

การควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

วัตถุประสงค์

๑. เพื่อให้การจัดการภายในหน่วยงานด้าน IT หรือศูนย์คอมพิวเตอร์ มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งเพื่อให้การปฏิบัติงานภายในศูนย์คอมพิวเตอร์เป็นไปอย่างมีระเบียบ มีระบบ และเอื้อต่อการให้บริการผู้ที่เกี่ยวข้อง รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการให้เกิดในระบบสารสนเทศ

๒. เพื่อให้การ จัดหา การมี และการใช้ระบบคอมพิวเตอร์และหรือระบบการสื่อสารข้อมูลของหน่วยงานราชการเป็นไปอย่างมีประสิทธิภาพ เหมาะสม และคุ้มค่ากับการลงทุน

๓. เพื่อให้มีระบบรักษาความปลอดภัยและการเข้าถึงด้าน Hardware Software แพ้มข้อมูลหรือฐานข้อมูลและรายงานที่รัดกุมเหมาะสม รวมทั้งเพื่อให้มีระบบป้องกันความเสียหายที่เกิดจากข้อผิดพลาดหรือจากการทุจริตที่อาจเกิดขึ้นภายในระบบงานคอมพิวเตอร์

๔. เพื่อให้ข้อมูลและหรือสารสนเทศ ตลอดจนรายงานหรือผลลัพธ์อื่น ๆ ที่จะได้จากระบบคอมพิวเตอร์เป็นไปอย่างมีถูกต้องครบถ้วน ทันเวลา และเชื่อถือได้

๕. เพื่อให้หน่วยงานต่างๆ ภายในองค์กรได้รับข้อมูลและสารสนเทศที่ถูกต้องตรงกัน และสามารถนำไปใช้ปฏิบัติงานได้อย่างมีประสิทธิภาพ โดยไม่ต้องบันทึกข้อมูลซ้ำ

ขอบเขตการควบคุม

ขอบเขตในการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

๑. การควบคุมทั่วไป เป็นการกำหนดแนวทางการควบคุมการทำงานและกิจกรรมทั่ว ๆ ไป ที่จะมีผลให้การควบคุมระบบต่างๆ ของศูนย์คอมพิวเตอร์มีประสิทธิภาพและประสิทธิผล ซึ่งได้แก่ การควบคุมเกี่ยวกับการกำหนดแผนและนโยบายด้าน IT การกำหนดวิธีการในการปฏิบัติงาน การจัดโครงสร้างและแบ่งแยกหน้าที่การควบคุมการใช้ด้าน Software และการรักษาความปลอดภัยภายในศูนย์คอมพิวเตอร์

๒. การควบคุมระบบงาน เป็นการกำหนดวิธีการควบคุมสำหรับระบบงาน ซึ่งได้แก่การควบคุมเกี่ยวกับการสร้างความมั่นใจว่าธุรกรรม (Transaction) ทุกรายการที่เกี่ยวข้องระบบงานคอมพิวเตอร์ ได้รับการอนุมัติ มีการนำเข้า ตรวจสอบ และประมวลผล อย่างถูกต้อง สมบูรณ์ ภายในเวลาที่เหมาะสม มีการป้องกันดูแลแพ้มข้อมูลฐานข้อมูล หรือ Output รวมทั้งการลดความสูญเสียที่อาจเกิดขึ้นจากการใช้ระบบงานและข้อมูล และมีการควบคุมหรือลดโอกาสการทำลายระบบงานและข้อมูล

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
<p>๑. การควบคุมทั่วไป</p> <p>๑.๑ การควบคุมด้านการบริหารจัดการ</p>	<p>๑. นโยบายด้านเทคโนโลยีสารสนเทศ (IT) ของรัฐบาล</p> <p>๒. นโยบายด้าน IT หรือแผนแม่บท IT ของหน่วยงาน</p> <p>๓. งบประมาณที่ได้รับ</p> <p>๔. วิสัยทัศน์ และความรู้ของผู้บริหาร</p> <p>๕. ชนิดและประเภทของ Hardware และ Software</p> <p>๖. โครงสร้างของศูนย์คอมพิวเตอร์ และการมอบหมายอำนาจหน้าที่และความรับผิดชอบ</p> <p>๗. จำนวนเจ้าหน้าที่ที่มีความรู้ความสามารถด้าน IT ในศูนย์คอมพิวเตอร์</p> <p>๘. การเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีสมัยใหม่</p> <p>๙. ระเบียบและวิธีปฏิบัติ</p>	<p>๑. แผนแม่บท IT ของหน่วยงานไม่สอดคล้องกับนโยบาย และภารกิจของหน่วยงาน รวมทั้งไม่มีการประชาสัมพันธ์หรือทำความเข้าใจเกี่ยวกับนโยบายด้าน IT ให้เจ้าหน้าที่ที่เกี่ยวข้องทราบ</p> <p>๒. แผนระยะยาวและแผนระยะสั้นไม่สอดคล้องกับแผนแม่บท IT</p> <p>๓. ผู้บริหารไม่เข้าใจและไม่สนับสนุนงานด้าน IT</p> <p>๔. เกิดการผูกขาดจากผู้ขายบางราย</p>	<p>๑. กำหนดให้เจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบทบทวนนโยบายด้าน IT และปรับเปลี่ยนแผนแม่บท IT ให้สอดคล้องกับนโยบายและภารกิจของหน่วยงานและงบประมาณที่ได้รับและนำเสนอผู้บริหารทราบ</p> <p>๒. ติดต่อสื่อสารเพื่อแลกเปลี่ยนข้อมูลข่าวสารด้าน IT และข้อมูลข่าวสารที่จำเป็นเกี่ยวกับแผนการพัฒนางานด้าน IT ให้เจ้าหน้าที่ทุกฝ่ายทราบ</p> <p>๓. หน่วยงานต้องจัดให้มีการแข่งขันอย่างเสรี ในการเสนอราคาหรือเข้ารับงานด้าน IT</p> <p>๔. ติดตามกระบวนการจัดซื้อจัดจ้างและตรวจสอบรายชื่อผู้ขายที่ทำสัญญาซื้อขายกับหน่วยงานตามความเหมาะสม</p>	<p>มีการประชาสัมพันธ์และทำความเข้าใจให้เจ้าหน้าที่ทุกคนในหน่วยงานทราบอย่างทั่วถึงเกี่ยวกับ</p> <p>๑.๑ นโยบายหรือแผนแม่บท IT</p> <p>๑.๒ ระบบงาน ข้อมูล และรายงาน ที่มีอยู่ในความดูแลรับผิดชอบของศูนย์คอมพิวเตอร์</p> <p>๒. มีการเผยแพร่ข้อมูลข่าวสารเกี่ยวกับการจัดซื้อจัดหาครุภัณฑ์คอมพิวเตอร์ และหรือ Software ให้บริษัทผู้ผลิตหรือตัวแทนจำหน่ายทราบอย่างทั่วถึง</p>	<p>๑. ติดตามผลการดำเนินงานของศูนย์คอมพิวเตอร์ ตามแผนแม่บท IT อย่างสม่ำเสมอ</p> <p>๒. ทบทวนการปฏิบัติงานด้าน IT อย่างเป็นระบบและต่อเนื่อง</p> <p>๓. ติดตามประเมินผล การประชาสัมพันธ์แผนหรือนโยบายด้าน IT และการเผยแพร่ข้อมูลข่าวสาร</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
		<p>๕. การจัดโครงการสร้างและอัปเดตกำลังในศูนย์คอมพิวเตอร์ไม่เหมาะสมและไม่สอดคล้องกับภารกิจด้าน IT</p> <p>๖. อัตราการหมุนเวียนเจ้าหน้าที่ที่มีความรู้ความชำนาญเฉพาะด้าน</p> <p>๗. เจ้าหน้าที่ด้าน IT ปรับตัวไม่ทันกับเทคโนโลยีสมัยใหม่ และไม่มีความรู้ความสามารถใช้เครื่องมือหรืออุปกรณ์คอมพิวเตอร์ที่ได้มาใหม่อย่างมีประสิทธิภาพได้</p> <p>๘. ไม่มีแผนและงบประมาณสำหรับการพัฒนาเจ้าหน้าที่ด้าน IT อย่างต่อเนื่อง</p>	<p>๕. จัดให้มีการทบทวนโครงสร้างและอัปเดตกำลังภายในศูนย์คอมพิวเตอร์ให้เหมาะสมกับสภาพแวดล้อมและภารกิจที่เปลี่ยนแปลง รวมทั้งกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในศูนย์คอมพิวเตอร์ให้เหมาะสม</p> <p>๖. จัดทำแผนการสืบทอดตำแหน่งงาน (Succession Plan) รวมทั้งจัดจ้างที่ปรึกษาหรือผู้เชี่ยวชาญด้าน IT เข้ามาช่วยงานด้าน IT เป็นครั้งคราวตามความจำเป็น</p> <p>๗. จัดให้มีการอบรมโดยผู้เชี่ยวชาญอย่างเพียงพอทุกครั้งที่มีการจัดหาเครื่องมือหรืออุปกรณ์คอมพิวเตอร์ใหม่</p> <p>๘. มีการแลกเปลี่ยนและถ่ายทอดความรู้ด้านเทคโนโลยีใหม่ให้แก่เจ้าหน้าที่ด้าน IT</p> <p>๙. จัดทำแผนล่วงหน้าในการพัฒนาและฝึกอบรมเจ้าหน้าที่ด้าน IT ให้ทันกับการเปลี่ยนแปลงของเทคโนโลยีใหม่ๆ</p>	<p>๓. ชี้แจงและทำความเข้าใจเกี่ยวกับการจัดโครงสร้างและการแบ่งหน้าที่ความรับผิดชอบในศูนย์คอมพิวเตอร์</p> <p>๔. สื่อสารและแลกเปลี่ยนข้อมูลข่าวสารด้าน IT กับหน่วยงานหรือบุคคลที่มีความรู้ความเชี่ยวชาญเฉพาะด้านอย่างสม่ำเสมอ.</p> <p>๕. มีการประชาสัมพันธ์เกี่ยวกับการพัฒนาและฝึกอบรมให้ทราบโดยทั่วกัน</p>	<p>๔. ประเมินความเหมาะสมของโครงสร้างอัปเดตกำลังและการมอบหมายหน้าที่ความรับผิดชอบในศูนย์คอมพิวเตอร์เป็นครั้งคราว</p> <p>๕. ประเมินผลแผนการสืบทอดตำแหน่งงานและผลการจ้างที่ปรึกษาและผลการดำเนินงานของที่ปรึกษา</p> <p>๖. ติดตามและประเมินศักยภาพเจ้าหน้าที่ด้าน IT อย่างสม่ำเสมอ</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
		<p>๙. เจ้าหน้าที่ปฏิบัติงานไม่เป็นไปตามระเบียบและวิธีปฏิบัติที่กำหนด</p>	<p>๑๐. จัดหางบประมาณและแหล่งเงินทุนสนับสนุนในการพัฒนาและฝึกอบรมให้แก่เจ้าหน้าที่อย่างต่อเนื่อง</p> <p>๑๑. จัดทำคู่มือการปฏิบัติงานและแบบฟอร์มมาตรฐานในการรับส่งงานระหว่างเจ้าหน้าที่ศูนย์คอมพิวเตอร์และผู้ใช้ (Users)</p> <p>๑๒. จัดให้มีการฝึกอบรมความรู้เกี่ยวกับระเบียบและวิธีปฏิบัติให้ผู้ที่เกี่ยวข้องทราบ</p>	<p>๖. เวียนแจ้งระเบียบวิธีปฏิบัติคู่มือการปฏิบัติงานและแบบฟอร์มมาตรฐานในการรับส่งงานให้ทราบทั่วกัน</p>	<p>๗. ติดตามผลการปฏิบัติงานของเจ้าหน้าที่ปฏิบัติงาน</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
<p>๑.๒. การควบคุมด้าน Hardware Software และ application</p>	<p>๑. ความต้องการใช้งานด้าน IT</p> <p>๒. นโยบายในการพัฒนาระบบงานและประสิทธิภาพของการบริหารจัดการที่เกี่ยวข้องกับการพัฒนาระบบงานของศูนย์คอมพิวเตอร์</p> <p>๓. ประสิทธิภาพของอุปกรณ์คอมพิวเตอร์และการใช้งานของผู้ที่เกี่ยวข้อง</p> <p>๔. มาตรการการบริหารทรัพยากรด้าน IT (วัสดุ ครุภัณฑ์ และของใช้สิ้นเปลืองต่างๆ เช่น กระดาษต่อเนื่อง ผ้าหมึก Tape แผ่น Diskette)</p>	<p>๑. การจัดซื้อระบบคอมพิวเตอร์และระบบรวมทั้งการพัฒนาหรือการปรับปรุงแก้ไขระบบงานไม่สอดคล้อง และไม่เพียงพอกับความต้องการใช้งานและอุปกรณ์เครื่องคอมพิวเตอร์ล้ำสมัย.</p> <p>๒. มีการพัฒนา/แก้ไข/ติดตั้ง/ใช้งาน ระบบงานโดยไม่ได้รับอนุญาต</p> <p>๓. เอกสารหลักฐานประกอบการออกแบบและเขียนโปรแกรมระบบงานไม่ครบถ้วนหรือสูญหายทำให้เกิดความไม่ต่อเนื่องในการดูแลหรือปรับปรุงแก้ไข (Maintainanc) ในภายหลัง</p> <p>๔. Source Program ระบบงานและเอกสารประกอบสูญหายหรือได้รับความเสียหายจากเหตุที่คาดไม่ถึง</p>	<p>๑. สํารวจความต้องการของผู้ใช้หรือผู้ที่เกี่ยวข้องทุกฝ่ายก่อนการจัดซื้อจัดจ้างหรือก่อนการพัฒนาและปรับปรุงแก้ไขระบบงาน</p> <p>๒. ผู้บริหารของหน่วยงานผู้ใช้ควรมีส่วนร่วมในการกำหนดความต้องการงานด้าน IT และการพัฒนาหรือปรับปรุงแก้ไขระบบงาน</p> <p>๓. กำหนดให้การพัฒนา//แก้ไข/ติดตั้ง/ใช้งาน ระบบงานที่สำคัญต้องได้รับอนุญาตจากผู้มีอำนาจ</p> <p>๔. กำชับให้ผู้มีหน้าที่รับผิดชอบจัดทำเอกสาร ประกอบระบบงานให้ครบถ้วน และจัดเก็บอย่างเป็นระบบ</p> <p>๕. สอบทานกระบวนการหรือวิธีการจัดเก็บเอกสาร หรือ Media ที่ใช้ประกอบการออกแบบระบบงานรวมทั้งวิธีการเก็บหรือดูแลรักษา Source Program อย่างสม่ำเสมอ</p> <p>๖. กำหนดให้มีการ Backup หรือทำสำเนา Source Program ระบบงาน และเอกสารประกอบที่สำคัญอย่างน้อย ๒ ชุด และแยกสถานที่จัดเก็บ รวมทั้งจัดทำทะเบียนคุมไว้เป็นหลักฐาน</p>	<p>๑. ประชาสัมพันธ์แผนการจัดซื้อจัดจ้างและแนวทางในการพัฒนาหรือปรับปรุงระบบงานให้ผู้เกี่ยวข้องทราบทั่วกัน</p> <p>๒. ชี้แจงหลักเกณฑ์หรือมาตรการในการปฏิบัติงานด้านการออกแบบการเขียนโปรแกรม รวมทั้งการจัดเก็บเอกสาร และ Source Program ให้ทราบทั่วกัน</p> <p>๓. ทำความเข้าใจโดยชี้แจงและจัดให้มี การประชาสัมพันธ์วิธีการใช้และการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ให้เจ้าหน้าที่ทุกฝ่ายที่เกี่ยวข้อง</p>	<p>๑. ติดตามผลการจัดซื้อระบบคอมพิวเตอร์รวมทั้งการพัฒนา ระบบงานให้เป็นไปตามข้อตกลงที่ได้จากการศึกษาและสำรวจความต้องการ</p> <p>๒. สอบทานความเหมาะสมของกระบวนการพัฒนาระบบงาน/การแก้ไข / การจัดตั้ง/การใช้งาน/การจัดเก็บ และการดูแลรักษา ระบบงาน Hardware และ Software</p> <p>๓. ประเมินความเหมาะสมของวิธีการและ มาตรการในการใช้ทรัพยากรด้าน IT</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
		<p>๕. เครื่องคอมพิวเตอร์และอุปกรณ์ถูกใช้งานอย่างไม่เหมาะสมและไม่ถูกวิธี ทำให้เกิดการเสื่อมสภาพก่อนเวลาอันควร</p> <p>๖. เครื่องคอมพิวเตอร์และอุปกรณ์สูญหาย หรือเกิดการเสียหาย</p> <p>๗. ไม่มีมาตรการหรือแผนรองรับเหตุฉุกเฉินหรือการหยุดชะงักของระบบคอมพิวเตอร์</p>	<p>๗. จัดให้มีคู่มือการใช้เครื่องคอมพิวเตอร์ และอุปกรณ์ที่ถูกวิธี</p> <p>๘. จัดให้มีระบบบำรุงรักษาที่ต่อเนื่องเหมาะสม และครอบคลุมครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ทุกประเภท</p> <p>๙. กำหนดให้มีการจัดทำทะเบียนคุมครุภัณฑ์คอมพิวเตอร์ พร้อมทั้งให้มีการสอบทานการลงทะเบียนคุมเป็นประจำ และจัดให้มีการตรวจนับครุภัณฑ์คอมพิวเตอร์อย่างน้อยปีละ ๑ ครั้ง</p> <p>๑๐. จัดให้มีการประกันภัยครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ที่ใช้กับงานสำคัญๆ</p> <p>๑๑. จัดให้มีแผนรองรับเหตุฉุกเฉินหรือเหตุหยุดชะงักของระบบคอมพิวเตอร์</p> <p>๑๒. มีการซักซ้อมการทำงานภายใต้แผนสำรองหรือระบบทดแทนในส่วนที่เป็นระบบงานสำคัญๆ ของหน่วยงานเป็นครั้งคราว หรือตามความเหมาะสม</p>	<p>๔. ชี้แจงและประชาสัมพันธ์ เกี่ยวกับแผนสำรอง หรือการดำเนินงานภายใต้แผนฉุกเฉินให้กับเจ้าหน้าที่ที่เกี่ยวข้องทราบอย่างทั่วถึง</p>	<p>๔. ประเมินและตรวจสอบความเพียงพอและความทันสมัยของคู่มือการใช้อุปกรณ์คอมพิวเตอร์</p> <p>๕. ประเมินการใช้ประโยชน์จากครุภัณฑ์คอมพิวเตอร์ทุกรายการ</p> <p>๖. ประเมินความเหมาะสมของระบบการประกันภัยครุภัณฑ์คอมพิวเตอร์และอุปกรณ์</p> <p>๗. ประเมินความเหมาะสมของแผนฉุกเฉินหรือระบบทดแทนเป็นครั้งคราวตามความเหมาะสม</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
		<p>๘. การใช้ทรัพยากรด้าน IT เป็นไปอย่างไม่เหมาะสม ทำให้เกิดความสิ้นเปลือง และใช้ประโยชน์อย่างไม่คุ้มค่า</p>	<p>๑๓. จัดให้มีระบบบริหารและตรวจสอบการใช้ทรัพยากรด้าน IT ที่เหมาะสม</p> <p>๑๔. จัดให้มีการอบรมและเสริมสร้างจริยธรรมหรือจิตสำนึกในการปฏิบัติงานให้เจ้าหน้าที่ที่เกี่ยวข้องให้ใช้ทรัพยากรด้าน IT อย่างประหยัดและสมประโยชน์</p>	<p>๕. ชี้แจง ประชาสัมพันธ์ ความรู้ เกี่ยวกับการใช้ ทรัพยากรด้าน IT ที่ถูก วิธีและเหมาะสมให้กับ เจ้าหน้าที่ทุกฝ่ายทราบ</p>	

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
<p>๑.๓. การควบคุมด้านการรักษาความปลอดภัย ของศูนย์คอมพิวเตอร์</p>	<p>มาตรการหรือนโยบายด้านการรักษาความปลอดภัยและการบำรุงรักษา</p>	<p>๑.ระบบรักษาความปลอดภัยของศูนย์คอมพิวเตอร์ไม่เพียงพอไม่รัดกุม ทำให้มีการเข้าออกศูนย์คอมพิวเตอร์โดยไม่ได้รับอนุญาต ๒. ไม่มีมาตรการป้องกันระบบคอมพิวเตอร์และระบบการสื่อสารข้อมูลรวมทั้งเกิดภัยอันตรายอื่นๆ เช่น Virus Computer การจารกรรมข้อมูลหรือการ Hacker ๓. มีการนำ Software จากภายนอกและไม่ได้รับอนุญาตเข้ามาใช้ในหน่วยงาน</p>	<p>๑. จัดให้มีระบบเวรยามหรือมาตรการการรักษาความปลอดภัย รวมทั้งการกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ที่เหมาะสมและรัดกุมและสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบข้อมูล ๒. กำกับดูแลให้มีการปฏิบัติตามมาตรการรักษาความปลอดภัยอย่างเคร่งครัด ๓. กำหนดให้มีการจัดทำทะเบียนคุมการติดตั้งหรือการนำ Software จากภายนอกเข้ามาใช้กับเครื่องคอมพิวเตอร์ในหน่วยงาน</p>	<p>๑. ชี้แจงประชาสัมพันธ์และให้ความรู้เกี่ยวกับระบบรักษาความปลอดภัยและภัยอันตรายต่างๆ หรือความเสียหายจากการใช้คอมพิวเตอร์หรืออุปกรณ์ด้าน IT ที่ไม่เหมาะสม ให้เจ้าหน้าที่ทราบทั่วกัน ๒. เวียนแจ้งมาตรการควบคุมการนำ Software มาจากภายนอกเข้ามาใช้ในหน่วยงาน ให้ทราบทั่วกัน</p>	<p>๑. ประเมินความเหมาะสมของมาตรการรักษาความปลอดภัย ๒. ประเมินสถิติที่เกิดจากการฝ่าฝืนการเข้าออกศูนย์คอมพิวเตอร์และระบบข้อมูลโดยไม่ได้รับอนุญาต ๓. ติดตามการใช้ Software ที่ติดตั้งในเครื่องคอมพิวเตอร์เป็นครั้งคราว ๔. ติดตามหรือสอบทานการปฏิบัติตามมาตรการรักษาความปลอดภัยเป็นครั้งคราว</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
<p>๒. การควบคุมระบบงาน</p> <p>๒.๑ การควบคุมการเข้าถึงระบบงาน เพิ่มข้อมูล และฐานข้อมูล</p>	<p>๑. มาตรการรักษาความปลอดภัยและกำหนดสิทธิในการเข้าถึงระบบงานและระบบข้อมูล</p> <p>๒. ความรู้ความสามารถตลอดจนทักษะในการใช้ Hardware Software และอุปกรณ์การสื่อสารของเจ้าหน้าที่ในศูนย์คอมพิวเตอร์และผู้ใช้</p> <p>๓. จริยธรรมและความซื่อสัตย์ของเจ้าหน้าที่ที่เกี่ยวข้อง</p>	<p>๑. ระบบรักษาความปลอดภัยรวมทั้งการกำหนดสิทธิในการเข้าถึงระบบงานและข้อมูลไม่รัดกุมหรือไม่เพียงพอ</p> <p>๒. ไม่มีการพัฒนาระบบงานให้ทันสมัยอยู่เสมอ</p> <p>๓. ผู้ใช้ (Users) ขาดความรู้ความชำนาญในการใช้เครื่องคอมพิวเตอร์ในการปฏิบัติงานรวมทั้งการใช้ระบบงาน</p>	<p>๑. ให้ผู้มีหน้าที่รับผิดชอบศึกษา ทบทวนระบบรักษาความปลอดภัยและการกำหนดสิทธิในการเข้าถึงระบบงาน และฐานข้อมูลที่สำคัญ</p> <p>๒. ให้มีเจ้าหน้าที่จัดทำทะเบียนคุม USER ID โดยเฉพาะ</p> <p>๓. มีการปรับปรุงพัฒนาระบบและสิทธิหรือ USER ID ในการเข้าถึงระบบงานและระบบข้อมูลเป็นระยะๆ</p> <p>๔. จัดให้มีคู่มือการปฏิบัติงานสำหรับผู้ใช้งาน (Users) ทุกระบบงานอย่างเพียงพอ และจัดฝึกอบรมผู้ใช้อย่างสม่ำเสมอ</p>	<p>๑. สื่อสารและทำความเข้าใจกับเจ้าหน้าที่ทุกฝ่ายของหน่วยงานเกี่ยวกับมาตรการรักษาความปลอดภัย การใช้งานในระบบงาน คอมพิวเตอร์ และการปฏิบัติงานด้าน IT</p> <p>๒. สื่อสารให้เจ้าหน้าที่ที่เกี่ยวข้องทราบถึงการใช้งานระบบงาน</p>	<p>๑. ประเมินความเหมาะสมของระบบรักษาความปลอดภัยและคู่มือการปฏิบัติงานเป็นระยะๆ</p> <p>๒. ประเมินผลการจัดอบรมและประเมินผลเจ้าหน้าที่ผ่านการฝึกอบรม</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
<p>๒.๒. การควบคุมการนำเข้าข้อมูล</p>	<p>๑. ประสิทธิภาพของระบบงานและระบบคอมพิวเตอร์</p> <p>๒. ความรู้และทักษะของเจ้าหน้าที่ที่เกี่ยวข้อง</p> <p>๓. ความพร้อมของเอกสารหรือข้อมูลที่จะนำเข้าสู่ระบบ</p>	<p>๑. บันทึกข้อมูลผิดพลาดไม่ครบถ้วน ไม่ถูกต้อง</p> <p>๒. ข้อมูลที่บันทึกเข้าระบบไม่ได้รับการตรวจทาน หรือสอบทานความถูกต้องก่อนการส่งต่อ</p>	<p>จัดให้มีการตรวจสอบข้อมูลหรือเข้าทั้งจัดให้มีรายงานจากโปนแกรมระบบงานสำหรับการตรวจสอบ หรือสอบทานความถูกต้องของข้อมูลก่อนการส่งต่อ</p>	<p>เวียนแจ้งให้เจ้าหน้าที่เกี่ยวข้องทราบถึงมาตรการหรือวิธีการนำเข้าข้อมูล</p>	<p>ประเมินความเหมาะสมของมาตรการการนำเข้าข้อมูลเป็นครั้งคราว</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
<p>๒.๓. การควบคุมด้านการประมวลผลเพื่อจัดทำข้อมูลสารสนเทศและรายงาน</p>	<p>๑. ความต้องการใช้ข้อมูลและสารสนเทศของฝ่ายบริหารและหน่วยงานที่เกี่ยวข้อง</p> <p>๒. แผนการปฏิบัติงานในห้องเครื่องคอมพิวเตอร์</p> <p>๓. ความรู้และทักษะของเจ้าหน้าที่ที่เกี่ยวข้อง</p> <p>๔. จริยธรรม และความซื่อสัตย์ของผู้นำข้อมูลเข้าระบบ</p>	<p>๑. ข้อมูลและรายงานที่ได้จากการประมวลผลไม่ตรงตามความต้องการ หรือไม่ทันกับความต้องการของผู้ที่เกี่ยวข้อง</p> <p>๒. ไม่มีการวางแผนเกี่ยวกับความต้องการใช้ข้อมูลและรายงานของผู้ที่เกี่ยวข้อง</p> <p>๓. ไม่มีการจัดทำแผนหรือตารางการปฏิบัติงานของเจ้าหน้าที่เครื่องคอมพิวเตอร์</p> <p>๔. เจ้าหน้าที่ขาดความรู้และขาดทักษะในการใช้ระบบคอมพิวเตอร์คำสั่งในการประมวลผล</p> <p>๕. เจ้าหน้าที่นำข้อมูลไปใช้เพื่อประโยชน์ส่วนตัว</p>	<p>๑. ศึกษาความต้องการของผู้ใช้หรือผู้ที่เกี่ยวข้องทุกฝ่ายเพื่อวางแผนล่วงหน้าในการจัดทำข้อมูลและรายงานให้ทันกับความต้องการ</p> <p>๒. จัดให้มีตารางการปฏิบัติงานรวมทั้งใบสั่งงานหรือเอกสารการส่งมอบงานสำหรับเจ้าหน้าที่ทำหน้าที่ประมวลผลและจัดทำตารางการส่งงานให้ชัดเจนเพื่อให้ข้อมูลและรายงานส่งถึงมือผู้ใช้ในเวลาที่เหมาะสม</p> <p>๓. มีการจัดระบบความคุ้มครองรับส่งการแลกเปลี่ยนและการสื่อสารข้อมูลหรือรายงานให้ถึงมือผู้ใช้อย่างเป็นระบบครอบคลุมและทันเวลาและมีการสื่อสารเพื่อให้ได้ข้อมูลย้อนกลับจากผู้ใช้</p> <p>๔. จัดให้มีการฝึกอบรมอย่างต่อเนื่องและให้มีการจัดทำคู่มือปฏิบัติงานในเรื่องต่าง ๆ ที่เกี่ยวข้อง</p> <p>๕. จัดอบรมแก่เจ้าหน้าที่ให้มีความเข้าใจเรื่อง Conflict of interest(ความขัดแย้งเกี่ยวกับผลประโยชน์)</p>	<p>เผยแพร่คู่มือหรือหลักเกณฑ์การปฏิบัติงานด้วยเครื่องคอมพิวเตอร์ให้ผู้ใช้ที่เกี่ยวข้องทราบทั่วกัน</p>	<p>๑. ประเมินผลการใช้ประโยชน์จากข้อมูลสารสนเทศและรายงาน</p> <p>๒. ประเมินความเหมาะสมของหลักเกณฑ์หรือมาตรการเกี่ยวกับการประมวลผล</p> <p>๓. ประเมินความเหมาะสมของการปฏิบัติงานและตารางการส่งมอบงาน</p> <p>๔. ประเมินความเหมาะสมของการจัดฝึกอบรมเจ้าหน้าที่ทำหน้าที่ประมวลผลเป็นครั้งคราว</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
<p>๒.๔. การควบคุมด้านการรับ – ส่งข้อมูล ระหว่างระบบงานและระหว่างหน่วยงาน</p>	<p>มาตรการหรือระเบียบวิธีการในการรับส่งข้อมูลและการสื่อสารข้อมูลในหน่วยงาน และนโยบายในการรักษาความลับของข้อมูล</p>	<p>๑. ข้อมูลหรือรายงานที่เป็นความลับของหน่วยงานถูกนำไปเผยแพร่ หรือนำไปใช้ประโยชน์โดยไม่ได้รับอนุญาต ๒. การส่งต่อข้อมูลไม่เป็นไปตามกำหนดเวลา</p>	<p>๑. กำหนดหลักเกณฑ์และมาตรการในการนำข้อมูลหรือรายงานออกนอกสถานที่ หรือออกจากศูนย์คอมพิวเตอร์ ๒. จัดให้มีระบบควบคุมการรับส่งข้อมูล หรือการส่งต่อข้อมูลระหว่างระบบงาน</p>	<p>เวียนแจ้งมาตรการรักษาความลับของข้อมูลและรายงานให้เจ้าหน้าที่ที่เกี่ยวข้องทราบทั่วกันรวมทั้งชี้แจงทำความเข้าใจเกี่ยวกับเวลาและกระบวนการในการส่งมอบงานในแต่ละขั้นตอน</p>	<p>ประเมินความเหมาะสมของระบบรักษาความปลอดภัยของข้อมูลและรายงาน รวมทั้งการกำหนดสิทธิในการเข้าถึงระบบงานและระบบข้อมูลอย่างสม่ำเสมอ</p>

แนวปฏิบัติการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (IT)

ขั้นตอนการดำเนินงาน	สภาพแวดล้อมการควบคุม	ปัจจัยเสี่ยง	กิจกรรมการควบคุม	สารสนเทศและการสื่อสาร	การติดตามและประเมินผล
<p>๒.๕. การควบคุมดูแลรักษาระบบงาน เพิ่มและฐานข้อมูล</p>	<p>ระบบจัดเก็บและรักษาข้อมูล</p>	<p>๑. ระบบจัดเก็บเพิ่มข้อมูล ฐานข้อมูล และรายงาน ต่างๆไม่ดี หรือไม่เหมาะสม ๒. สื่อหรือ MEDIA ที่ใช้ในการสำรองข้อมูลไม่มีคุณภาพ</p>	<p>๑. กำหนดระบบการจัดเก็บ และสำรองเพิ่มข้อมูล ฐานข้อมูล และรายงานต่างๆ ให้เหมาะสมกับการใช้งาน ๒. จัดให้มีการสำรองข้อมูลให้ครบถ้วนตามความเหมาะสมของแต่ละระบบงาน และตามเวลาที่กำหนด ๓. จัดให้มีการทดสอบความถูกต้องของข้อมูลที่สำรองไว้เป็นครั้งคราวและทำรายงานผลการทดสอบ</p>	<p>ประชาสัมพันธ์และชี้แจงมาตรการในการดูแลและเก็บรักษา ระบบงาน ระบบข้อมูล ให้เจ้าหน้าที่ที่เกี่ยวข้องทราบ</p>	<p>ประเมินความเหมาะสมของระบบจัดเก็บและสำรองเพิ่มข้อมูล ฐานข้อมูลและรายงาน</p>

