การควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

วัตถุประสงค์

1. เพื่อให้การจัดการภายในหน่วยงานด้าน IT หรือศูนย์คอมพิวเตอร์ มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งเพื่อให้การปฏิบัติงานภายในศูนย์คอมพิวเตอร์เป็นไปอย่างมีระเบียบ มีระบบ และเอื้อต่อการให้บริการผู้ที่เกี่ยวข้อง รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการให้เกิดในระบบสารสนเทศ
2. เพื่อให้การจัดหาการมีและการใช้ระบบคอมพิวเตอร์และหรือระบบการสื่อสารข้อมูลของหน่วยงานราชการเป็นไปอย่างมีประสิทธิภาพ เหมาะสม และคุ้มค่ากับการลงทุน
3. เพื่อให้มีระบบรักษาความปลอดภัยและการเข้าถึงด้าน Hardware Software แฟ้มข้อมูลหรือฐานข้อมูล และรายงานที่รัดกุมเหมาะสม รวมทั้งเพื่อให้มีระบบป้องกันความเสียหายที่เกิดจากข้อผิดพลาดหรือจากการทุจริตที่อาจเกิดขึ้นภายในระบบงานคอมพิวเตอร์
4. เพื่อให้ข้อมูลและหรือสารสนเทศ ตลอดจนรายงานหรือผลลัพธ์อื่น ๆ ที่จะได้จากระบบคอมพิวเตอร์เป็นไปอย่างมีถูกต้องครบถ้วน ทันเวลา และเชื่อถือได้
5. เพื่อให้หน่วยงานต่างๆ ภายในองค์กรได้รับข้อมูลและสารสนเทศที่ถูกต้องตรงกัน และสามารถนำไปใช้ปฏิบัติงานได้อย่างมีประสิทธิภาพ โดยไม่ต้องบันทึกข้อมูลซ้ำ

ขอบเขตการควบคุม

ขอบเขตในการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

1. การควบคุมทั่วไป เป็นการกำหนดแนวทางการควบคุมการทำงานและกิจกรรมทั่ว ๆไป ที่จะมีผลให้การควบคุมระบบต่างๆ ของศูนย์คอมพิวเตอร์มีประสิทธิภาพและประสิทธิผล ซึ่งได้แก่ การควบคุมเกี่ยวกับการกำหนดแผนและนโยบายด้าน IT การกำหนดวิธีการในการปฏิบัติงาน การจัดโครงสร้างและแบ่งแยกหน้าที่ การควบคุมการใช้ด้าน Software และการ รักษาความปลอดภัยภายในศูนย์คอมพิวเตอร์
2. การควบคุมระบบงาน เป็นการกำหนดวิธีการควบคุมสำหรับระบบงาน ซึ่งได้แก่การควบคุมเกี่ยวกับการสร้างความมั่นใจว่าธุรกรรม (Transaction) ทุกรายการที่เกี่ยวข้องระบบงานคอมพิวเตอร์ ได้รับการอนุมัติ มีการนำเข้า ตรวจสอบ และประมวลผล อย่างถูกต้อง สมบูรณ์ ภายในเวลาที่เหมาะสม มีการป้องกันดูแลแฟ้มข้อมูล ฐานข้อมูล หรือ Output รวมทั้งการลดความสูญเสียที่อาจจะเกิดขึ้นจากการใช้ระบบงานและข้อมูล และมีการควบคุมหรือลดโอกาสการทำลายระบบงานและข้อมูล

แนวปฏิบัติการควบคุมภายในด้านเทศโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
1. การควบคุมทั่วไป **1.1 การควบคุมด้านการบริหารจัดการ**	1. นโยบายด้านเทคโนโลยีสารสนเทศ (IT) ของรัฐบาล 2. นโยบายด้าน IT หรือแผนแม่บท IT ของหน่วยงาน 3. งบประมาณที่ได้รับ 4. วิสัยทัศน์ และความรู้ของผู้บริหาร 5. ชนิดและประเภทของ Hardware และ Software 6. โครงสร้างของศูนย์คอมพิวเตอร์ และการมอบหมายอำนาจหน้าที่และความรับผิดชอบ 7. จำนวนเจ้าหน้าที่ที่มีความรู้ความสามารถด้าน IT ในศูนย์คอมพิวเตอร์ 8. การเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีสมัยใหม่ 9.ระเบียบและวิธีปฏิบัติ	1. แผนแม่บท IT ของหน่วยงานไม่สอดคล้องกับนโยบาย และภารกิจของหน่วยงาน รวมทั้งไม่มีการประชาสัมพันธ์หรือทำความเข้าใจเกี่ยวกับนโยบายด้าน IT ให้เจ้าหน้าที่ที่เกี่ยวข้องทราบ 2. แผนระยะยาวและแผนระยะสั้นไม่สอดคล้องกับแผนแม่บท IT 3. ผู้บริหารไม่เข้าใจและไม่สนับสนุนงานด้าน IT 4. เกิดการผูกขาดจากผู้ขายบางราย	1. กำหนดให้เจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบทบทวนนโยบายด้าน IT และปรับเปลี่ยนแผนแม่บท IT ให้สอดคล้องกับนโยบายและภารกิจของหน่วยงานและงบประมาณที่ได้รับและนำเสนอผู้บริหารทราบ 2. ติดต่อสื่อสารเพื่อแลกเปลี่ยนข้อมูลข่าวสารด้าน IT และข้อมูลข่าวสารที่จำเป็นเกี่ยวกับแผนการพัฒนางานด้าน IT ให้เจ้าหน้าที่ทุกฝ่ายทราบ 3. หน่วยงานต้องจัดให้มีการแข่งขันอย่างเสรี ในการเสนอราคาหรือเข้ารับงานด้าน IT 4. ติดตามกระบวนการจัดซื้อจัดจ้างและตรวจสอบรายชื่อผู้ชายที่ทำสัญญาซื้อขายกับหน่วยงานตามความเหมาะสม	มีการประชาสัมพันธ์และทำความเข้าใจให้เจ้าหน้าที่ทุกคนในหน่วยงานทราบอย่างทั่วถึงเกี่ยวกับ 1.1 นโยบายหรือแผนแม่บท IT 1.2 ระบบงาน ข้อมูล และรายงาน ที่มีอยู่ในความดูแลรับผิดชอบของศูนย์คอมพิวเตอร์ 2. มีการเผยแพร่ข้อมูลข่าวสารเกี่ยวกับการจัดซื้อจัดหาครุภัณฑ์คอมพิวเตอร์และหรือ Software ให้บริษัทผู้ผลิตหรือตัวแทนจำหน่ายทราบอย่างทั่วถึง	1. ติดตามผลการดำเนินงานของศูนย์คอมพิวเตอร์ ตามแผนแม่บท IT อย่างสม่ำเสมอ 2. ทบทวนการปฏิบัติงานด้าน IT อย่างเป็นระบบและต่อเนื่อง 3. ติดตามประเมินผลการประชาสัมพันธ์แผนหรือนโยบายด้าน IT และการเผยแพร่ข้อมูลข่าวสาร

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
		5. การจัดโครงการสร้างและอัตรากำลังในศูนย์คอมพิวเตอร์ไม่เหมาะสมและไม่สอดคล้องกับภารกิจด้าน IT	5. จัดให้มีการทบทวนโครงสร้างและอัตรากำลังภายในศูนย์คอมพิวเตอร์ให้เหมาะสมกับสภาพแวดล้อมและภารกิจที่เปลี่ยนแปลง รวมทั้งกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในศูนย์คอมพิวเตอร์ให้เหมาะสม	3. ชี้แจงและทำความเข้าใจเกี่ยวกับการจัดโครงสร้างและการแบ่งหน้าที่ความรับผิดชอบในศูนย์คอมพิวเตอร์	4. ประเมินความเหมาะสมของโครงสร้าง อัตรากำลังและการมอบหมายหน้าที่ความรับผิดชอบในศูนย์คอมพิวเตอร์เป็นครั้งคราว
		6. อัตราการหมุนเวียนเจ้าหน้าที่ที่มีความรู้ความชำนาญเฉพาะด้าน	6. จัดทำแผนการสืบทอดตำแหน่งงาน (Succession Plan) รวมทั้งจัดจ้างที่ปรึกษาหรือผู้เชี่ยวชาญด้าน IT เข้ามาช่วยงานด้าน IT เป็นครั้งคราวตามความจำเป็น		5. ประเมินผลแผนการสืบทอดตำแหน่งงานและผลการจ้างที่ปรึกษาและผลการดำเนินงานของที่ปรึกษา
		7. เจ้าหน้าที่ด้าน IT ปรับตัวไม่ทันกับเทคโนโลยีสมัยใหม่และไม่มีความรู้ความสามารถใช้เครื่องมือหรืออุปกรณ์คอมพิวเตอร์ที่ได้มาใหม่อย่างมีประสิทธิภาพได้	7. จัดให้มีการอบรมโดยผู้เชี่ยวชาญอย่างเพียงพอทุกครั้งที่มีการจัดหาเครื่องมือหรืออุปกรณ์คอมพิวเตอร์ใหม่ 8. มีการแลกเปลี่ยนและถ่ายทอดความรู้ด้านเทคโนโลยีใหม่ให้แก่เจ้าหน้าที่ด้าน IT	4. สื่อสารและแลกเปลี่ยนข้อมูลข่าวสารด้าน IT กับหน่วยงานหรือบุคคลที่มีความรู้ความเชี่ยวชาญเฉพาะด้านอย่างสม่ำเสมอ.	6. ติดตามและประเมินศักยภาพเจ้าหน้าที่ด้าน IT อย่างสม่ำเสมอ
		8. ไม่มีแผนและงบประมาณสำหรับการพัฒนาเจ้าหน้าที่ด้าน IT อย่างต่อเนื่อง	9. จัดทำแผนล่วงหน้าในการพัฒนาและฝึกอบรมเจ้าหน้าที่ด้าน IT ให้ทันกับการเปลี่ยนแปลงของเทคโนโลยีใหม่ๆ	5. มีการประชาสัมพันธ์เกี่ยวกับการพัฒนาและฝึกอบรมให้ทราบโดยทั่วกัน	

แนวปฏิบัติการควบคุมภายในด้านเทศโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
			10.จัดหางบประมาณและแหล่งเงินทุนสนับสนุนในการพัฒนาและฝึกอบรมให้แก่เจ้าหน้าที่อย่างต่อเนื่อง		
		9. เจ้าหน้าที่ปฏิบัติงานไม่เป็นไปตามระเบียบและวิธีปฏิบัติที่กำหนด	11. จัดทำคู่มือการปฏิบัติงานและแบบฟอร์มมาตรฐานในการรับส่งงานระหว่างเจ้าหน้าที่ศูนย์คอมพิวเตอร์และผู้ใช้ (Users) 12. จัดให้มีการฝึกอบรมความรู้เกี่ยวกับระเบียบและวิธีปฏิบัติให้ผู้ที่เกี่ยวข้องทราบ	6. เวียนแจ้งระเบียบ วิธีปฏิบัติคู่มือการปฏิบัติงานและแบบฟอร์มมาตรฐานในการรับส่งงานให้ทราบทั่วกัน	7. ติดตามผลการปฏิบัติงานของเจ้าหน้าที่ผู้ปฏิบัติงาน

แนวปฏิบัติการควบคุมภายในด้านเทศโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
1.2. การควบคุมด้าน Hardware Software และ application	1. ความต้องการใช้งานด้าน IT 2. นโยบายในการพัฒนาระบบงานและประสิทธิภาพของการบริหารจัดการที่เกี่ยวข้องกับการพัฒนาระบบงานของศูนย์คอมพิวเตอร์ 3. ประสิทธิภาพของอุปกรณ์คอมพิวเตอร์และการใช้งานของผู้ที่เกี่ยวข้อง 4. มาตรการการบริหารทรัพยากรด้าน IT (วัสดุครุภัณฑ์ และของใช้สิ้นเปลืองต่างๆ เช่น กระดาษต่อเนื่อง ผ้าหมึก Tape แผ่น Diskette)	1. การจัดซื้อระบบคอมพิวเตอร์และระบบ รวมทั้งการพัฒนาหรือการปรับปรุงแก้ไขระบบงานไม่สอดคล้อง และไม่เพียงพอกับความต้องการใช้งาน และอุปกรณ์เครื่องคอมพิวเตอร์ล้าสมัย. 2. มีการพัฒนา/แก้ไข/ติดตั้ง/ใช้งาน ระบบงานโดยไม่ได้รับอนุญาต 3. เอกสารหลักฐานประกอบการออกแบบและเขียนโปรแกรมระบบงานไม่ครบถ้วนหรือสูญหายทำให้เกิดความไม่ต่อเนื่องในการดูแลหรือปรับปรุงแก้ไข (Maintainanc) ในภายหลัง 4. Source Program ระบบงานและเอกสารประกอบสูญหายหรือได้รับความเสียหายจากเหตุที่คาดไม่ถึง	1. สำรวจความต้องการของผู้ใช้หรือผู้ที่เกี่ยวข้องทุกฝ่ายก่อนการจัดซื้อจัดจ้างหรือก่อนการพัฒนาและปรับปรุงแก้ไขระบบงาน 2. ผู้บริหารของหน่วยงานผู้ใช้ควรมีส่วนร่วมในการกำหนดความต้องการงานด้าน IT และการพัฒนาหรือปรับปรุงแก้ไขระบบงาน 3. กำหนดให้การพัฒนา//แก้ไข/ติดตั้ง/ใช้งาน ระบบงานที่สำคัญต้องได้รับอนุญาตจากผู้มีอำนาจ 4. กำชับให้ผู้มีหน้าที่รับผิดชอบจัดทำเอกสาร ประกอบระบบงานให้ครบถ้วนและจัดเก็บอย่างเป็นระบบ 5. สอบทานกระบวนการหรือวิธีการจัดเก็บเอกสารหรือ Media ที่ใช้ประกอบการออกแบบระบบงานรวมทั้งวิธีการเก็บหรือดูแลรักษา Source Program อย่างสม่ำเสมอ 6. กำหนดให้มีการ Backup หรือทำสำเนา Source Program ระบบงาน และเอกสารประกอบที่สำคัญอย่างน้อย 2 ชุด และแยกสถานที่จัดเก็บ รวมทั้งจัดทำทะเบียนคุมไว้เป็นหลักฐาน	1. ประชาสัมพันธ์แผนการจัดซื้อจัดจ้างและแนวทางในการพัฒนาหรือปรับปรุงระบบงานให้ผู้เกี่ยวข้องทราบทั่วกัน 2. ชี้แจงหลักเกณฑ์หรือมาตรการในการปฏิบัติงานด้านการออกแบบการเขียนโปรแกรม รวมทั้งการจัดเก็บเอกสาร และ Source Program ให้ทราบทั่วกัน 3. ทำความเข้าใจโดยชี้แจงและจัดให้มี การประชาสัมพันธ์วิธีการใช้และการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ให้เจ้าหน้าที่ทุกฝ่ายที่เกี่ยวข้อง	1. ติดตามผลการจัดซื้อระบบคอมพิวเตอร์ รวมทั้งการพัฒนาระบบงานให้เป็นไปตามข้อตกลงที่ได้จากการศึกษาและสำรวจความต้องการ 2. สอบทานความเหมาะสมของกระบวนการพัฒนาระบบงาน/การแก้ไข /การจัดตั้ง/การใช้งาน/การจัดเก็บและการดูแลรักษาระบบงาน Hardware และ Software 3. ประเมินความเหมาะสมของวิธีการและมาตรการในการใช้ทรัพยากรด้าน IT

แนวปฏิบัติการควบคุมภายในด้านเทศโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
		5. เครื่องคอมพิวเตอร์และอุปกรณ์ถูกใช้งานอย่างไม่เหมาะสมและไม่ถูกวิธี ทำให้เกิดการเสื่อมสภาพก่อนเวลาอันควร 6. เครื่องคอมพิวเตอร์และอุปกรณ์สูญหาย หรือเกิดการเสียหาย	7. จัดให้มีคู่มือการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่ถูกวิธี 8. จัดให้มีระบบบำรุงรักษาที่ต่อเนื่องเหมาะสม และครอบคลุมครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ทุกประเภท 9. กำหนดให้มีการจัดทำทะเบียนคุมครุภัณฑ์คอมพิวเตอร์ พร้อมทั้งให้มีการสอบทานการลงทะเบียนคุมเป็นประจำ และจัดให้มีการตรวจนับครุภัณฑ์คอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง 10. จัดให้มีการประกันภัยครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ที่ใช้กับงานสำคัญๆ		4. ประเมินและตรวจสอบความเพียงพอและความทันสมัยของคู่มือการใช้อุปกรณ์คอมพิวเตอร์ 5. ประเมินการใช้ประโยชน์จากครุภัณฑ์คอมพิวเตอร์ทุกรายการ 6. ประเมินความเหมาะสมของระบบการประกันภัยครุภัณฑ์คอมพิวเตอร์และอุปกรณ์
		.7. ไม่มีมาตรการหรือแผนรองรับเหตุฉุกเฉินหรือการหยุดชะงักของระบบคอมพิวเตอร์	11. จัดให้มีแผนรองรับเหตุฉุกเฉินหรือเหตุหยุดชะงักของระบบคอมพิวเตอร์	4. ชี้แจงและประชาสัมพันธ์ เกี่ยวกับแผนสำรอง หรือการดำเนินงานภายใต้แผนฉุกเฉินให้กับเจ้าหน้าที่ที่เกี่ยวข้องทราบอย่างทั่วถึง	7. ประเมินความเหมาะสมของแผนฉุกเฉินหรือระบบทดแทนเป็นครั้งคราวตามความเหมาะสม

แนวปฏิบัติการควบคุมภายในด้านเทศโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
		8. การใช้ทรัพยากรด้าน IT เป็นไปอย่างไม่เหมาะสม ทำให้เกิดความสิ้นเปลืองและใช้ประโยชน์อย่างไม่คุ้มค่า	12. มีการซักซ้อมการทำงานภายใต้แผนสำรองหรือระบบทดแทนในส่วนที่เป็นระบบงานสำคัญๆ ของหน่วยงานเป็นครั้งคราว หรือตามความเหมาะสม 13. จัดให้มีระบบบริหารและตรวจสอบการใช้ทรัพยากรด้าน IT ที่เหมาะสม 14. จัดให้มีการอบรมและเสริมสร้างจริยธรรมหรือจิตสำนึกในการปฏิบัติงานให้เจ้าหน้าที่ที่เกี่ยวข้องให้ใช้ทรัพยากรด้าน IT อย่างประหยัดและสมประโยชน์	5. ชี้แจง ประชาสัมพันธ์ความรู้เกี่ยวกับการใช้ทรัพยากรด้าน IT ที่ถูกวิธีและเหมาะสมให้กับเจ้าหน้าที่ทุกฝ่ายทราบ	

แนวปฏิบัติการควบคุมภายในด้านเทศโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
1.3. การควบคุมด้านการรักษาความปลอดภัยของศูนย์คอมพิวเตอร์	มาตรการหรือนโยบายด้านการรักษาความปลอดภัยและการบำรุงรักษา	1.ระบบรักษาความปลอดภัยของศูนย์คอมพิวเตอร์ไม่เพียงพอไม่รัดกุม ทำให้มีการเข้าออกศูนย์คอมพิวเตอร์โดยไม่ได้รับอนุญาต 2. ไม่มีมาตรการป้องกันระบบคอมพิวเตอร์และระบบการสื่อสารข้อมูล รวมทั้งเกิดภัยอันตรายอื่นๆ เช่น Virus Computer การจารกรรมข้อมูลหรือการHacker 3. มีการนำ Software จากภายนอกและไม่ได้รับอนุญาตเข้ามาใช้ในหน่วยงาน	1. จัดให้มีระบบเวรยามหรือมาตรการการรักษาความปลอดภัย รวมทั้งการกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ที่เหมาะสมและรัดกุมและสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบข้อมูล 2. กำกับดูแลให้มีการปฏิบัติตามมาตรการรักษาความปลอดภัยอย่างเคร่งครัด 3. กำหนดให้มีการจัดทำทะเบียนคุมการติดตั้งหรือการนำ Software จากภายนอกเข้ามาใช้กับเครื่องคอมพิวเตอร์ในหน่วยงาน	1. ชี้แจงประชาสัมพันธ์และให้ความรู้เกี่ยวกับระบบรักษาความปลอดภัยและภยันตรายต่างๆ หรือความเสียหายจากการใช้คอมพิวเตอร์หรืออุปกรณ์ด้าน IT ที่ไม่เหมาะสมให้เจ้าหน้าที่ทราบทั่วกัน 2. เวียนแจ้งมาตรการควบคุมการนำ Software มาจากภายนอกเข้ามาใช้ในหน่วยงาน ให้ทราบทั่วกัน	1. ประเมินความเหมาะสมของมาตรการรักษาความปลอดภัย 2. ประเมินสถิติที่เกิดจากการฝ่าฝืนการเข้าออกศูนย์คอมพิวเตอร์และระบบข้อมูลโดยไม่ได้รับอนุญาต 3. ติดตามการใช้ Software ที่ติดตั้งในเครื่องคอมพิวเตอร์เป็นครั้งคราว 4. ติดตามหรือสอบทานการปฏิบัติตามมาตรการรักษาความปลอดภัยเป็นครั้งคราว

แนวปฏิบัติการควบคุมภายในด้านเทศโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
2. การควบคุมระบบงาน **2.1 การควบคุมการเข้าถึงระบบงาน แฟ้มข้อมูล และฐานข้อมูล**	1. มาตรการรักษาความปลอดภัยและกำหนดสิทธิในการเข้าถึงระบบงานและระบบข้อมูล 2. ความรู้ความสามารถตลอดจนทักษะในการใช้ Hardware Software และอุปกรณ์การสื่อสารของเจ้าหน้าที่ในศูนย์คอมพิวเตอร์และผู้ใช้ 3. จริยธรรมและความซื่อสัตย์ของเจ้าหน้าที่ที่เกี่ยวข้อง	1. ระบบรักษาความปลอดภัย รวมทั้งการกำหนดสิทธิในการเข้าถึงระบบงาน และข้อมูลไม่รัดกุมหรือไม่เพียงพอ 2. ไม่มีการพัฒนาระบบวานให้ทันสมัยอยู่เสมอ 3. ผู้ใช้ (Users) ขาดความรู้ความชำนาญในการใช้เครื่องคอมพิวเตอร์ในการปฏิบัติงานรวมทั้งการใช้ระบบงาน	1. ให้ผู้มีหน้าที่รับผิดชอบศึกษาทบทวนระบบรักษาความปลอดภัยและการกำหนดสิทธิในการเข้าถึงระบบงาน และฐานข้อมูลที่สำคัญ 2.ให้มีเจ้าหน้าที่จัดทำทะเบียนคุม USER ID โดยเฉพาะ 3. มีการปรับปรุงพัฒนาระบบและสิทธิหรี USER ID ในการเข้าถึงระบบงานและระบบข้อมูลเป็นระยะๆ 4. จัดให้มีคู่มือการปฏิบัติงาน สำหรับผู้ใช้งาน (Users) ทุกระบบงานอย่างเพียงพอ และจัดฝึกอบรมผู้ใช้รายใหม่อย่างสม่ำเสมอ	1. สื่อสารและทำความเข้าใจกับเจ้าหน้าที่ทุกฝ่ายของหน่วยงานเกี่ยวกับมาตรการรักษาความปลอดภัย การใช้งานในระบบงานคอมพิวเตอร์และการปฏิบัติงานด้าน IT 2. สื่อสารให้เจ้าหน้าที่ที่เกี่ยวข้องทราบถึงการใช้ระบบงาน	1. ประเมินความเหมาะสมของระบบรักษาความปลอดภัยและคู่มือการปฏิบัติงานเป็นระยะ ๆ 2. ประเมินผลการจัดอบรมและประเมินผลเจ้าหน้าที่ที่ผ่านการฝึกอบรม

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
2.2. การควบคุมการนำเข้าข้อมูล	1. ประสิทธิภาพของระบบงานและระบบคอมพิวเตอร์ 2. ความรู้และทักษะของเจ้าหน้าที่ที่เกี่ยวข้อง 3. ความพร้อมของเอกสารหรือข้อมูลที่จะนำเข้าระบบ	1. บันทึกข้อมูลผิดพลาดไม่ครบถ้วน ไม่ถูกต้อง 2. ข้อมูลที่บันทึกเข้าระบบไม่ได้รับการตรวจทาน หรือสอบทานความถูกต้องก่อนการส่งต่อ	จัดให้มีการตรวจสอบข้อมูลหรือเข้าทั้งจัดให้มีรายงานจากโปนแกรมระบบงานสำหรับใช้ในการตรวจสอบ หรือสอบทานความถูกต้องของข้อมูลก่อนการส่งต่อ	เวียนแจ้งให้เจ้าหน้าที่เกี่ยวข้องทราบถึงมาตรการหรือวิธีการนำเข้าข้อมูล	ประเมินความเหมาะสมของมาตรการการนำเข้าข้อมูลเป็นครั้งคราว

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
2.3. การควบคุมด้านการประมวลผลเพื่อจัดทำข้อมูลสารสนเทศและรายงาน	1. ความต้องการใช้ข้อมูลและสารสนเทศของฝ่ายบริหารและหน่วยงานที่เกี่ยวข้อง 2. แผนการปฏิบัติงานในห้องเครื่องคอมพิวเตอร์ 3. ความรู้และทักษะของเจ้าหน้าที่ที่เกี่ยวข้อง 4. จริยธรรม และความซื่อสัตย์ของผู้นำข้อมูลเข้าระบบ	1. ข้อมูลและรายงานที่ได้จากการประมวลผลไม่ตรงตามความต้องการ หรือไม่ทันกับความต้องการของผู้ที่เกี่ยวข้อง 2. ไม่มีการวางแผนเกี่ยวกับความต้องการใช้ข้อมูลและรายงานของผู้ที่เกี่ยวข้อง 3. ไม่มีการจัดทำแผนหรือตารางการปฏิบัติงานของเจ้าหน้าที่เครื่องคอมพิวเตอร์ 4. เจ้าหน้าที่ขาดความรู้ และขาดทักษะในการใช้ระบบคอมพิวเตอร์คำสั่งในการประมวลผล 5. เจ้าหน้าที่นำข้อมูลไปใช้เพื่อประโยชน์ส่วนตัว	1. ศึกษาความต้องการของผู้ใช้หรือผู้ที่เกี่ยวข้องทุกฝ่ายเพื่อวางแผนล่วงหน้าในการจัดทำข้อมูลและรายงานให้ทันกับความต้องการ 2. จัดให้มีตารางการปฏิบัติงานรวมทั้งใบสั่งงานหรือเอกสารการส่งมอบงานสำหรับเจ้าหน้าที่ที่ทำหน้าที่ประมวลผลและจัดทำตารางการส่งงานให้ชัดเจนเพื่อให้ข้อมูลและรายงานส่งถึงมือผู้ใช้ในเวลาที่เหมาะสม 3. มีการจัดระบบความคุมการรับส่งการแลกเปลี่ยนและการสื่อสารข้อมูลหรือรายงานให้ถึงมือผู้ใช้อย่างเป็นระบบครอบคลุม และทันเวลาและมีการสื่อสาร เพื่อให้ได้ข้อมูลย้อนกลับจากผู้ใช้ 4. จัดให้มีการฝึกอบรมอย่างต่อเนื่องและให้มีการจัดทำคู่มือปฏิบัติงานในเรื่องต่าง ๆที่ เกี่ยวข้อง 5. จัดอบรมแก่เจ้าหน้าที่ให้มีความเข้าใจเรื่อง Conflict of interest (ความขัดแย้งเกี่ยวกับผลประโยชน์)	เผยแพร่คู่มือหรือหลักเกณฑ์การปฏิบัติงานด้วยเครื่องคอมพิวเตอร์ให้ผู้ที่เกี่ยวข้องทราบทั่วกัน	1. ประเมินผลการใช้ประโยชน์จากข้อมูลสารสนเทศและรายงาน 2. ประเมินความเหมาะสมของหลักเกณฑ์หรือมาตรการเกี่ยวกับการการประมวลผล 3. ประเมินความเหมาะของการปฏิบัติงานและตารางการส่งมอบงาน 4. ประเมินความเหมาะสมของการจัดฝึกอบรมเจ้าหน้าที่ที่ทำหน้าที่ประมวลผลเป็นครั้งคราว

แนวปฏิบัติการควบคุมภายในด้านเทศโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
2.4. การควบคุมด้านการรับ – ส่งข้อมูลระหว่างระบบงานและระหว่างหน่วยงาน	มาตรการหรือระเบียบวิธีการในการรับส่งข้อมูล และการสื่อสารข้อมูลในหน่วยงานและนโยบายในการรักษาความลับของข้อมูล	1. ข้อมูลหรือรายงานที่เป็นความลับของหน่วยงานถูกนำไปเผยแพร่ หรือนำไปใช้ประโยชน์โดยไม่ได้รับอนุญาต 2. การส่งต่อข้อมูลไม่เป็นไปตามกำหนดเวลา	1. กำหนดหลักเกณฑ์และมาตรการในการนำข้อมูลหรือรายงานออกนอกสถานที่ หรือออกจากศูนย์คอมพิวเตอร์ 2. จัดให้มีระบบควบคุมการรับส่งข้อมูล หรือการส่งต่อข้อมูลระหว่างระบบงาน	เวียนแจ้งมาตรการรักษาความลับของข้อมูลและรายงานให้เจ้าหน้าที่ที่เกี่ยวข้องทราบทั่วกัน รวมทั้งชี้แจงทำความเข้าใจเกี่ยวกับเวลาและกระบวนในการส่งมอบงานในแต่ละขั้นตอน	ประเมินความเหมาะสมของระบบรักษาความปลอดภัยของข้อมูลและรายงาน รวมทั้งการกำหนดสิทธิในการเข้าถึงระบบงานและระบบข้อมูลอย่างสม่ำเสมอ

แนวปฏิบัติการควบคุมภายในด้านเทศโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
2.5. การควบคุมดูแลรักษาระบบงาน แฟ้มและฐานข้อมูล	ระบบจัดเก็บและรักษาข้อมูล	1. ระบบจัดเก็บแฟ้มข้อมูล ฐานข้อมูล และรายงานต่างๆ ไม่ดี หรือไม่เหมาะสม 2. สื่อหรือ MEDIA ที่ใช้ในการสำรองข้อมูลไม่มีคุณภาพ	1. กำหนดระบบการจัดเก็บ และสำรองแฟ้มข้อมูล ฐานข้อมูล และรายงานต่างๆ ให้เหมาะสมกับการใช้งาน 2. จัดให้มีการสำรองข้อมูลให้ครบถ้วนตามความเหมาะสมของแต่ละระบบงาน และตามเวลาที่กำหนด 3. จัดให้มีการทดสอบความถูกต้องของข้อมูลที่สำรองไว้เป็นครั้งคราว และทำรายงานผลการทดสอบ	ประชาสัมพันธ์และชี้แจงมาตรการในการดูแลและเก็บรักษาระบบงาน ระบบข้อมูลให้เจ้าหน้าที่ที่เกี่ยวข้องทราบ	ประเมินความเหมาะสมของระบบจัดเก็บและสำรองแฟ้มข้อมูล ฐานข้อมูลและรายงาน