่วยเพื่อปรับ การออกแบบฐานข้อมูลที่เหมาะสม

3.4.3 การออกแบบข้อมูลระดับกายภาพ (Physical Database Design) ขั้นตอนนี้เป็นการนำเอาข้อมูลที่ออกแบบในระดับตรรกะมากำหนดโครงสร้างข้อมูล การจัดเก็บ วิธีการเข้าถึงข้อมูล รวมถึงการจัดการด้านระบบความปลอดภัย เพื่อให้ฐานข้อมูล ทำงานได้อย่างมีประสิทธิภาพ

สิ่งที่ต้องดำเนินการ

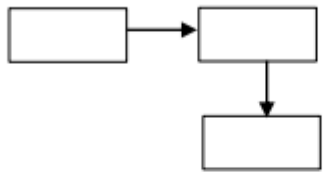
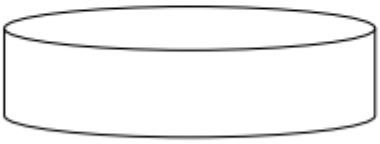
1. จัดทำรายงานการออกแบบฐานข้อมูล
2. Database Schema
3. Data Dictionary
4. เลือกเครื่องมือ : โปรแกรมสร้าง Database Schema

ขั้นตอนในการออกแบบฐานข้อมูล



รูปที่ 7 แสดงขั้นตอนการออกแบบฐานข้อมูล

ตารางแสดงการออกแบบ ฐานข้อมูลในแต่ละระดับ

การออกแบบ	เค้าร่าง(Schema)	ขั้นตอน
ระดับแนวคิด (CONCEPTUAL)	 ER-โมเดล	- กำหนดเอนทิตี้ แอททริบิวต์ คีย์หลัก คีย์นอก และความสัมพันธ์ระหว่าง เอนทิตี้ - วาดแผนภาพ (ERD) แปลง ERD ให้เป็นโครงสร้างตาราง - จัดทำพจนานุกรมข้อมูล (Data Dictionary)
ระดับตรรกะ (LOGICAL)	Table Definitions	- ภาษาที่ใช้สำหรับการนิยามข้อมูล DDL สำหรับรีเลชั่น แอททริบิวต์ และข้อกำหนดต่าง ๆ
ระดับกายภาพ (PHYSICAL)	 Database	- การกำหนดโครงสร้างของข้อมูล การจัดเก็บ (Storage) - วิธีการเข้าถึงข้อมูล (Access Method) การประมาณเนื้อที่ในการจัดเก็บข้อมูล - กำหนดระบบรักษาความปลอดภัยของฐานข้อมูล

รูปที่ 8 แสดงการออกแบบฐานข้อมูลในแต่ละระดับ

3.5 การออกแบบโปรแกรม (Program Design) ประกอบด้วยวิธีการดังนี้ คือ

3.5.1 ออกแบบโปรแกรมโดยใช้ อัลกอริธึม (Algorithm) เป็นการอธิบายถึงลำดับ ขั้นตอนการทำงานของการแก้ปัญหาโดยใช้ประโยคข้อความที่ชัดเจนไม่คลุมเครือ สามารถบอกลำดับ การทำงานได้

3.5.2 ออกแบบโปรแกรมโดยใช้ รหัสจำลอง (Pseudo Code) เป็นการออกแบบ ขั้นตอนการทำงานของโปรแกรมโดยการใช้ข้อความภาษาอังกฤษที่ใกล้เคียงกับภาษาคอมพิวเตอร์ ซึ่ง มีหลักการทำงานและประโยชน์เหมือนกับการใช้อัลกอริธึม

3.5.3 การออกแบบโปรแกรมโดยใช้ ผังงาน (Flowchart) คือ การใช้สัญลักษณ์ รูปภาพ หรือกล่องข้อความบรรยายรายละเอียดการทำงาน และใช้ลูกศรบอกทิศทางลำดับ ของการทำงาน

สัญลักษณ์ในการเขียนผังงาน FlowChart

สัญลักษณ์	คำอธิบาย
	จุดเริ่มต้นและสิ้นสุดของกระบวนการ
	กระบวนการที่มีกิจกรรมย่อยอยู่ภายใน
	กิจกรรมและการปฏิบัติงาน
	การตัดสินใจ
	ฐานข้อมูล
	เอกสาร/ รายงาน
	เอกสาร รายงานหลายแบบ ประเภท
	ทิศทาง/ การเคลื่อนไหวของงาน
	ทิศทางการนาเข้า/ ส่งออกของเอกสาร/ รายงาน
	จุดเชื่อมต่อระหว่างขั้นตอน/ กระบวนการ

รูปที่ 9 แสดงสัญลักษณ์ในการเขียนผังงาน Flow Chart

โดยผู้ออกแบบโปรแกรมสามารถเลือกใช้วิธีการออกแบบวิธีใดวิธีการหนึ่ง หรือ สามารถใช้หลายวิธีประกอบกันก็ได้ ตามความเหมาะสมของระบบสารสนเทศที่พัฒนาอยู่

สิ่งที่ต้องดำเนินการ

1. Prototype หรือ workflow ของระบบ

4. การพัฒนาระบบ (Systems Development)

เป็นขั้นตอนในการนำข้อมูลเฉพาะ ของการออกแบบมาทำการเขียนโปรแกรมเพื่อให้ เป็นไปตามคุณลักษณะและรูปแบบ ต่าง ๆ ที่ได้กำหนดไว้ หลังจากเขียนโปรแกรมเรียบร้อยแล้ว จะต้องทำการทดสอบโปรแกรม ตรวจสอบหาข้อผิดพลาดของโปรแกรมที่พัฒนาขึ้นมา

กระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ: กระบวนการย่อยการพัฒนาระบบ (Systems Development)

รูปที่ 10 แสดงขั้นตอนในการพัฒนาระบบ (Systems Development)

ขั้นตอนการพัฒนาระบบ ประกอบด้วย

4.1 การเขียนโปรแกรม (Coding) เป็นการนำข้อกำหนดที่ได้ในขั้นตอนการออกแบบมา แปลงเป็นชุดคำสั่ง มีขั้นตอนการเขียนโปรแกรม ดังนี้

4.1.1 เลือกภาษาที่ต้องการใช้ในการเขียนโปรแกรม ภาษาที่ใช้ในการเขียน โปรแกรม ขึ้นอยู่กับความถนัด ประเภทของงานและคุณสมบัติเฉพาะของเครื่องคอมพิวเตอร์

4.1.2 เขียนคำสั่งในการติดต่อฐานข้อมูล หรือ แฟ้มข้อมูล

4.1.3 เขียนเมนู เพื่อเป็นการควบคุมการทำงานและเป็นตัวบอกหน้าที่การทำงานในแต่ละส่วน

4.1.4 เขียนคำสั่ง (Function) การทำงานหลักของโปรแกรมพร้อมทั้งกำหนดวิธีการเก็บข้อมูลและเรียกใช้ตัวแปร

4.1.5 เขียนคำสั่งในการตรวจเช็กข้อผิดพลาดในการทำงานของโปรแกรม

4.1.6 สร้างรายงานและส่วนแสดงผลของคำสั่งที่ได้

4.1.7 Compile โปรแกรมที่เขียนขึ้นให้เป็นภาษาที่เครื่องคอมพิวเตอร์สามารถอ่านได้

สิ่งที่ต้องดำเนินการ

1. ระบบสารสนเทศที่จะพัฒนา

4.2 การทดสอบโปรแกรม (Testing) เป็นขั้นตอนของการทดสอบระบบก่อนที่จะนำไปใช้งานจริง โดยนำเอาระบบหรือโปรแกรมที่สร้างมาทดสอบกับข้อมูลเบื้องต้นเสียก่อน

4.2.1 ทดสอบการใช้งานระบบตามแต่ละกรณี (Test Case)

4.2.2 ทดสอบการใช้งานระบบตามแต่ละขั้นตอนการทำงาน (e-Test)

4.2.3 ทดสอบการใช้งานระบบตามปริมาณการใช้งานระบบ (e-Load)

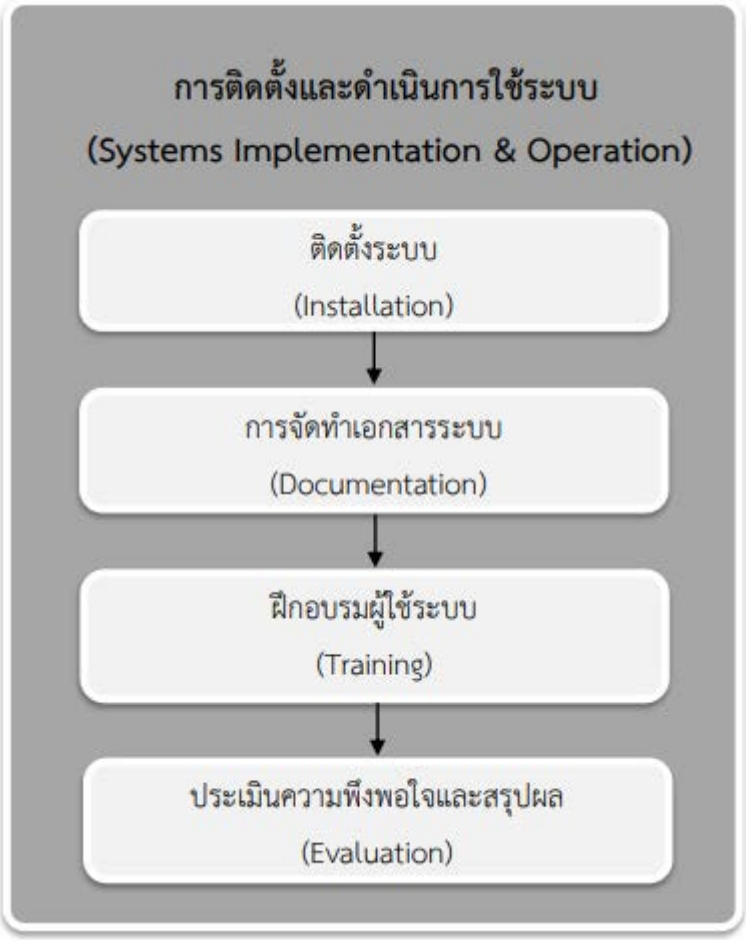
สิ่งที่ต้องดำเนินการ

1. รายงานการทดสอบระบบ

5.การติดตั้งและดำเนินการใช้ระบบ (Systems Implementation & Operation)

เมื่อดำเนินการสร้างระบบ และตรวจสอบแก้ไขเสร็จเรียบร้อยแล้ว ระบบงานจะถูกส่ง มอบและติดตั้งระบบ (Installed System) เพื่อใช้ในการปฏิบัติงาน โดยทำการติดตั้งตัวโปรแกรม ติดตั้งอุปกรณ์ พร้อมทั้งจัดทำคู่มือและจัดเตรียมหลักสูตรฝึกอบรมผู้ใช้งานที่เกี่ยวข้อง เพื่อให้ระบบ ใหม่สามารถใช้งานได้

กระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ: กระบวนการย่อยการติดตั้งและ ดำเนินการใช้ระบบ (Systems Implementation & Operation)



รูปที่ 11 แสดงขั้นตอนในการการติดตั้งและดำเนินการใช้ระบบ (Systems Implementation & Operation)

สิ่งที่ต้องดำเนินการ

1. จัดทำเอกสาร (Documentation)
2. ประเมินความพึงพอใจ
3. รายงานสรุปแบบประเมินความพึงพอใจ การติดตั้งและดำเนินการใช้ระบบมีขั้นตอนดังนี้

5.1 ติดตั้งระบบ (Installation) เป็นการติดตั้งโดยการแทนที่ระบบเก่า

5.1.1 แบบที่ 1 การนำระบบงานใหม่ไปแทนที่ระบบงานเก่าทันที

5.1.2 แบบที่ 2 การทำงานแบบเดิมควบคู่กับการใช้ระบบสารสนเทศใหม่ เป็นแบบ คู่ขนาน ซึ่งวิธีนี้จะค่อยเป็นค่อยไป ต่างจากแบบที่ 1

5.2 การจัดทำเอกสารคู่มือ (Documentation) และการแก้ไขข้อผิดพลาด การจัดทำเอกสารระบบ (Documentation) เอกสารมีความสำคัญต่อการปฏิบัติงาน และดูแลรักษาระบบ เช่น เอกสารคู่มือระบบและโปรแกรม คู่มือการปฏิบัติงาน หรือคู่มือผู้ใช้ เนื่องจากถ้าไม่มีคู่มือหรือเอกสาร เหล่านี้อธิบายแล้วหากการดำเนินงานมีปัญหาขัดข้องก็จะทำให้ ใช้เวลามากในการแก้ปัญหา การ จัดทำเอกสารจึงเป็นสิ่งจำเป็นและจะต้องทำไปพร้อมกับการพัฒนาระบบเอกสารที่ต้องจัดทำ ประกอบด้วย

5.2.1 เอกสารประกอบการใช้งานระบบ (User Documentation)

5.2.2 เอกสารประกอบสำหรับผู้เขียนโปรแกรมและพัฒนาระบบ (Technical Documentation)

5.3 ฝึกอบรมผู้ใช้ระบบ (Training) ซึ่งหลังจากติดตั้งและใช้งานระบบแล้ว มีข้อสังเกตว่าระบบงานใหม่ที่นำเข้ามาใช้แทนระบบงานเก่าผู้ใช้ย่อมไม่คุ้นเคย ดังนั้น จะต้องมีการจัดฝึกอบรม การใช้งานระบสารสนเทศให้กับผู้ใช้ และคอยช่วยเหลือ แนะนำ รวมถึงแก้ไขปัญหาที่เกิดจากการใช้ งานระบบสารสนเทศเป็นครั้งคราวจนกว่าผู้ใช้จะสามารถทำงานกับระบบใหม่ได้ เพื่อช่วยให้ผู้ใช สามารถใช้ระบบเป็นและใช้ได้อย่างมีประสิทธิภาพ

5.4 ประเมินความพึงพอใจและสรุปผล (Evaluation) ซึ่งในขั้นนี้ผู้พัฒนาระบบจะสรุปผลการดำ เนินการของการพัฒนาระบบต่อผู้บริหารของศูนย์ ฯ และติดตามประเมินผลการใช้ งานระบบโดยอาจกำหนดเป็นรอบระยะเวลาตามแผนการพัฒนาระบบ

5.4.1 ประเมินความพึงพอใจผู้ใช้งานระบบสารสนเทศ

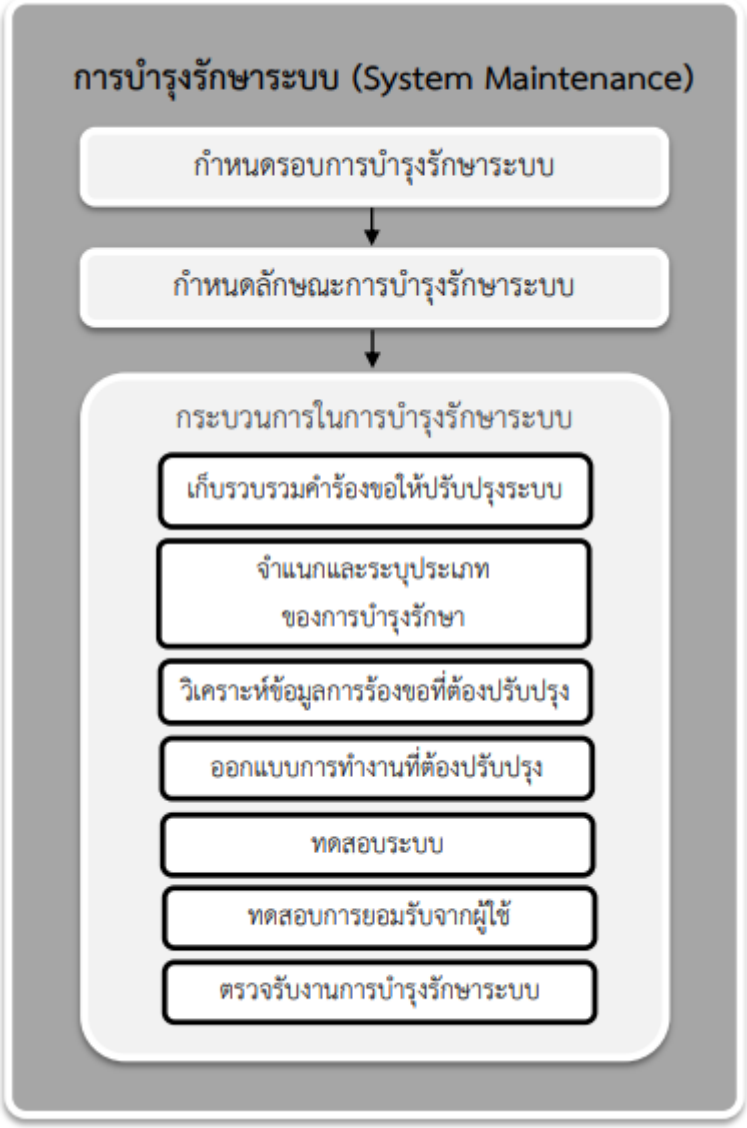
5.4.2 ประเมินความพึงพอใจการให้บริการของหน่วยพัฒนาระบบเทคโนโลยีสารสนเทศ

5.4.3 จัดทำรายงานสรุปผลการประเมินความพึงพอใจ

6. การบำรุงรักษาระบบ (System Maintenance)

การบำรุงรักษาระบบเป็นขั้นตอนสุดท้ายในการวิเคราะห์และออกแบบระบบ ซึ่งจะเกิดขึ้น หลังจากการติดตั้ง และใช้งานระบบแล้ว ทำให้ทราบถึงข้อผิดพลาดของโปรแกรม หรือความสามารถ ในการตอบสนองความต้องการของผู้ใช้ การพัฒนาระบบสารสนเทศเพื่อใช้งานจะประสบความสำเร็จ ได้นั้น จำเป็นจะต้องดูแลบำรุงรักษาระบบให้สามารถใช้งานได้อย่างเป็นปัจจุบัน โดยระบบต้อง สามารถทำงานได้ถูกต้อง และตรงความต้องการของผู้ใช้อีกด้วย

กระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ: กระบวนการย่อยการบำรุงรักษาระบบ (System Maintenance)



รูปที่ 12 แสดงขั้นตอนในการบำรุงรักษาระบบ (System Maintenance)

สิ่งที่ต้องดำเนินการ

- รายงานการบำรุงรักษาระบบ ขั้นตอนการบำรุงรักษาระบบประกอบด้วย

1. กำหนดรอบการบำรุงรักษาระบบ
2. กำหนดลักษณะการบำรุงรักษาระบบ
3. กระบวนการบำรุงรักษาระบบ

6.1 เก็บรวบรวมคำร้องขอให้ปรับปรุงระบบ ในกรณีที่ผู้ใช้งานระบบพบ ข้อผิดพลาดของระบบสารสนเทศ หรือมีความต้องการเปลี่ยนแปลงระบบ จะแจ้งปัญหาและความ ต้องการเหล่านั้นให้กับผู้ดูแลระบบทราบ ซึ่งผู้ดูแลระบบจะรับคำร้องทั้งหมดเพื่อนำมาวิเคราะห์และ ดำเนินการต่อไป ในการรับคำร้องเหล่านี้อาจ

ต้องมีการสัมภาษณ์ผู้ใช้งานที่เกี่ยวข้องให้ทราบถึง รายละเอียดกระบวนการทำงานหรือระเบียบของมหาวิทยาลัย เพื่อไม่ให้การแก้ไขปรับเปลี่ยน กระทบต่อการใช้งานในระบบงานอื่น ๆ

6.2 จำแนกและระบุประเภทของการบำรุงรักษาหลังจากรับคำร้องจากผู้ใช้งานแล้ว ผู้ดูแลระบบต้องจำแนกคำร้องเหล่านั้นว่าเป็นการบำรุงรักษาระบบประเภทใด และอยู่ในเงื่อนไข การบำรุงรักษาระบบหรือไม่ รวมถึงการพิจารณาอนุมัติหรือปฏิเสธ หากอนุมัติจะต้องประมาณขนาด ของการแก้ไขปรังปรุงระบบ จัดลำดับความสำคัญ และกำหนดระยะเวลาการดำเนินงาน

6.3 วิเคราะห์ข้อมูลการร้องขอที่ต้องปรับปรุง โดยดูผลกระทบที่เกิดจากการ ซ่อมบำรุง (Impact Analysis) การวิเคราะห์ปัจจัยด้านบุคคล (Human Factor) และต้นทุน- ผลประโยชน์ (Cost-benefit Effective) รวมถึงการวิเคราะห์รายละเอียดเนื้องาน ซึ่งต้องสอบถาม ข้อมูลที่ชัดเจนจากผู้ใช้ที่เกี่ยวข้อง

6.4 ออกแบบการทำงานที่ต้องปรับปรุง โดยนำรายละเอียดการปรับปรุงแก้ไข ระบบสารสนเทศที่ได้จากการวิเคราะห์ออกแบบโมดูลที่ต้องได้รับการเปลี่ยนแปลงแก้ไข โดยคำนึงถึง โมดูลอื่น ๆ ที่ได้รับ ผลกระทบด้วย

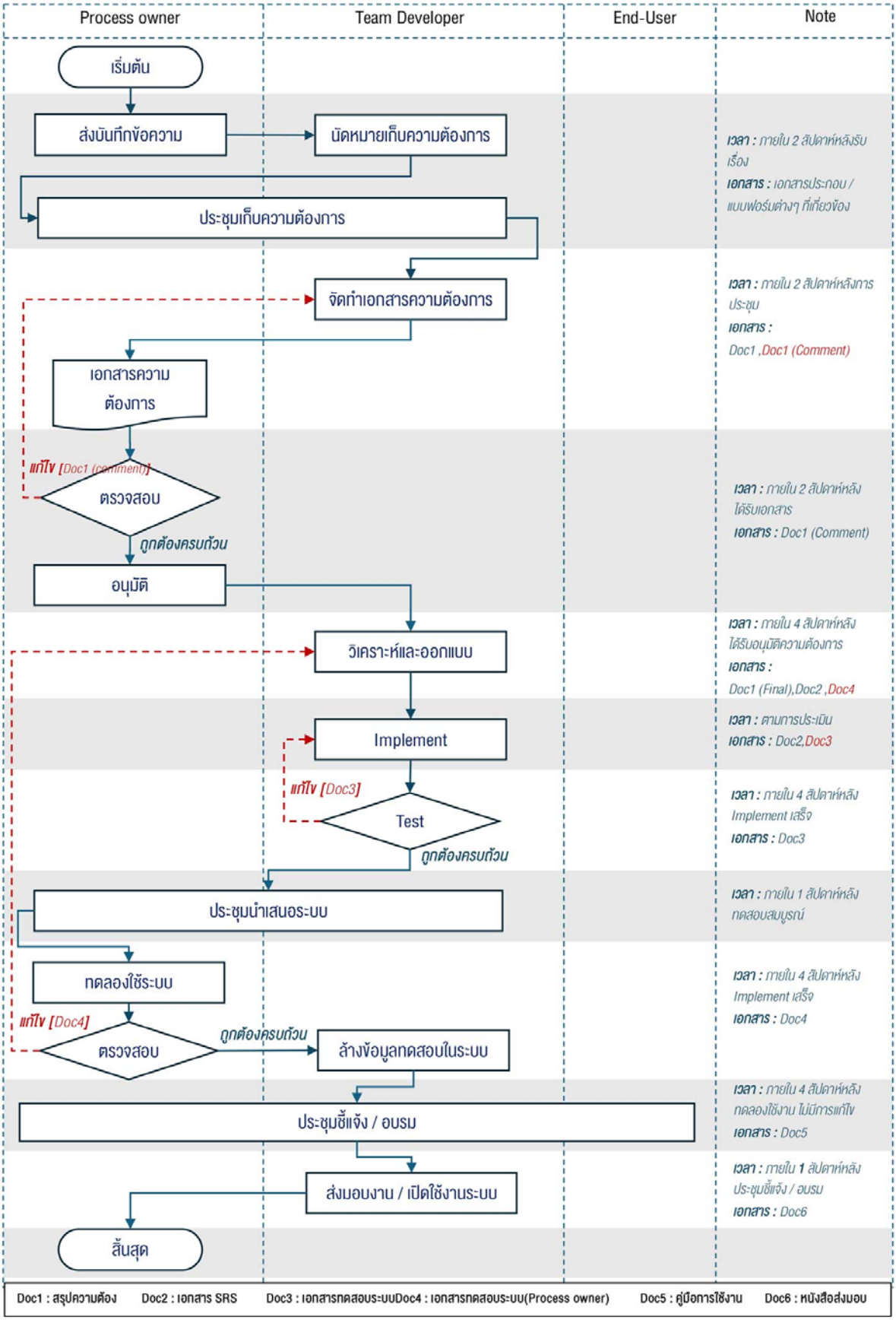
6.5 ดำเนินงานปรับปรุงระบบ ผู้ดูแลระบบทำการปรับปรุงแก้ไขระบบสารสนเทศ ตามที่ได้วิเคราะห์ออกแบบไว้ โดยในขั้นตอนการปรับปรุงโปรแกรมจะมีฐานข้อมูลสำรองที่ Server สำหรับการทดสอบข้อมูลระหว่างการพัฒนาปรังปรุงระบบสารสนเทศ

6.6 ทดสอบระบบ ทดสอบการปรับปรุงแก้ไขระบบสารสนเทศโดยผู้ดูแลระบบ เพื่อตรวจสอบความถูกต้องในการทำงานของโปรแกรม โดยพิจารณาไม่ให้มีข้อผิดพลาดด้านโปรแกรม และให้ระบบสารสนเทศสามารถทำงานถูกต้องตามคำร้องขอการปรับปรุงระบบสารสนเทศของผู้ใช้

6.7 ทดสอบการยอมรับจากผู้ใช้โดยบันทึกข้อมูลลงในระบบเพื่อทดสอบการ ทำงานของระบบสารสนเทศหลังจากการปรับปรุงแก้ไขแล้ว ซึ่งหากมีข้อผิดพลาด หรือไม่ตรงตาม ความต้องการของผู้ใช้ ผู้ดูแลระบบจะดำเนินการแก้ไขต่อไป

6.8 ตรวจรับงานการบำรุงรักษาระบบ เมื่อผู้ใช้ทดสอบระบบแล้ว ผู้ดูแลระบบ จะแจ้งผลการบำรุงรักษาระบบต่อผู้บริหารศูนย์เทคโนโลยีดิจิทัล และทำการสำรองไฟล์เก่า พร้อมทั้ง ปรับปรุงไฟล์ใหม่เพื่อให้ผู้ใช้สามารถใช้งานระบบสารสนเทศที่ทำการปรับปรุงให้เป็นปัจจุบัน และ ขั้นตอนต่อไปผู้ใช้ระบบทำการตรวจรับการบำรุงรักษาระบบ เป็นขั้นตอนสุดท้ายในกระบวนการ บำรุงรักษาระบบ

แผนภูมิการทำงานกระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ



รูปที่ 13 แสดงขั้นตอนการกระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ

แบบฟอร์มขอพัฒนาโปรแกรมคอมพิวเตอร์หรือแก้ไขโปรแกรมคอมพิวเตอร์

ส่วนที่ 1 หน่วยงาน

หน่วยงาน..... วันที่.....

ความต้องการ ☐ แก้ไข หรือเปลี่ยนแปลง ระบุชื่อโปรแกรม.....

☐ ต้องการมีโปรแกรมใหม่ ชื่อโปรแกรม.....

รายละเอียดที่ต้องการแก้ไขหรือเปลี่ยนแปลงหรือมีโปรแกรมใหม่

.....

เหตุผลที่ต้องแก้ไขหรือเปลี่ยนแปลง หรือมีโปรแกรมใหม่

.....

ลงชื่อ.....ผู้ขอ

(.....)

ส่วนที่ 2 งานเทคโนโลยีสารสนเทศ

☐ พิจารณาแล้วเห็นควรอนุมัติ เพราะ

.....

☐ พิจารณาแล้วไม่ควรอนุมัติ เนื่องจาก

.....

ลงชื่อ.....เจ้าหน้าที่

(.....)

ส่วนที่ 3 ผู้อนุมัติ

☐ เห็นควรอนุมัติ

.....

☐ ไม่เห็นควรอนุมัติ เนื่องจาก

.....

ลงชื่อ.....ผู้อนุมัติ

(.....)

ส่วนที่ 4 งานเทคโนโลยีสารสนเทศ

☐ ดำเนินการตามส่วนที่ 3 แล้ว

ลงชื่อ.....ผู้ตรวจสอบ

(.....)

แบบฟอร์มบันทึกข้อผิดพลาดระบบ

วันที่.....

ส่วนที่ 1 สำหรับผู้แจ้งข้อผู้ผิดพลาด

ชื่อระบบ.....

ข้อผิดพลาดที่พบ.....

.....

.....

ลักษณะการส่งไฟล์

☐ mail:piyarach.so@up.ac.th ☐ เอกสารแนบ ☐ อื่นๆ.....

ลงชื่อ.....ผู้ขอ

(.....)

ส่วนที่ 2 สำหรับผู้นำเดินการแก้ไข

☐ ผู้พัฒนาระบบ ☐ ผู้ดูแลระบบ

ขั้นตอนการดำเนินการแก้ไข

.....

.....

.....

.....

.....

ลงชื่อ.....ผู้ดำเนินการแก้ไข

(.....)

วันที่...../...../.....

Upili-it03.03

แบบฟอร์มบันทึกการโอนย้ายระบบ

วันที่.....

ส่วนที่ 1 สำหรับผู้แก้ไขโปรแกรม

ชื่อระบบ.....

รายละเอียดการแก้ไข.....

.....

.....

.....

ลงชื่อ.....ผู้แก้ไขโปรแกรม

(.....)

วันที่...../...../.....

ส่วนที่ 2 สำหรับผู้ทำการโอนย้าย

☐ โอนย้ายระบบสำเร็จ ☐ โอนย้ายระบบไม่สำเร็จ

รายละเอียด

.....

.....

.....

.....

.....

ลงชื่อ.....ผู้ดำเนินโอนย้าย

(.....)

วันที่...../...../.....

แบบฟอร์มบันทึกตรวจสอบการทำงานโปรแกรมอัตโนมัติ

ลำดับ	ระบบ	รายการ	สถานะ	วันที่	ผู้ตรวจสอบ	หมายเหตุ

แบบรายงานทบทวนปรับปรุงสิทธิ์การใช้งานระบบสารสนเทศ ปีงบประมาณ.....

งานเทคโนโลยีสารสนเทศ สถาบันนวัตกรรมการเรียนรู้

ระบบสารสนเทศ.....

ลำดับที่	รายชื่อผู้ใช้งานระบบ	สิทธิ์การใช้งาน			หมายเหตุ
		Admin	Editor	User	

ลงชื่อผู้ตรวจสอบ .....

(.....)

วันที่...../...../.....

ลงชื่อหัวหน้างาน .....

(.....)

วันที่...../...../.....

ทะเบียนการขออนุมัติใช้งานระบบ

ลำดับที่	รายชื่อโปรแกรม	สถานะ	วันที่ขออนุมัติ	เอกสารแนบ	หมายเหตุ

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน
(Backup and IT Continuity Plan)

วัตถุประสงค์

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

แนวปฏิบัติระบบสำรองของระบบสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน โดยมอบหมายให้ผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ ดังนี้

1. ผู้ดูแลระบบต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

1.1 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมด พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

1.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูลหากระบบใดที่มีการเปลี่ยนแปลงบ่อยควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูลดังนี้

1.2.1 กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

1.2.2 กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม(Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

1.2.3 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จเป็นต้น

1.2.4 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลการ Configuration ข้อมูลในฐานข้อมูล เป็นต้น

1.2.5 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถ แสดงถึงระบบซอฟต์แวร์วันที่/เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

1.2.6 จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิด ภัยพิบัติ เช่น ไฟไหม้ เป็นต้น

1.2.7 ทดสอบบันทึกข้อมูลที่สำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

1.2.8 จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

1.2.9 ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

1.2.10 กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

2. ให้จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุง แผนเตรียมความ

พร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งาน ตามภารกิจตามแนวทางต่อไปนี้

2.1 มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วย วิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

2.1.1 มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

2.1.2 มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว กรณีฉุกเฉินที่ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

2.1.3 มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

2.1.4 มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

2.1.5 มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

2.1.6 การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

2.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถ ปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

2.3 กำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณี ที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

2.4 ผู้ดูแลระบบต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

2.5 ผู้ดูแลระบบมีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ 1 ครั้ง

2.6 ผู้ดูแลระบบต้องกำหนดชนิดของข้อมูลและระยะเวลาที่ต้องการจะสำรองข้อมูลว่า ข้อมูลที่ต้องการสำรองเป็นข้อมูลชนิดใด และต้องใช้พื้นที่สำหรับการสำรองข้อมูลเท่าใด

2.7 ผู้ดูแลระบบจัดทำการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายที่มีความสำคัญโดยมีการสำรอง แบบเต็มรูปแบบ (Full Backup) อย่างน้อยเดือนละ 1 ครั้ง โดยกำหนดให้เป็นวันศุกร์แรกของเดือนหรือวันอื่นตามความเหมาะสม

2.8 ผู้ดูแลระบบต้องจัดทำการสำรองข้อมูลแบบบางส่วน (Incremental Backup) อย่างน้อยสัปดาห์ละ 1 ครั้ง

2.9 ผู้ดูแลระบบต้องจัดทำการทดสอบการกู้กลับคืนของข้อมูล (Restore) ทุก 6 เดือน

2.10 ผู้ดูแลระบบต้องจัดให้มีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

2.11 ข้อมูลที่สำรองและถูกจัดลำดับความสำคัญมากที่สุด ต้องมีการสำรองข้อมูลมากกว่า 1 ชุด และต้องทำการสำรองข้อมูลไปยังสถานที่อื่นเพื่อความปลอดภัย

การสำรองข้อมูล

1. รายละเอียดของข้อมูลที่จำเป็นของระบบสารสนเทศที่ต้องทำการสำรองข้อมูลประจำปี โดยทำการสำรวจและเก็บข้อมูลของระบบงานต่างๆ และแบ่งประเภทของข้อมูลที่ต้องจัดเก็บ ดังนี้

1.1. ข้อมูลระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่ายหลัก

1.2. ข้อมูลระบบสารสนเทศต่างๆ เช่น โปรแกรมระบบงานคอมพิวเตอร์ (application system) ชุดคำสั่งที่ใช้ทำงาน เป็นต้น

1.3. ข้อมูลระบบฐานข้อมูลของระบบสารสนเทศต่างๆ

ทั้งนี้ รวมถึงการกำหนดว่าจะสำรองข้อมูลทั้งเครื่องคอมพิวเตอร์แม่ข่ายหรือเฉพาะตำแหน่งที่ต้องการจัดเก็บข้อมูลเท่านั้นด้วย

2. ตารางการดำเนินงานในการสำรองข้อมูลโดยครอบคลุมข้อมูลประเภทต่างๆและความถี่ในการสำรอง ดังนี้

ลำดับ	ประเภทข้อมูล	ความถี่ในการสำรอง	ผู้รับผิดชอบหลัก	ผู้รับผิดชอบรอง
1.	ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่ายหลัก	ทุก 6 เดือน และทุกครั้งที่มีการปรับเปลี่ยนค่า (configuration)	ศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร	นายปิยะราช สุขภิญโญ
2.	ระบบสารสนเทศต่างๆ	ทุก 6 เดือน และทุกครั้งที่มีการปรับเปลี่ยนค่า configuration	นางสาวสุดา ใจแก้ว	นายปิยะราช สุขภิญโญ
3.	ระบบฐานข้อมูลของระบบสารสนเทศต่างๆ	ทุกวันหรือทุกสัปดาห์ (ความถี่ในการสำรองขึ้นอยู่กับระดับความสำคัญของข้อมูลและทุกครั้งที่มีการเปลี่ยนแปลงข้อมูล)	นางสาวสุดา ใจแก้ว	นายปิยะราช สุขภิญโญ
4.	เว็บไซต์	ทุกวัน	นางสาวสุดา ใจแก้ว	นายปิยะราช สุขภิญโญ
5.	ระบบคอมพิวเตอร์แม่ข่าย(Full System Backup)	ทุก 6-9 เดือน หรือทุกครั้งที่มีการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายหรือระบบปฏิบัติการใหม่	นายนาถพล สิริบรรสพ	นายปิยะราช สุขภิญโญ

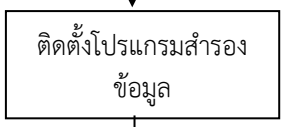
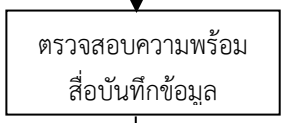
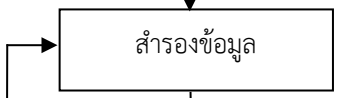
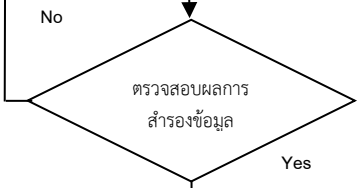
3. จัดทำรายละเอียดการสำรองข้อมูลสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ต้องประกอบด้วยรายการที่สำรองข้อมูล วิธีการสำรองข้อมูล และสื่อที่ใช้

4. ทำการตรวจสอบความถูกต้องทุกครั้งหลังจากการสำรองข้อมูล

5. ทำสำเนาชุดสำรองข้อมูลอย่างน้อยจำนวน 2 ชุด จัดเก็บไว้ในสถานที่ต่างกัน

6. ให้มีการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายเพื่อลดความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์ต่างๆ

กระบวนการการทำงาน (Work Flow) การสำรองและกู้คืนข้อมูลสารสนเทศ (Backup and Recovery)

ลำดับ	ผังกระบวนการ	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา	แบบฟอร์ม	เอกสารอ้างอิง
1		เครื่องคอมพิวเตอร์แม่ข่ายตามรายการสำรองข้อมูล ของกระบวนการในการสำรองข้อมูล	นักวิชาการคอมพิวเตอร์	10 นาที		
2		ติดตั้งโปรแกรมสำรองข้อมูลในเครื่องคอมพิวเตอร์	นักวิชาการคอมพิวเตอร์	60 นาที		
3		ตรวจสอบความพร้อมสื่อบันทึกข้อมูล	นักวิชาการคอมพิวเตอร์	10 นาที		
4		ดำเนินการ Backup ระบบข้อมูลด้วยโปรแกรมหรือ External	นักวิชาการคอมพิวเตอร์	10 นาที		
5		ตรวจสอบผลการสำรองข้อมูลสารสนเทศ	นักวิชาการคอมพิวเตอร์	10 นาที		
6		บันทึกผลการสำรองข้อมูลสารสนเทศ	นักวิชาการคอมพิวเตอร์	10 นาที		

การกู้คืนข้อมูล และการทดสอบกู้คืนข้อมูล

1. โดยปกติระบบจะสามารถให้บริการได้จะต้องมีส่วนประกอบที่ต้องอยู่ในสภาพที่พร้อมให้บริการได้ตลอดเวลา ประกอบด้วย ระบบเครือข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่ายอุปกรณ์จัดเก็บข้อมูลภายนอก หากระบบไม่สามารถให้บริการได้ จำเป็นต้องกู้ระบบกลับคืนโดยเร็วที่สุดหรือเท่าที่จะทำได้ โดยดำเนินการ ดังนี้

1.1. ซ่อมบำรุงครุภัณฑ์/อุปกรณ์ที่เกิดความเสียหายภายใน 48 ชั่วโมง

1.2. เปลี่ยนครุภัณฑ์/อุปกรณ์ที่เสียหาย

1.3. ขอยืมครุภัณฑ์/อุปกรณ์จากหน่วยงานอื่นชั่วคราว

1.4. จัดหาอุปกรณ์ใหม่

1.5. นำข้อมูลที่ได้สำรองไว้มาทำการ Restore เพื่อให้ระบบสามารถใช้งานได้ตามระยะเวลาที่กำหนด

1.6. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ความถูกต้องของข้อมูล และระบบอื่นๆ ที่เกี่ยวข้อง

2. กรณีที่มีความเสียหายต่อระบบปฏิบัติการ ระบบงานสารสนเทศ หรือระบบฐานข้อมูล จะต้องดำเนินการกู้คืนข้อมูลให้สามารถใช้งานได้ภายใน 24 ชั่วโมง โดยมีค่าข้อมูลสูญหายที่สามารถยอมรับได้ย้อนหลังไม่เกิน 48 ชั่วโมง

3. กำหนดรายละเอียดการจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และติดตั้งซอฟต์แวร์ใหม่เพื่อทดแทนเครื่องเดิมที่เสียหาย ในกรณีที่มีเครื่องคอมพิวเตอร์/อุปกรณ์เสียหาย ให้ทำการจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ใหม่มาทดแทนภายในระยะเวลา 15 วันทำการ โดยกำหนดให้มีคุณสมบัติของเครื่องให้เทียบเท่าหรือสูงกว่าเครื่องคอมพิวเตอร์/อุปกรณ์เดิมที่เสียหาย หลังจากนั้นให้ทำการติดตั้งซอฟต์แวร์ระบบสารสนเทศและระบบฐานข้อมูลให้เรียบร้อยภายในเวลา 3 วันทำการ

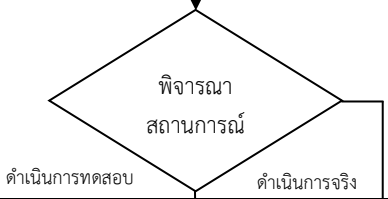
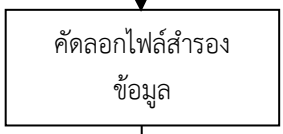
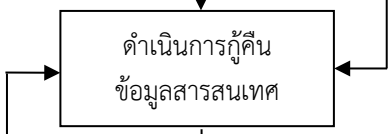
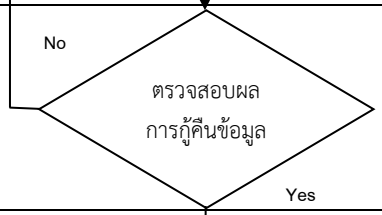
4. ทำการสุ่มทดสอบกู้คืนระบบบนเครื่องคอมพิวเตอร์แม่ข่ายในสถานการณ์ที่เครื่องคอมพิวเตอร์แม่ข่ายเกิดความเสียหาย

5. ในกรณีที่ระบบมีความเสียหายในระดับรุนแรงจำเป็นต้องมีการกู้คืน จะต้องแจ้งให้ผู้บังคับบัญชาและผู้มีส่วนเกี่ยวข้องทราบภายใน 1 วันทำการ

รายละเอียดระบบงานสารสนเทศและข้อมูลที่ทำการสำรอง

ลำดับ	ชื่อระบบ	IP Address	(ความถี่ในการสำรอง)	ผู้รับผิดชอบ
1.	Server ให้บริการเว็ปไซต์ศูนย์บรรณสารและการเรียนรู้	10.209.10.48	1 เดือน	นางสาวสุดา ใจแก้ว
2.	Server ฐานข้อมูล Oracle สำหรับโปรแกรม ALIST	10.208.10.240	1 สัปดาห์	นายปิยะราช สุขภิญโญ
3.	Server เว็ปและโปรแกรม ALIST	10.209.10.158	1 สัปดาห์	นายปิยะราช สุขภิญโญ
4.	Server กล้องวงจรปิด	10.220.27.xxx	1 เดือน	นางสาวสุดา ใจแก้ว
5.	Server เว็ปสถาบันนวัตกรรมการเรียนรู้	10.209.10.55	1 เดือน	นายนาถพล สิริบรรสพ
6.	Server Application สถาบันนวัตกรรมการเรียนรู้	10.209.10.107	1 เดือน	นายปิยะราช สุขภิญโญ
7.	Server โปรแกรม ฐานข้อมูลคลังปัญญา	10.209.10.67	1 สัปดาห์	นางสาวสุดา ใจแก้ว

กระบวนการการทำงาน (Work Flow) การกู้คืนข้อมูลสารสนเทศ (Recovery)

ลำดับ	ผังกระบวนการ	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา	แบบฟอร์ม	เอกสารอ้างอิง
1		กำหนดเครื่องคอมพิวเตอร์แม่ข่ายที่จะกู้คืนข้อมูล	นักวิชาการคอมพิวเตอร์	10 นาที		
2		พิจารณาสถานการณ์ของการกู้คืนข้อมูล	นักวิชาการคอมพิวเตอร์	60 นาที		
3		คัดลอกไฟล์สำรองข้อมูลสารสนเทศเพื่อทดสอบการกู้คืนข้อมูล	นักวิชาการคอมพิวเตอร์	10 นาที		
4		ดำเนินการกู้คืนข้อมูลสารสนเทศตามกระบวนการในการสำรองและกู้คืนข้อมูล	นักวิชาการคอมพิวเตอร์	10 นาที		
5		ตรวจสอบผลการกู้คืนข้อมูล	นักวิชาการคอมพิวเตอร์	10 นาที		
6		บันทึกผลการกู้คืนข้อมูล	นักวิชาการคอมพิวเตอร์	10 นาที		

แนวทางปฏิบัติเพื่อป้องกันภัยพิบัติฉุกเฉินด้านระบบสารสนเทศ

1. การบำรุงรักษาทั่วไป

1.1 มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้ โดยผู้ดูแลเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบรวมถึงมีการรับประกันความเสียหายจากผู้ขาย และมีการดูแลอย่างถูกต้องและต่อเนื่อง

1.2 ปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

1.3 ทำความสะอาดเครื่องคอมพิวเตอร์อยู่เสมอ และมีการตรวจสอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ

1.4 ใช้คำสั่งของระบบปฏิบัติการในการบำรุงรักษาเครื่องเป็นประจำ

1.5 การฝึกอบรมผู้ดูแลระบบและผู้ใช้งานให้มีความรู้ความเข้าใจในระบบงาน รวมทั้งการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ

1.6 การจัดเตรียมอุปกรณ์ที่จำเป็น ในการเตรียมความพร้อมรับภัยพิบัติฉุกเฉินที่จะเกิดขึ้นต่อระบบสารสนเทศ ดังนี้

1.6.1 แผ่น boot disk

1.6.2 แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/ระบบงานต่าง ๆ

1.6.3 แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

1.6.4 แผ่นโปรแกรมป้องกันมัลแวร์

1.6.5 แผ่น driver อุปกรณ์ต่าง ๆ

1.6.6 ระบบสำรองไฟฉุกเฉิน

1.6.7 อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

2. มาตรการรักษาความปลอดภัยระบบสารสนเทศ

2.1 กำหนดเจ้าหน้าที่รับผิดชอบในการดำเนินการไว้อย่างชัดเจน

2.2 ป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ โดยการติดตั้ง Firewall เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย ป้องกันการบุกรุกจากผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบเครือข่าย และกำหนดให้ Firewall มีการทำงานตลอดเวลา

2.3 กำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์และในกรณีที่พบว่ามีการใช้งานหรือมีการเปลี่ยนแปลงในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับ บัญชาทราบทันที

2.4 ทำการทดสอบโปรแกรมระบบรักษาความปลอดภัยและประสิทธิภาพการใช้งานสม่ำเสมอ

2.5 การจัดเก็บข้อมูลที่มีชั้นความลับ จะต้องมีมาตรการควบคุมการเข้าถึงข้อมูล เช่นการใส่รหัสผ่าน การเข้ารหัส เป็นต้น

3. มาตรการในการป้องกันมัลแวร์

3.1 ป้องกันมัลแวร์ โดยมีการติดตั้งซอฟแวร์ป้องกันมัลแวร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย ซึ่งผู้ใช้งานจำเป็นต้องระมัดระวังการใช้งานระบบคอมพิวเตอร์โดย เฉพาะการเชื่อมต่ออินเทอร์เน็ต เพื่อไมให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้โดยมีวิธีการ ดังนี้

3.1.1 ติดตั้งโปรแกรมป้องกันมัลแวร์ที่เหมาะสมและอัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ

3.1.2 เปิดใช้งาน Auto Protect

3.1.3 ตรวจสอบหามัลแวร์ทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูลต่างๆ

3.1.4 ใช้โปรแกรมเพื่อทำการตรวจหามัลแวร์อย่างน้อยสัปดาห์ละ 1 ครั้ง

3.2 การป้องกันภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ

3.2.1 ระวังภัยจากการเปิดไฟล์สื่อบันทึกข้อมูลต่าง ๆ เช่น External HarddiskUSB Flash Drive ควรมีการสแกนหามัลแวร์ก่อนเปิดใช้งานทุกครั้ง

3.2.2 ใช้ความระมัดระวังในการเปิด e-mail เช่น อย่าเปิดไฟล์ที่ไม่ทราบแหล่งที่มา หรือถ้าไม่ทราบแหล่งที่มาควรลบทิ้งทันที

3.2.3 หลีกเลี่ยงการแชร์ไฟโดยไม่จำเป็น หากมีการแชร์ไฟล์จะต้องมีมาตรการควบคุมการเข้าถึงข้อมูล เช่น การใส่รหัสผ่าน การเข้ารหัส เป็นต้น

3.2.4 ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จาก Internet เช่น ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่น่าเชื่อถือ

3.2.5 ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น *,pif เป็นต้น

3.2.6 หลีกเลี่ยงการใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

4. มาตรการป้องกันปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

4.1 ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ซึ่งมีระยะเวลาการสำรองไฟได้ประมาณ 15 – 30 นาที

4.2 เปิดเครื่องสำรองไฟตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟให้อยู่ในสภาพพร้อมใช้งานได้ตลอดเวลา

4.3 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

5. กระบวนการแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบสารสนเทศ

5.1 กรณีเครื่องคอมพิวเตอร์แม่ข่ายถูกมัลแวร์โจมตี

5.1.1 การสรุปเหตุเบื้องต้น โดยเครื่องคอมพิวเตอร์จะมีการทำงานที่ผิดปกติไป

- เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ เช่น ไม่สามารถ log in เข้าระบบได้
- ไฟล์งานในเครื่องคอมพิวเตอร์หายไป โดยการสังเกตจากข้อความที่แจ้งเตือน
- โปรแกรมไม่สามารถทำงานได้ (Run ไม่ขึ้น)
- มี System Message ที่แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้

5.2.1 แนวทางการปฏิบัติ กรณีต้องติดตั้งระบบใหม่ มีขั้นตอนการติดตั้งระบบ ดังนี้

- ดำเนินการจดบันทึก / สรุป และทำการ Pint Screen ข้อความที่ผิดปกติ
- แจ้งผู้รับผิดชอบ หรือเจ้าหน้ารักษาความปลอดภัยระบบสารสนเทศ
- ติดตั้งโปรแกรมระบบปฏิบัติการใหม่
- ตั้งค่าระบบการให้บริการของเครื่องคอมพิวเตอร์แม่ข่าย
- ดึงข้อมูลจากระบบสำรองข้อมูลเข้ามาในระบบฐานข้อมูลเดิม

5.2 กรณีถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคล (Hacker) โดยไม่ได้รับอนุญาต

5.2.1 การสรุปเหตุเบื้องต้น

- เกิดความผิดปกติทางกายภาพ เช่น ดิสก์สูญหาย หรือเสียหาย
- เกิดจากการทำงานของระบบ เช่น ไม่สามารถเข้าถึงข้อมูลได้
- มี System Message ที่แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้

5.2.2 แนวทางการปฏิบัติ

- ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา

- ตัดการเชื่อมต่อของเครื่องคอมพิวเตอร์แม่ข่ายหรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย
- เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก
- วิเคราะห์การถูกโจมตี โดย ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) และไฟล์อื่น ๆ
- วิเคราะห์ Log fle ตรวจสอบโปรแกรมหรือ ข้อมูลที่ผู้บุกรุกทิ้งไว้
- ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System
- ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ
- กู้คืนระบบคอมพิวเตอร์ ระบบฐานข้อมูลหรือระบบสารสนเทศที่เสียหายหรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่
- งดใช้เซอร์วิส (service) ที่ไม่จำเป็น
- ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)
- อุดช่องโหวในระบบเครือข่าย
- เปลี่ยนแปลงพาสเวิร์ดใหม่ หลังจากได้แก้ไขช่องโหว่ของระบบ

5.3 กรณี ระบบฐานข้อมูลเสียหาย ข้อมูลสูญหาย ถูกทำลายหรือถูกแก้ไขโดยไม่ได้รับอนุญาต

5.3.1 การสรุปเหตุเบื้องต้น

- เกิดความผิดปกติทางกายภาพ เช่น ดิสก์สูญหาย หรือเสียหาย
- เกิดจากการทำงานของระบบ เช่น ไม่สามารถเข้าถึงข้อมูลได้
- มี System Message ที่แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้

5.3.2 แนวทางการปฏิบัติ

- ดำเนินการจดบันทึก / สรุป และทำการ Pint Screen ข้อความที่ผิดปกติ
- แจ้งผู้รับผิดชอบ หรือเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ
- นำข้อมูลสำรอง (Back Up) ในช่วงที่ต้องการมากู้คืนข้อมูล
- ทำการตรวจสอบความถูกต้องของข้อมูล ว่าข้อมูลมีความสมบูรณ์ ครบถ้วนมีความน่าเชื่อถือ

5.4 กรณีระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

5.4.1 การสรุปเหตุเบื้องต้น

- ไฟฟ้าขัดข้อง (ไฟตก)
- ไฟฟ้าดับ

5.4.2 แนวทางการปฏิบัติ

- ตรวจสอบว่าไฟฟ้าขัดข้อง/ไฟฟ้าดับ เกิน 15 นาทีหรือไม่
- ปิดอุปกรณ์เครือข่าย
- ปิดเครื่องคอมพิวเตอร์แม่ข่ายและระบบสารสนเทศ
- เมื่อไฟฟ้าเข้าสู่สภาวะปกติ ให้เปิดเครื่องคอมพิวเตอร์แม่ข่ายและระบบสารสนเทศ
- เปิดอุปกรณ์เครือข่าย

- ตรวจสอบความเสียหายระบบสารสนเทศ

5.5 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

5.5.1 การสรุปเหตุเบื้องต้น

- เครื่องคอมพิวเตอร์ เรียกดูข้อมูลจากระบบ Intranet ไม่ได้

5.5.2 แนวทางการปฏิบัติ

- แจ้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ
- ตรวจสอบระบบเครือข่ายภายใน (LAN) และระบบเชื่อมโยง
- แก้ไขโดยใช้อุปกรณ์ Hardware สับเปลี่ยน กรณ์อุปกรณ์เครือข่ายชำรุดหากเกินขีดความสามารถของหน่วยให้แจ้ง ดำเนินการต่อไป
- หลังการตรวจสอบแก้ไขเสร็จเรียบร้อยแล้ว ให้ทำการทดลองระบบและตรวจ สอบผลการใช้งาน
- บันทึกผลการตรวจสอบแก้ไข

6. ปัญหาและอุปสรรคในการดำเนินการ

6.1 มีข้อจำกัดด้านทรัพยากรเทคโนโลยีสารสนเทศในการดำเนินงาน

6.2 การจัดทำฐานข้อมูลยังไม่มีความครบถ้วน ตามความเหมาะสม ภารกิจที่ต้องดำเนินการมีปริมาณมากกว่าจำนวนบุคลากรผู้รับผิดชอบ

6.3 ระบบที่ดำเนินการพัฒนาในปีปัจจุบันอาจต้องมีการปรับปรุงเพื่อให้เป็นไปตามความต้องการใช้งานต่อยอดในการบริหารจัดการด้านระบบสารสนเทศ

แผนรองรับสถานการณ์ฉุกเฉิน สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

1. กรณีเครื่องติดไวรัสคอมพิวเตอร์

1.1. กรณีถูกไวรัสหรือผู้บุกรุก ให้ผู้ใช้งานสแกนไวรัส ตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย เช่น การถอดสายแลนออกหรือการตัดการเชื่อมต่อแบบไร้สาย (Wi-Fi) เพื่อจำกัดความเสียหายที่ไวรัสคอมพิวเตอร์อาจแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่นๆ ในระบบเครือข่าย

1.2. ในกรณีแก้ไขเองไม่ได้ ให้สำรองข้อมูลที่จำเป็น และแจ้งเจ้าหน้าที่งานเทคโนโลยีสารสนเทศ เพื่อดำเนินการแก้ไข

1.3. กำจัดไวรัสเครื่องคอมพิวเตอร์ดำเนินการแก้ไข กู้คืนข้อมูลหรือระบบที่เสียหาย

1.4. ติดตั้งระบบปฏิบัติการใหม่

1.5. วิเคราะห์สาเหตุและผลกระทบที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ในระบบเครือข่าย

1.6. ดำเนินการป้องกันเพื่อหยุดยั้งการแพร่กระจายของไวรัสคอมพิวเตอร์

กระบวนการการทำงาน (Work Flow) การปฏิบัติการณ์กรณีเครื่องติดไวรัสคอมพิวเตอร์

ลำดับ	ผังกระบวนการ	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา	แบบฟอร์ม	เอกสารอ้างอิง
1	เครื่องคอมพิวเตอร์ติดไวรัส	เครื่องคอมพิวเตอร์ติดไวรัส	นักวิชาการคอมพิวเตอร์	10 นาที		
2	สแกนไวรัส	สแกนไวรัส ตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย	นักวิชาการคอมพิวเตอร์	60 นาที		
3	กำจัดไวรัสเครื่องคอมพิวเตอร์ (กำจัดได้ / กำจัดไม่ได้)	กำจัดไวรัสเครื่องคอมพิวเตอร์ ดำเนินการแก้ไข	นักวิชาการคอมพิวเตอร์	60 นาที		
4	ดำเนินการกู้คืนข้อมูลสารสนเทศ	สำรองข้อมูล กู้คืนข้อมูลหรือระบบที่เสียหาย	นักวิชาการคอมพิวเตอร์	60 นาที		
5	ติดตั้งระบบปฏิบัติการใหม่	ติดตั้งระบบปฏิบัติการใหม่	นักวิชาการคอมพิวเตอร์	60 นาที		
6	บันทึกผล	บันทึกผล	นักวิชาการคอมพิวเตอร์	10 นาที		

2. กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม

2.1 กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องตัดสัญญาณเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกบุกรุก

2.2 และวิเคราะห์หาสาเหตุของการเข้ามาในระบบ โดยการตรวจสอบจาก log file และประเมินความเสียหายที่เกิดขึ้น

2.3 ผู้ดูแลระบบดำเนินการแก้ไข

2.4 แจ้งผู้ใช้งานรับทราบปัญหาระบบขัดข้อง

2.5 ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

2.6 ในกรณีที่ไม่สามารถกู้คืนระบบได้ ต้องติดตั้งระบบใหม่ และนำข้อมูลที่สำรองไว้ นำกลับมาใช้

กระบวนการการทำงาน (Work Flow) การปฏิบัติการณ์ กรณีโดนเจาะระบบหรือตรวจพบภัยคุกคาม

ลำดับ	ผังกระบวนการ	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา	แบบฟอร์ม	เอกสารอ้างอิง
1	ตรวจพบภัยคุกคาม	ตรวจพบภัยคุกคาม	นักวิชาการคอมพิวเตอร์	10 นาที		
2	ตัดสัญญาณเครื่องออกจากระบบเครือข่าย	ตัดสัญญาณเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกบุกรุก	นักวิชาการคอมพิวเตอร์	60 นาที		
3	ตรวจสอบ วิเคราะห์ ประเมินความเสียหาย	วิเคราะห์หาสาเหตุของการเข้ามาในระบบ โดยการตรวจสอบจาก log file และประเมินความเสียหาย	นักวิชาการคอมพิวเตอร์	60 นาที		
4	แก้ไขได้ การแก้ไขความเสียหาย แก้ไขไม่ได้	ผู้ดูแลระบบดำเนินการแก้ไข	นักวิชาการคอมพิวเตอร์	60 นาที		
5	แจ้งผู้ใช้งานรับทราบปัญหา	แจ้งผู้ใช้งานรับทราบปัญหาระบบขัดข้อง	นักวิชาการคอมพิวเตอร์	60 นาที		
6	หาวิธีปิดช่องโหว่	ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆ				
	ติดตั้งระบบปฏิบัติการใหม่	ติดตั้งระบบใหม่ และนำข้อมูลที่สำรองไว้นำกลับมาใช้				
	บันทึกผล	บันทึกผล	นักวิชาการคอมพิวเตอร์	10 นาที		

แบบฟอร์มบันทึกผลการสำรองข้อมูล

วัน/เดือน/ปี	รายละเอียดของ File ที่ Backup					รูปแบบสื่อที่จัดเก็บ**/แหล่งจัดเก็บ	การตรวจสอบ File หลัง Backup	
	ชื่อเครื่อง/IP Address	Drive	ชื่อ Folder	File			ผลการตรวจสอบ***	ผู้ตรวจสอบ
				ชื่อ File	ประเภท File*			

*** ประเภท File** หมายถึง Word, Excel, pdf., Video, image หรืออื่นๆ

****รูปแบบสื่อที่จัดเก็บ** หมายถึง Thumb Drive, External Hard disk หรือ สื่อประเภทอื่น ๆ

***** ผลการตรวจสอบ** ให้ระบุผลการตรวจสอบสภาพของ File ว่า สมบูรณ์หรือไม่ และสามารถนำกลับมาใช้ใหม่ได้หรือไม่

แบบฟอร์มบันทึกการเก็บข้อมูลสำรอง แบบฝาก External Hard disk

ลำดับ	วันที่ส่ง	รายการ	จำนวน	สถานที่จัดเก็บ	ผู้ส่งมอบ	ผู้รับมอบ	หมายเหตุ

การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

วัตถุประสงค์

การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk และ availability risk

แนวทางปฏิบัติ

1. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

1.1. ต้องมีขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (computer operator) เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

1.2. ควรกำหนดให้เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ปฏิบัติงานโดยผ่านเมนู และควรจำกัดการปฏิบัติงานโดยใช้ command line เท่าที่จำเป็น

1.3. ควรกำหนดให้มีการบันทึก (log book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้

1.3.1. ผู้ปฏิบัติงาน

1.3.2. เวลาปฏิบัติงาน

1.3.3. รายละเอียดการปฏิบัติงาน

1.3.4. ปัญหาที่เกิดขึ้นและการแก้ไข

1.3.5. สถานะของระบบ

1.3.6. ผู้ตรวจทานการปฏิบัติงาน

2. การติดตามการทำงานของระบบคอมพิวเตอร์ (monitoring)

2.1. ต้องติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เช่น ระบบห้องสมุดอัติโนมัติ ALIST ระบบ RFID

2.2. ควรบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่างๆ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ

3. การจัดการปัญหาต่างๆ

3.1. ต้องกำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน เช่น กำหนดผู้รับผิดชอบในการแก้ไขปัญหาระบบ รวมถึงเบอร์โทรศัพท์ของผู้ที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่มีปัญหา

3.2. ควรมีระบบจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้น และรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหาและตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป

4. การควบคุมการจัดทำรายงาน

4.1. การขอให้จัดพิมพ์รายงานต่างๆ ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่

4.2. ควรมีทะเบียนคุมการพิมพ์และการจัดส่งรายงาน จัดเก็บรายงานต่าง ๆ ที่ได้จัดพิมพ์แล้วอย่างรัดกุม และกำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

ขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ

ขั้นตอนการเปิดใช้งานระบบห้องสมุดอัตโนมัติ ALIST

หน้าที่ความรับผิดชอบ

ดูแลรับผิดชอบฐานข้อมูลและควบคุมทำให้เจ้าหน้าที่ให้บริการแก่ผู้ใช้บริการได้อย่างมีประสิทธิภาพ จัดการระบบห้องสมุดอัตโนมัติในเรื่องของการตั้งค่าของ module (โมดูล) (System Administrator Module) ใช้ในการทำงานและกำหนดสิทธิของระดับผู้ใช้งานแต่ละส่วน ให้คำปรึกษาและช่วยแก้ไขปัญหาให้กับเจ้าหน้าที่สำหรับการใช้งานระบบ

ระเบียบปฏิบัติ/ขั้นตอน

- ติดตั้งโปรแกรมห้องสมุดอัตโนมัติ ALIST แก่เจ้าหน้าที่ที่เกี่ยวข้องในศูนย์บรรณสารฯ
- การกำหนดนโยบายและสิทธิ์การใช้งานก่อนเริ่มใช้งานระบบ
- เจ้าหน้าที่ใช้งานตามสิทธิ์ที่ได้รับ
- ติดต่อประสานงานกับศูนย์คอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ เรื่องระบบมีปัญหา

กระบวนการการทำงาน (Work Flow) การเปิดใช้งานระบบห้องสมุดอัตโนมัติ ALIST

ลำดับ	ผังกระบวนการ	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา	แบบฟอร์ม	เอกสารอ้างอิง
1	ติดตั้งโปรแกรมห้องสมุดอัตโนมัติ ALIST	งานเทคโนโลยีได้รับมอบหมายให้ติดตั้งโปรแกรมห้อง สมุดอัตโนมัติ ALIST	นักวิชาการคอมพิวเตอร์	30 นาที		
2	ตั้งค่าระบบเริ่มต้นเพื่อเริ่มใช้งาน	ตั้งค่าระบบเริ่มต้นกำหนดนโยบายและสิทธิ์การใช้งานก่อนเริ่มใช้งานระบบ	นักวิชาการคอมพิวเตอร์	50 นาที		
3	ตั้งค่ารายชื่อผู้ใช้งาน	ตั้งค่ารายชื่อเจ้าหน้าที่ใช้งานตามสิทธิ์ที่ได้รับ	นักวิชาการคอมพิวเตอร์	20 นาที		
4	สอนการใช้งานระบบเบื้องต้น	สอนการใช้งานระบบเบื้องต้น	นักวิชาการคอมพิวเตอร์	60 นาที		
5	บันทึกผล	บันทึกผลการสำรองข้อมูลสารสนเทศ	นักวิชาการคอมพิวเตอร์	10 นาที		

ขั้นตอนการเปิดใช้งานระบบประตู RFID

หน้าที่ความรับผิดชอบ

ดูแลรับผิดชอบฐานข้อมูลและควบคุม จัดการเรื่องของการตั้งค่าของประตู RFID เพื่อให้พร้อมใช้งาน เพื่อป้องกันการสูญหายของทรัพยากรภายศูนย์รบรรณสารและการเรียนรู้

ระเบียบปฏิบัติ/ขั้นตอน

- ประสานงานบริษัทเรื่องการติดตั้งระบบ RFID
- ตรวจเช็คคอมพิวเตอร์ตรงประตูเข้า-ออก
- เปิดโปรแกรม RFID ให้พร้อมใช้งาน
- เช็คตู้คืนหนังสืออัตโนมัติว่าเปิดใช้งานไหม
- ปิดระบบเมื่อไม่ได้ใช้งาน

ขั้นตอนการเปิดใช้งานระบบตู้คืนหนังสืออัตโนมัติ

หน้าที่ความรับผิดชอบ

ดูแลรับผิดชอบฐานข้อมูลและควบคุม จัดการเรื่องของการตั้งค่าของตู้คืนหนังสือ เพื่อให้พร้อมใช้งาน สำหรับการคืนหนังสือล่วงเวลาและป้องกันการสูญหายของทรัพยากรของศูนย์รบรรณสารและการเรียนรู้

ระเบียบปฏิบัติ/ขั้นตอน

- ประสานงานบริษัทเรื่องการติดตั้งระบ
- เปิดเครื่องคอมพิวเตอร์ที่อยู่ภายในตู้
- รอโปรแกรมที่ Run อัติโนมัติเปิดใช้งาน
- หมั่นตรวจเช็คให้ระบบเปิดใช้งานตลอดเวลา