(ร่าง)

ระเบียบปฏิบัติด้านความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ

สำนักงานปลัดกระทรวงสาธารณสุข

สารบัญ

ระเบียบปฏิบัติสำหรับการบริหารจัดการ
ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

ระเบียบปฏิบัติสำหรับการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
ผู้รับผิดชอบ : คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1.	จัดให้มีการทำ และปรับปรุงนโยบายด้านความมั่นคงปลอดภัยอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง	ตรวจสอบการปรับปรุงนโยบายตามระเบียบนี้	มีการพิจารณาเพื่อปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง (โดยที่นโยบายอาจจะมีการปรับปรุงหรือไม่ก็ตาม)
2.	แสดงเจตนารมณ์ หรือสื่อสารให้เจ้าหน้าที่ทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยขององค์กรโดยเคร่งครัด อย่างสม่ำเสมอ	-ตรวจสอบการสั่งการให้มีการปรับปรุงนโยบายด้านความมั่นคงปลอดภัย -ตรวจสอบการสั่งการให้มีการตรวจสอบการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัย -ตรวจสอบการแจ้งเวียนเกี่ยวกับนโยบายด้านความมั่นคงฯ ที่ได้มีการปรับปรุงใหม่	-มีการพิจารณาเพื่อปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง -มีการตรวจสอบการปฏิบัติตามนโยบายด้านความมั่นคงอย่างน้อยปีละ 1 ครั้ง -มีการสื่อสาร แจ้งเวียน หรือแถลงนโยบายด้านความมั่นคงที่ปรับปรุงใหม่ โดยผู้บริหารฯ
3.	จัดให้มีการประชุมเกี่ยวกับการบริหารจัดการด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง โดยกำหนดให้มีวาระการประชุมที่ต้องหารือกันอย่างน้อยดังนี้ - การตรวจสอบการปฏิบัติตามนโยบายความมั่นคงฯ และผลการตรวจสอบ - แผนการดำเนินการเชิงป้องกัน/แก้ไข จากผลการตรวจสอบดังกล่าว - การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป - การประเมินความเสี่ยงและแผนลดความเสี่ยง รวมทั้งจัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่เพียงพอต่อการจัดการดังกล่าว	ตรวจสอบรายงานการประชุมของคณะกรรมการบริหารฯ เกี่ยวกับการจัดการด้านความมั่นคงปลอดภัย	รายงานการประชุมของคณะกรรมการเกี่ยวกับการจัดการด้านความมั่นคงปลอดภัย ต้องมีวาระการประชุมครบตามที่กำหนดไว้ รวมทั้งมีการจัดสรรทรัพยากรที่เพียงพอต่อการดำเนินการ
4.	จัดให้มีการสร้างความตระหนักทางด้านความมั่นคงปลอดภัยเพื่อให้เจ้าหน้าที่ขององค์กร มีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ในเบื้องต้น อย่างน้อยปีละ 1 ครั้ง	-ตรวจสอบเรื่องการสร้างความตระหนักด้านความมั่นคงปลอดภัยสำหรับเจ้าหน้าที่ขององค์กร เช่นการเชิญผู้เชี่ยวชาญภายจากองค์กรต่างๆ มาให้ความรู้เกี่ยวกับความ	-มีการจัดอบรมเพื่อสร้างความตระหนักหรือ -มีการเชิญผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจากภายนอกมาให้ความรู้กับเจ้าหน้าที่ทั้งหมด

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
		มั่นคงปลอดภัย หรือในฟอรัม KM อาจจัดให้มีการให้ความรู้ดังกล่าว	
5.	จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อลดความเสี่ยง หรือปัญหาที่พบ	ตรวจสอบแผนการประเมินและลดความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ	แผนดังกล่าวได้รับการปฏิบัติ โดยมีผลการดำเนินการเป็นลายลักษณ์อักษร
6.	จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัย โดยผู้ตรวจสอบภายในด้านสารสนเทศ ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุง หรือแก้ไขปัญหาที่พบ	-ตรวจสอบผลการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงโดยทีมผู้ตรวจสอบภายใน -ตรวจสอบผลการตรวจโดยสรุปและแผนการปรับปรุงหรือแก้ไขปัญหาที่พบ	-มีผลการตรวจสอบการปฏิบัติตามนโยบายฯ -มีผลการตรวจโดยสรุปและแผนการปรับปรุงหรือแก้ไขปัญหาที่พบ
7.	จัดให้มีการแจ้งเวียนให้เจ้าหน้าที่ทั้งหมดได้ระมัดระวัง และดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน เพื่อป้องกันการสูญหาย อย่างน้อยปีละ 1 ครั้ง	ตรวจสอบหนังสือแจ้งเวียนเพื่อให้เจ้าหน้าที่ได้ระมัดระวังทรัพย์สินขององค์กร	มีหนังสือแจ้งเวียนดังกล่าว
8.	กำหนดนโยบายการใช้งานระบบเครือข่ายอย่างชัดเจนว่าบริการใดที่อนุญาตให้ใช้งาน และบริการใดไม่อนุญาตให้ใช้งาน เช่น การใช้งาน MSN ดูหนังฟังเพลงผ่านทางอินเตอร์เน็ต เป็นต้น รวมทั้งปรับปรุงนโยบายตามความจำเป็น **นโยบายการใช้งานระบบเครือข่าย** ขณะนี้ประกอบด้วย ▪ ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้ - การพนัน - วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และพระมหากษัตริย์ - ลามก อนาจาร - อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม ▪ ห้ามเล่นเกมส์ ดูภาพยนต์ หรือฟังเพลง ผ่านทางอินเทอร์เน็ตในเวลาทำงาน	ตรวจสอบการกำหนดหรือปรับปรุงนโยบายการใช้งานระบบเครือข่าย	มีการกำหนดหรือปรับปรุงนโยบายการใช้งานระบบเครือข่าย

ระเบียบปฏิบัติสำหรับการบริหารจัดการคอมพิวเตอร์และระบบเครือข่าย

ระเบียบปฏิบัติสำหรับการจัดการกับเอกสารที่เกี่ยวข้องกับระบบ

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย และ/หรือ ผู้พัฒนาระบบ

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	จัดทำ และ ปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย รวมทั้งให้จัดเก็บไว้ในสถานที่ที่มีความปลอดภัยอย่างน้อย ให้ครอบคลุมระบบงาน เครื่องเซิร์ฟเวอร์ และอุปกรณ์ที่มีความสำคัญ ดังนี้ o คู่มือระบบงานต่างๆ ทั้งในส่วนของผู้ใช้งานและผู้ดูแลระบบ o คู่มือการตรวจสอบสถานะของเซิร์ฟเวอร์ และระบบเครือข่าย o คู่มือการตรวจสอบระบบและอุปกรณ์ต่างๆ ในห้องเครื่อง o คู่มือการสำรองข้อมูล o คู่มือการตรวจสอบทรัพยากรของระบบ	ตรวจสอบการปรับปรุงคู่มือครั้งล่าสุด	คู่มือได้รับการปรับปรุงเนื้อหา วันและเวลาให้ทันสมัย
2	ให้จำกัดการเข้าถึงคู่มือการปฏิบัติงานเฉพาะทีมงานที่มีความเกี่ยวข้องเท่านั้น	ตรวจสอบว่ามีการจำกัดการเข้าถึงคู่มืออย่างไร	คู่มือได้รับการจัดเก็บเป็นอย่างดี
3	หากมีการจัดเก็บคู่มือการปฏิบัติงานไว้บนระบบเครือข่าย จัดให้มีการป้องกันการเข้าถึงเพื่อให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น	ตรวจสอบว่ามีการจำกัดการเข้าถึงคู่มือในระบบเครือข่ายอย่างไร	-มีการกำหนดสิทธิโดยกำหนดให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้ -บัญชีรายชื่อผู้มีสิทธิเข้าถึงคู่มือในระบบเครือข่าย

ระเบียบปฏิบัติสำหรับการจัดการระบบเครือข่าย

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	ปรับปรุงผังเครือข่ายให้มีความทันสมัย อย่างน้อยปีละ 1 ครั้ง	ตรวจสอบการปรับปรุงผังเครือข่ายครั้งล่าสุด	ผังเครือข่ายได้รับการปรับปรุงเนื้อหา วันและเวลาให้ทันสมัย
2	จัดแบ่ง และปรับปรุงระบบเครือข่ายออกเป็นกลุ่ม ๆ ตามลักษณะการใช้งาน เช่น แบ่งตามกลุ่มเครื่องเซิร์ฟเวอร์ เครื่องลูกข่าย และ ระบบงานที่มีความสำคัญ	ตรวจสอบการจัดแบ่งเครือข่ายตามความจำเป็นในการเข้าถึงข้อมูลของกอง/ฝ่าย/งาน	ผังเครือข่ายที่มีการแบ่งตามกลุ่มของผู้ใช้งาน เช่น แบ่งตามกอง/ฝ่าย/งาน
3	จำกัดการเชื่อมต่อไปยังเครื่องเซิร์ฟเวอร์ ระบบงาน หรืออุปกรณ์ที่มีความสำคัญ โดยจะต้องกำหนดให้เครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่อได้จะต้องเป็นเครื่องที่มาจากเครื่องของผู้ดูแลระบบเท่านั้น	ตรวจสอบการเชื่อมต่อไปยังเครื่องเซิร์ฟเวอร์ หรือระบบงานเหล่านั้น	เครื่องของผู้ใช้งานต้องไม่สามารถเชื่อมต่อไปยังเซิร์ฟเวอร์สำคัญเหล่านั้น
4	ปิดบริการบนเครื่องเซิร์ฟเวอร์ที่ไม่มีความจำเป็นในการใช้งาน	ตรวจสอบการเปิดบริการบนเครื่องเซิร์ฟเวอร์เหล่านั้น	-บัญชีรายชื่อของบริการ (หรือพอร์ต) ที่จำเป็นต้องเปิดให้บริการบนเครื่องเซิร์ฟเวอร์ -เครื่องเซิร์ฟเวอร์ต้องไม่เปิดบริการที่ไม่จำเป็นทิ้งไว้
5	กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลที่ใช้สำหรับการเชื่อมต่อจาก<u>ภายใน</u>เครือข่ายเพื่อเข้าสู่เครื่องเซิร์ฟเวอร์ หรืออุปกรณ์เครือข่าย (กรมต้องกำหนดโปรแกรมนี้ขึ้นมา และ ใช้เป็นมาตรฐานเดียวกันในการเชื่อมต่อไปยังเครื่องเซิร์ฟเวอร์ หรืออุปกรณ์เครือข่าย)	ตรวจสอบรายชื่อโปรแกรมมาตรฐานสำหรับการเชื่อมต่อภายใน	มีรายชื่อโปรแกรมมาตรฐานที่ใช้สำหรับการเชื่อมต่อภายใน
6	กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลที่ใช้สำหรับการเชื่อมต่อ<u>จากระยะไกล</u>ภายนอกองค์กรเข้ามาสู่เครือข่ายภายในองค์กร (กรมต้องกำหนดโปรแกรมนี้ขึ้นมา และใช้เป็นมาตรฐานเดียวกันในการเชื่อมต่อจากภายนอกเข้ามา)	ตรวจสอบรายชื่อโปรแกรมมาตรฐานสำหรับการเชื่อมต่อจากภายนอกองค์กร	มีรายชื่อโปรแกรมมาตรฐานที่ใช้สำหรับการเชื่อมต่อจากภายนอก
7	ติดตั้ง Patch แบบอัตโนมัติ บนเครื่องคอมพิวเตอร์ส่วนบุคคลของผู้ใช้งานทั้งหมดขององค์กร	ตรวจสอบการตั้งค่า Patch บนเครื่องคอมพิวเตอร์ส่วนบุคคล	เครื่องคอมพิวเตอร์ส่วนบุคคลได้รับการตั้งค่าให้ดำเนินการ Patch แบบอัตโนมัติ
8	ปรับแต่งไฟร์วอลล์เพื่อให้เป็นไปตาม**นโยบายการใช้งานระบบเครือข่าย**ที่ผู้บริหารได้กำหนดไว้	ตรวจสอบการปรับแต่งไฟร์วอลล์ตามนโยบายดังกล่าว	มีการกำหนดกฎในไฟร์วอลล์เพื่อให้สอดคล้องกับนโยบายดังกล่าว

ระเบียบปฏิบัติสำหรับการจัดการการลาออกหรือย้ายหน่วยงานของเจ้าหน้าที่

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	ถอดถอนสิทธิของผู้ที่ลาออกหรือย้ายหน่วยงานออกจากระบบต่างๆ ทั้งหมดโดยทันทีที่ได้รับแจ้งจากกองการเจ้าหน้าที่	ตรวจสอบรายชื่อผู้ลาออกหรือย้ายหน่วยงานในปีนั้นและดูว่าได้มีการถอดถอนสิทธิแล้วหรือไม่	- มีการบันทึกข้อมูลการลาออกหรือย้ายหน่วยงานลงในแบบฟอร์มบันทึกข้อมูลผู้ลาออกหรือย้ายหน่วยงาน - มีการตรวจสอบสภาพคอมพิวเตอร์ที่อยู่ในความครอบครองของผู้ที่ลาออกว่ายังอยู่ในสภาพที่ใช้งานได้หรือไม่ และบันทึกผลการตรวจสภาพเครื่องลงในแบบฟอร์มดังกล่าว

ระเบียบปฏิบัติสำหรับการใช้งานห้องเครื่อง

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	ห้ามนำบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น	สังเกตการณ์เพื่อดูว่ามีคนนอกเข้ามาในห้องเครื่องโดยมีกิจที่ต้องทำหรือไม่ โดยปกติบุคคลเหล่านั้นต้องลงชื่อไว้พร้อมกิจที่ต้องการปฏิบัติ	สมุดบันทึกลงนามบุคคลภายนอก วันเวลาการเข้า และกิจที่ต้องการปฏิบัติ
2	ห้ามใส่รองเท้าเข้าห้องเครื่อง	สังเกตการณ์เพื่อดูว่ามีการใส่รองเท้าเข้าไปในห้องเครื่องหรือไม่	ไม่สังเกตพบว่ามีการใส่รองเท้าเข้าไปในห้องเครื่อง
3	ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้องเครื่อง	สังเกตการณ์เพื่อดูว่ามีการนำอาหารหรือเครื่องดื่มเข้าไปในห้องเครื่องหรือไม่	ไม่สังเกตพบว่ามีการนำอาหารหรือเครื่องดื่มเข้าไปในห้องเครื่อง
4	ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องให้ปิดล็อคอยู่เสมอ	สังเกตการณ์เพื่อดูว่ามีการล็อกประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องหรือไม่	ไม่สังเกตพบว่ามีการเปิดประตูทางเข้า-ออก และหน้าต่างทิ้งไว้
5	ตรวจสอบสภาพการทำงานของอุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ ได้แก่ ▪ ระบบกระแสไฟฟ้า ▪ ระบบการควบคุมความชื้น ▪ ระบบการระบายอากาศ	ตรวจสอบว่ามีการลงบันทึกการตรวจสอบระบบดังกล่าวหรือไม่	มีการลงบันทึกการตรวจสอบอุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ดังกล่าวทุกวัน

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
	▪ ระบบการปรับอุณหภูมิ ▪ ระบบกระแสไฟฟ้าสำรอง ▪ ระบบ UPS ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ อย่างน้อยวันละ 1 ครั้ง ยกเว้นการตรวจสอบระบบกระแสไฟฟ้าสำรอง ให้ตรวจสอบเดือนละ 1 ครั้ง		
6	จัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือทรัพย์สินอื่นๆ ไว้ในบริเวณที่มีความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย	ตรวจสอบการจัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ในห้องเครื่อง	ไม่พบว่ามีเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่จัดวางอยู่ในสภาพที่เสี่ยงต่อการล้มหรือเสียหาย
7	ติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพิ่มเติมตามความจำเป็น เช่น ในกรณีที่เป็นมุมอับ รวมทั้งตรวจสอบการทำงานของกล้องให้มีการทำงานอย่างถูกต้อง ต่อเนื่องและให้สามารถเก็บภาพได้ในมุมกว้าง และไม่มีสิ่งกีดขวาง โดยบันทึกภาพล่าสุดไว้อย่างน้อย 1 เดือน	ตรวจสอบตำแหน่งติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อให้ครอบคลุมพื้นที่โดยรอบ	- มีการติดตั้งกล้องโทรทัศน์วงจรปิดอย่างเพียงพอ - มีการเก็บภาพบันทึกไว้ในสื่อบันทึกข้อมูลไว้อย่างน้อย 1 เดือน
8	ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยปีละ 1 ครั้ง ว่ายังใช้งานได้เป็นปกติ หรือไม่	- ตรวจสอบจากป้ายที่ติดอยู่บนอุปกรณ์ดับเพลิงว่ามีการตรวจสอบครั้งล่าสุดเมื่อใด - ตรวจสอบแรงดันในถังดับเพลิง	-พบว่าป้ายได้รับการปรับปรุงตามวันและเวลาที่ตรวจสอบล่าสุด -เข็มหน้าปัทม์แสดงแรงดันในถังดับเพลิงจะต้องแสดงว่ามีแรงดันอย่างเพียงพอ
9	ให้ดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องเครื่องอย่างสม่ำเสมอ ต้องไม่เก็บกล่องกระดาษหรือสิ่งที่จะเป็นเชื้อเพลิงไว้ในห้องเครื่อง	ตรวจสอบความสะอาดและเป็นระเบียบเรียบร้อยรวมทั้งการไม่เก็บกล่องกระดาษต่างๆ ไว้ในห้องเครื่อง	ไม่พบว่าห้องเครื่องมีการเก็บกล่องกระดาษต่างๆ และห้องเครื่องมีความสะอาดและเป็นระเบียบเรียบร้อย
10	ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย	ตรวจสอบการจัดเก็บสายสัญญาณสื่อสารว่าอยู่ในสภาพเรียบร้อยหรือไม่	ไม่พบการเดินสายสัญญาณที่เกะกะขวางทางหรือรกรุงรัง
11	ตรวจสอบห้องสายสัญญาณสื่อสารให้มีการปิดล็อกอยู่เสมอ	สังเกตการณ์เพื่อดูว่ามีการล็อกประตูทางเข้า-ออกของห้องสายสัญญาณสื่อสารหรือไม่	ไม่สังเกตพบว่ามีการเปิดประตูทางเข้า-ออกทิ้งไว้
12	จัดทำหรือต่อสัญญาการบำรุงรักษาระบบงานสำคัญ ไฟร์วอลล์ เราท์เตอร์ อุปกรณ์ UPS สำหรับระบบงานสำคัญ และเครื่องปรับอากาศในห้องเครื่อง ให้ครบถ้วน	ตรวจสอบว่าระบบเหล่านั้นได้รับการต่อสัญญาการบำรุงรักษาอย่างครบถ้วนหรือไม่	สัญญาการบำรุงรักษาระบบเหล่านั้นมีการต่อสัญญาสำหรับปีปัจจุบัน

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
13	จัดให้ระบบงานสำคัญ เครื่องเซิร์ฟเวอร์ และอุปกรณ์ที่มีความสำคัญต้องมีอุปกรณ์ UPS และระบบกระแสไฟฟ้าสำรอง (electricity power generator) เพื่อสนับสนุนการทำงานอย่างครบถ้วน	ตรวจสอบว่ามีระบบกระแสไฟฟ้าสำรองจ่ายให้กับระบบเหล่านั้นครบถ้วนหรือไม่	-ในกรณีที่มีระบบงานใหม่เกิดขึ้นต้องพบว่าได้มีการหารือเรื่องการคำนวณโหลดการจ่ายกระแสไฟฟ้าสำรองเพิ่มเติมสำหรับระบบงานใหม่ที่เกิดขึ้น -แผนการเตรียมอุปกรณ์ UPS และระบบกระแสไฟฟ้าสำรองให้เพียงพอกับระบบทั้งหมดเหล่านั้น

ระเบียบปฏิบัติสำหรับการจัดการทรัพยากรของเครื่องเซิร์ฟเวอร์

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1.	ดำเนินการตรวจสอบทรัพยากรของเซิร์ฟเวอร์สำหรับระบบงานสำคัญอย่างน้อยสัปดาห์ละ 1 ครั้ง สิ่งที่ควรตรวจสอบ ประกอบด้วย ปริมาณการใช้ CPU ปริมาณการใช้ฮาร์ดดิสก์ ปริมาณการใช้หน่วยความจำ และปริมาณการใช้เครือข่าย รวมทั้งควรมีการตรวจสอบการใช้งานเครือข่ายโดยภาพรวม (เช่น โดยการใช้โปรแกรม MRTG)	ตรวจสอบว่าทรัพยากรของเซิร์ฟเวอร์สำหรับระบบงานยังมีเพียงพอต่อการใช้งาน (กรมต้องกำหนดปริมาณการใช้ทรัพยากรมากที่สุด (threshold) สำหรับระบบงานเหล่านั้น ซึ่งไม่ควรสูงกว่าร้อยละ 80)	- แบบฟอร์มบันทึกผลการตรวจสอบการใช้ทรัพยากรของเซิร์ฟเวอร์สำหรับระบบงาน โดยให้พิจารณาเทียบกับปริมาณการใช้ทรัพยากรมากที่สุดสำหรับเซิร์ฟเวอร์ (Threshold)
2.	บันทึกข้อมูลการใช้ทรัพยากรดังกล่าวไว้ด้วย (เพื่อใช้ในการตรวจสอบแนวโน้มการใช้ทรัพยากร รวมทั้งวางแผนจัดซื้อเพิ่มเติมตามความจำเป็นในอนาคต)	ตรวจสอบว่ามีการบันทึกข้อมูลทรัพยากรระบบในทุกสัปดาห์หรือไม่	มีการบันทึกข้อมูลลงในแบบฟอร์มบันทึกผลการตรวจสอบการใช้ทรัพยากรของระบบในทุกสัปดาห์
3.	ตั้งและหมั่นตรวจสอบสัญญาณนาฬิกาของเครื่องเซิร์ฟเวอร์ตามที่ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ระบุไว้ และของระบบงานสำคัญให้มีความถูกต้องอยู่เสมอ (โดยสามารถอ้างอิงเวลาได้จาก "clock.thaicert.org")	ตรวจสอบว่าสัญญาณนาฬิกาของเครื่องเหล่านั้นได้รับการตั้งให้ตรงหรือไม่	ไม่พบว่ามีเครื่องเซิร์ฟเวอร์ที่สัญญาณนาฬิกาผิดเพี้ยน โดยสามารถตรวจสอบเวลาปัจจุบันได้จาก - สถาบันมาตรวิทยาแห่งชาติ (203.185.69.60) - กรมอุทกศาสตร์ กองทัพเรือ (time.navy.mi.th) - National Institute of Standards and Technology, US. (time.nist.gov) - ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (clock.thaicert.nectec.or.th หรือ clock.thaicert.org) แหล่งเอกสารอ้างอิง: www.etcommission.go.th/documents/standard/time_sync_server_v1_0.pdf

ระเบียบปฏิบัติสำหรับการจัดการไวรัส

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1.	ตรวจสอบว่าเครื่องเซิร์ฟเวอร์ป้องกันไวรัสยังทำงานตามปกติ และมีการปรับปรุงฐานข้อมูลไวรัส (Virus signature) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบดำเนินการแก้ไข (ข้อนี้จะใช้ได้กับองค์กรที่มีการใช้งานโปรแกรมป้องกันไวรัสแบบ Client/Server เท่านั้น)	ตรวจสอบการปรับปรุงฐานข้อมูลไวรัสจากเมนูการใช้งานของโปรแกรมป้องกันไวรัสบนเซิร์ฟเวอร์นั้น	หน้าจอแสดงผลการปรับปรุงฐานข้อมูลครั้งล่าสุด (ภายหลังจากเลือกเมนูนั้น)
2.	ทำการติดตั้งโปรแกรมป้องกันไวรัสให้กับผู้ใช้งานเพื่อให้ทำงานในลักษณะทันทีทันใด (Real-time Scan) เมื่อมีการเปิดไฟล์ขึ้นมาใช้งาน	ตรวจสอบการตั้งค่าของโปรแกรมป้องกันไวรัสบนเครื่องของผู้ใช้งาน เพื่อให้โปรแกรมทำการตรวจสอบไวรัสได้อย่างทันทีทันใดเมื่อมีการเปิดไฟล์ขึ้นมาใช้งาน	หน้าจอแสดงการตั้งค่าอย่างถูกต้องของโปรแกรมป้องกันไวรัสบนเครื่องผู้ใช้งาน
3.	ทำการติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยกับเครื่องลูกข่ายทั้งหมด เครื่องเซิร์ฟเวอร์สำหรับระบบงานสำคัญ และเครื่องเมล์เซิร์ฟเวอร์	ตรวจสอบการติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสบนระบบสำคัญเหล่านั้นให้ครบถ้วน	ไม่พบว่ามีระบบสำคัญที่ไม่ได้รับการติดตั้งหรือปรับปรุงโปรแกรมป้องกันไวรัส

แนวทางปฏิบัติสำหรับการสำรองข้อมูล

ผู้รับผิดชอบ : ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และ ผู้พัฒนาระบบ และ ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	กำหนดรายชื่อของระบบงานสำคัญทั้งหมด และเมล์เซิร์ฟเวอร์	ตรวจสอบว่าการสำรองข้อมูลครอบคลุมถึงระบบเหล่านั้นอย่างครบถ้วนหรือไม่	- มีแผนการสำรองข้อมูล ซึ่งประกอบด้วย -ชื่อของระบบ -ชนิดของข้อมูล -ตำแหน่งหรือชื่อผู้รับผิดชอบในการสำรอง -ความถี่ในการสำรองข้อมูล -ประเภทของการสำรองข้อมูล (full, differential, incremental backup) -สถานที่เก็บ (รวมถึงการเก็บไว้นอกสถานที่ด้วย) - มีแบบฟอร์มบันทึกการสำรองข้อมูลตามแผนการสำรองข้อมูล แบบฟอร์มควรประกอบด้วย -ชื่อของระบบ -ชนิดของข้อมูล -ตำแหน่งหรือชื่อผู้ดำเนินการสำรอง -วัน เวลาที่สำรองข้อมูล เช่น วัน/เวลาที่เริ่มต้น และสิ้นสุด -ประเภทของการสำรองข้อมูล (full, differential, incremental backup) -สถานที่เก็บ (รวมถึงการเก็บไว้นอกสถานที่ด้วย) -ผลการสำรองข้อมูล (สำเร็จ/ไม่สำเร็จ) -การแก้ไขในกรณีที่ไม่สำเร็จ
2	กำหนดรายชื่อของเซิร์ฟเวอร์ตามที่ พ.ร.บ.ฯ ได้กำหนดไว้ เช่น เว็บเซิร์ฟเวอร์ เป็นต้น	ตรวจสอบว่าการสำรองข้อมูลครอบคลุมถึงระบบเหล่านั้นอย่างครบถ้วนหรือไม่	หลักฐานเช่นเดียวกับข้อ 1
3	กำหนดผู้รับผิดชอบในการสำรองข้อมูล	ตรวจสอบชื่อผู้รับผิดชอบในการสำรองข้อมูลตามแผนการสำรองข้อมูล	ดูในแผนการสำรองข้อมูลและแบบฟอร์มจากข้อข้างต้น

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
4	กำหนดชนิดของข้อมูลบนระบบงานหรือบนเซิร์ฟเวอร์ดังกล่าวที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วย ▪ ข้อมูลในฐานข้อมูลของระบบงาน ▪ ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น ▪ ข้อมูลอีเมล์	ตรวจสอบชนิดของข้อมูลที่ได้รับการสำรองไปเก็บไว้ ตามแผนการสำรองข้อมูล	ดูในแผนการสำรองข้อมูลและแบบฟอร์มจากข้อข้างต้น
5	กำหนดความถี่ในการสำรองข้อมูลของระบบงานหรือเซิร์ฟเวอร์ดังกล่าว	ตรวจสอบความถี่ในการสำรองข้อมูลตามแผนการสำรองข้อมูล	ดูในแผนการสำรองข้อมูลและแบบฟอร์มจากข้อข้างต้น
6	ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย 1 ชุด	ตรวจสอบการนำข้อมูลสำรองไปเก็บไว้นอกสถานที่	ดูในแผนการสำรองข้อมูลและแบบฟอร์มจากข้อข้างต้น

ระเบียบปฏิบัติในการจัดเก็บข้อมูลล็อกตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	จัดเก็บข้อมูลล็อกดังต่อไปนี้ เครื่องเซิร์ฟเวอร์ FTP (FTP.log), Mail (SMTP.log), Firewall/Proxy/Gateway (เช่น FW.log), Web (Access.log), RADIUS (RADIUS.log) หรือ TACACS+ (TACACS.log) อย่างน้อยเป็นระยะเวลา 90 วัน	ตรวจสอบวันที่เริ่มต้นจัดเก็บข้อมูลล็อกและวันที่ปัจจุบัน ว่าอย่างน้อยเป็นระยะเวลา 90 วัน	ตรวจสอบวัน เวลาที่เริ่มต้นจัดเก็บและวันที่ปัจจุบัน
2	จำกัดการเข้าถึงข้อมูลล็อกดังกล่าวโดยกำหนดให้เฉพาะผู้ดูแลระบบเครือข่ายเท่านั้นที่สามารถเข้าถึงได้	ตรวจสอบสิทธิการเข้าถึงข้อมูลล็อกตามกลุ่มผู้มีสิทธิ	-บัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลล็อก -ไม่พบว่ามีผู้อื่นที่สามารถเข้าถึงข้อมูลล็อกได้

ระเบียบปฏิบัติในการลงทะเบียนและควบคุมการเข้าถึงระบบ

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย และ ผู้พัฒนาระบบงาน

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	กำหนดให้มีการลงทะเบียนสำหรับผู้ใช้งานใหม่ตาม "**แบบฟอร์มสำหรับลงทะเบียนผู้ใช้งาน**" และกำหนดสิทธิของผู้ใช้งานตามที่ระบุไว้ในแบบฟอร์มฯ แต่ควรให้สิทธิความจำเป็นในการใช้งานเท่านั้น	ตรวจสอบความสอดคล้องระหว่างแบบฟอร์มลงทะเบียนกับบัญชีผู้ใช้งานของระบบ	บัญชีผู้ใช้งานในระบบสอดคล้องกับแบบฟอร์มลงทะเบียน
2	ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งานสำหรับเจ้าหน้าที่ของกรม อย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง	-ตรวจสอบรายการชื่อผู้ที่ลาออก หรือย้ายแผนก -ตรวจสอบว่ารายชื่อดังกล่าวต้องไม่สามารถเข้าถึงระบบได้ (กองการเจ้าหน้าที่จะต้องแจ้งภายในระยะเวลาอันสมควรเกี่ยวกับการลาออกหรือย้ายแผนกของเจ้าหน้าที่ เช่น ภายใน 1 เดือน)	-หนังสือที่เกี่ยวข้องกับแจ้งเวียนการลาออกหรือย้ายแผนก (ต้องจัดเก็บและแยกเอกสารดังกล่าวไว้ต่างหากเพื่อง่ายในการตรวจสอบในภายหลัง) -ไม่พบบัญชีผู้ใช้งานของผู้ที่ลาออก หรือย้ายแผนก ยังคงค้างอยู่ในระบบงาน
3	ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งานสำหรับหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง	-ตรวจสอบบัญชีผู้เข้าถึงระบบจากหน่วยงานภายนอก -ตรวจสอบว่าบัญชีดังกล่าวต้องไม่สามารถเข้าถึงระบบได้ เมื่อหมดสัญญาการจ้างงานแล้ว หรือไม่มีความจำเป็นต้องใช้งานอีกต่อไป และบันทึกผลการตรวจสอบไว้ในแบบฟอร์มตรวจสอบการเข้าถึงระบบจากหน่วยงานภายนอก	-บัญชีผู้เข้าถึงระบบจากหน่วยงานภายนอก -แบบฟอร์มตรวจสอบการเข้าถึงระบบจากหน่วยงานภายนอก -ไม่พบบัญชีผู้ใช้งานจากหน่วยงานภายนอก-ดังกล่าว ยังคงค้างอยู่บนระบบงาน เมื่อหมดความจำเป็นแล้ว
4	ให้ทำการจัดส่งบัญชีผู้ใช้งานและรหัสผ่าน โดยใส่ซองปิดผนึก และประทับตรา "ลับ" และ ส่งไปยังผู้ใช้งาน และแนบเอกสาร "**ระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และ ระบบเครือข่าย**" รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด	สังเกตการณ์วิธีการจัดส่งบัญชีผู้ใช้งาน	ไม่สังเกตพบว่ามีผู้ใช้งานที่ได้บัญชีผู้ใช้โดยไม่เป็นไปตามระเบียบปฏิบัติดังกล่าว

ระเบียบปฏิบัติในการพัฒนาระบบงาน

ผู้รับผิดชอบ : ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และ/หรือ ผู้พัฒนาระบบงาน และ/หรือ ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	จัดให้มีการตรวจรับและทดสอบระบบงานใหม่โดยผู้ใช้งานที่เกี่ยวข้องให้ครอบคลุมตามข้อกำหนดที่ระบุไว้ใน TOR จนกระทั่งการตรวจรับเสร็จสิ้น จึงจะเปิดให้บริการระบบงานนั้นได้	ตรวจสอบการตรวจรับตาม TOR ที่กำหนดไว้	เอกสารผลการตรวจรับโดยอ้างอิงตามหัวข้อต่างๆ ที่ปรากฏใน TOR
2	สำหรับระบบงานสำคัญ ให้กำหนดมาตรฐานการเข้ารหัสข้อมูลที่มีการรับ-ส่งระหว่างเครื่องลูกข่ายกับเครื่องเซิร์ฟเวอร์ และกำหนดให้พัฒนาระบบตามมาตรฐานนี้	ตรวจสอบว่าระบบงานสำคัญได้รับการพัฒนาตามมาตรฐานการเข้ารหัสข้อมูลที่องค์กรระบุไว้	-มาตรฐานการเข้ารหัสข้อมูลที่มีการรับ-ส่งระหว่างเครื่องลูกข่ายกับเครื่องเซิร์ฟเวอร์ -ไม่พบว่าระบบงานสำคัญได้รับการพัฒนาด้วยวิธีการอื่น ที่นอกเหนือจากมาตรฐานดังกล่าว
3	แสดงข้อความเตือนที่หน้าจอภายหลังจากการล็อกอินเสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ *"ระบบนี้เป็นระบบที่เป็นทรัพย์สินของกรม การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงาน หากมีการตรวจพบอาจมีการลงโทษทางวินัยหรือดำเนินการทางกฎหมายตามความเหมาะสม นอกจากนั้นแล้วกรมมีสิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้ใช้ระบบงานนี้"*	ตรวจสอบหน้าจอภายหลังการล็อกอินสำเร็จว่ามีข้อความดังกล่าวปรากฏหรือไม่	พบว่าระบบงานมีข้อความดังกล่าวปรากฏภายหลังการล็อกอินสำเร็จ
4	พัฒนาระบบงานตาม**แนวทางในการตรวจสอบข้อมูลนำเข้า (Guideline for Input Validation)**	-กรณีจ้าง ตรวจสอบใน TOR ว่าได้มีการแนบแนวทางดังกล่าวไว้เป็นส่วนหนึ่งของเอกสารการจ้างพัฒนาระบบงานหรือไม่ -กรณีพัฒนาเอง ตรวจสอบว่าระบบงานสามารถรับข้อมูลที่ไม่ตรงตามแนวทางดังกล่าวหรือไม่	-กรณีจ้าง พบว่ามีการกำหนดแนวทางดังกล่าวไว้เป็นส่วนหนึ่งของ TOR และพบว่าเมื่อทดสอบระบบงานนั้นแล้ว ระบบงานจะต้องรับข้อมูลเฉพาะที่สอดคล้องกับแนวทางดังกล่าวเท่านั้น -กรณีพัฒนาเอง พบว่าเมื่อทดสอบระบบงานนั้นแล้ว ระบบงานจะต้องรับข้อมูลเฉพาะที่สอดคล้องกับแนวทางดังกล่าวเท่านั้น
5	ทำการทดสอบระบบงาน และบันทึกผลการทดสอบเก็บไว้เป็นลายลักษณ์อักษรตาม**แนวทางในการตรวจสอบข้อมูลนำเข้า (Input Validation Guideline)**	ตรวจสอบว่าระบบงานสามารถรับข้อมูลที่ตรงตามแนวทางแนวทางดังกล่าวหรือไม่	-ผลการทดสอบตามแผนการทดสอบข้อมูลนำเข้าเพื่อป้องกันความผิดพลาดของข้อมูลนำเข้า

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
			-ผลการทดสอบต้องสอดคล้องกับแนวทางดังกล่าว -พบว่าเมื่อทดสอบระบบงานนั้นแล้ว ระบบงานจะต้องรับข้อมูลเฉพาะที่สอดคล้องกับแนวทางดังกล่าวเท่านั้น
6	พัฒนาระบบงานเพื่อให้สามารถกำหนดรหัสผ่านที่มีความเข้มแข็งตาม**ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน**	ตรวจสอบว่าระบบงานสามารถกำหนดรหัสผ่านตามระเบียบการตั้งรหัสผ่านหรือไม่	ระบบงานสามารถตั้งรหัสผ่านได้ตามระเบียบดังกล่าว
7	รวบรวมและจัดเก็บซอร์สโค้ดของระบบงานทั้งหมดไว้ในสถานที่เดียวกันที่มีความปลอดภัยและควบคุมให้มีเวอร์ชันของซอร์สโค้ด อย่างน้อย 2 เวอร์ชันล่าสุดและกำหนดให้ผู้ที่เกี่ยวข้องเท่านั้นจึงจะสามารถเข้าถึงได้	-ตรวจสอบสถานที่จัดเก็บซอร์สโค้ดของระบบงานและจำนวนเวอร์ชัน -ตรวจสอบสิทธิการเข้าถึงซอร์สโค้ด	-บัญชีรายชื่อผู้มีสิทธิเข้าถึงซอร์สโค้ดของระบบงาน -ไม่พบบัญชีผู้ใช้งานอื่นที่สามารถเข้าถึงซอร์สโค้ดดังกล่าวได้ -พบว่ามีการจัดซอร์สโค้ดไว้อย่างน้อย 2 เวอร์ชันล่าสุด
8	จัดให้มีการอบรมสำหรับระบบงานใหม่ให้แก่ผู้ใช้งานทั้งหมดที่เกี่ยวข้อง	ตรวจสอบวันและเวลา สถานที่ และหลักสูตรการอบรมสำหรับระบบงานใหม่นั้น	- เอกสารหรือคู่มือประกอบการอบรมสำหรับระบบงานใหม่นั้น - แบบฟอร์มลงทะเบียนรายชื่อผู้เข้ารับการอบรม
9	จัดทำคู่มือการใช้งานสำหรับระบบงานใหม่อย่างน้อยสำหรับผู้ใช้งาน และผู้ดูแลระบบ	ตรวจสอบคู่มือสำหรับระบบงานใหม่ว่ามีครบถ้วนหรือไม่	คู่มือสำหรับผู้ใช้งานและผู้ดูแลระบบ

แนวทางในการตรวจสอบข้อมูลนำเข้า (Guideline for input validation)

ผู้รับผิดชอบ : ผู้พัฒนาระบบ

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	ปฏิบัติตามแนวทางในการตรวจสอบข้อมูลนำเข้าดังนี้ เพื่อป้องกันข้อมูลนำเข้ามีความผิดพลาด o ตรวจสอบข้อมูลนำเข้าให้ตรงกับชนิดของข้อมูลของตัวแปรของโปรแกรม o ตรวจสอบข้อมูลนำเข้าให้อยู่ภายในช่วงของค่าของตัวแปรของโปรแกรม o ตรวจสอบข้อมูลนำเข้าให้อยู่ภายในค่าขอบเขตบนและล่างของตัวแปรของโปรแกรม o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันไม่ให้อยู่นอกช่วงของค่าที่กำหนดไว้ o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันข้อมูลขาดหายหรือไม่ครบถ้วน o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันการใส่ตัวอักษรไม่ถูกต้อง o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันการลืมใส่ค่าคีย์หรือไม่ให้คีย์มีความซ้ำซ้อนกัน o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันการใส่ตัวอักษรพิเศษต่างๆ	ตรวจสอบว่าระบบงานจะต้องสามารถรับข้อมูลนำเข้าได้ตรงตามเงื่อนไขดังกล่าว	-ผลการทดสอบตามแผนการทดสอบข้อมูลนำเข้าเพื่อป้องกันความผิดพลาดของข้อมูลนำเข้า -ผลการทดสอบต้องสอดคล้องกับแนวทางในการตรวจสอบข้อมูลนำเข้า -พบว่าเมื่อทดสอบระบบงานนั้นแล้ว ระบบงานจะต้องรับข้อมูลเฉพาะที่สอดคล้องกับแนวทางดังกล่าวเท่านั้น

ระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และระบบเครือข่าย

ระเบียบปฏิบัติสำหรับการใช้งานเครื่องคอมพิวเตอร์และเครือข่ายอย่างเหมาะสม

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	ให้ผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในกรณีที่ทำเครื่องให้ชำรุดหรือสูญหายไปโดยประมาทหรือเลินเล่อ	มีการตั้งกรรมการเพื่อสอบในกรณีที่ทำให้เครื่องชำรุดหรือสูญหายไปโดยประมาทหรือเลินเล่อ	ผลการพิจารณาโดยกรรมการ
2	ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 3 ชั่วโมง	สังเกตดูว่ายังมีผู้ใช้งานที่เปิดเครื่องทิ้งไว้หรือไม่	ไม่พบว่ามีเครื่องของผู้ใช้งานที่เปิดทิ้งไว้โดยไม่เป็นไปตามระเบียบ
3	ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาที	ตรวจสอบว่าเครื่องคอมพิวเตอร์ส่วนบุคคลได้รับการตั้งค่า Screen Saver อย่างถูกต้อง	ไม่พบว่าเครื่องส่วนบุคคลยังไม่ได้รับการตั้งค่า Screen Saver ตามที่กำหนดไว้
4	ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคล และระบบเครือข่ายเหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานทรัพย์สินของตนเอง	สังเกตจากการระมัดระวังและดูแลรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานใช้งาน	-ไม่พบว่าเครื่องคอมพิวเตอร์ส่วนบุคคลมีการสูญหาย -พบว่าการใช้งานเครื่องคอมพิวเตอร์โน้ตบุ๊คนอกสถานที่เป็นไปตามระเบียบที่กำหนดไว้ -ไม่พบว่าเครื่องคอมพิวเตอร์โน้ตบุ๊คมีการสูญหาย
5	ห้ามเจ้าหน้าที่ทั่วไปติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย	- ตรวจสอบการติดตั้งโปรแกรมประเภท sniffer ในเครื่องของผู้ใช้งาน โดยพิจารณาจากตัวอย่างรายชื่อโปรแกรมประเภท sniffer	ไม่พบการติดตั้งโปรแกรมประเภท sniffer ในเครื่องของผู้ใช้งาน
6	ห้ามเจ้าหน้าที่ทั่วไปติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในระบบเครือข่ายขององค์กร เพื่อให้บุคคลอื่นสามารถเข้าถึงหรือเชื่อมต่อเพื่อเข้าสู่ระบบเครือข่ายขององค์กร	-สังเกตหรือตรวจสอบดูว่ามีการติดตั้งโปรแกรมหรืออุปกรณ์ที่ใช้สำหรับการเชื่อมต่อทางเครือข่ายในสำนักงานของผู้ใช้งานหรือไม่ -กรณีที่องค์กรมีบัญชีทรัพย์สินของฮาร์ดแวร์และซอฟต์แวร์ สามารถตรวจสอบอุปกรณ์ใหม่ๆ ที่พบในสำนักงานเทียบกับบัญชีนี้ได้	ไม่พบว่ามีการติดตั้งโปรแกรม โมเด็มหรืออุปกรณ์สำหรับการเชื่อมต่อในระบบเครือข่ายในสำนักงานของผู้ใช้งาน

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
7	ต้องขออนุมัติจากทางฝ่ายอาคารหรือผู้มีอำนาจ ในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกสำนักงาน	สังเกตหรือขอดูใบขออนุญาตนำอุปกรณ์คอมพิวเตอร์ของสำนักงานออกนอกองค์กร	-ไม่พบการสูญหายของอุปกรณ์คอมพิวเตอร์ -ไม่พบว่าในใบขออนุญาตนำอุปกรณ์คอมพิวเตอร์ออกนอกสถานที่ กรอกข้อมูลไว้ไม่ชัดเจนหรือไม่มีการอนุญาตจากผู้มีอำนาจ
8	ให้ออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ	สังเกตการเข้าใช้งานและออกจากระบบงานเมื่อเสร็จสิ้นภารกิจ	-ไม่พบว่ามีการล็อกอินเข้าใช้ระบบและเปิดทิ้งไว้เป็นระยะเวลานานโดยไม่ได้ทำอะไรกับระบบ

ระเบียบปฏิบัติสำหรับการป้องกันไวรัส

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1.	ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบแจ้งเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศเพื่อดำเนินการแก้ไขโดยทันที	-ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสบนเครื่องของผู้ใช้งานว่ายังสามารถตรวจสอบไวรัสได้ตามปกติหรือไม่ -ตรวจสอบการปรับปรุงฐานข้อมูลไวรัสจากเมนูการใช้งานของโปรแกรมป้องกันไวรัสบนเครื่องของผู้ใช้งาน	หน้าจอแสดงผลการปรับปรุงฐานข้อมูลครั้งล่าสุด (ภายหลังจากเลือกเมนูนั้น)
2.	หากเครื่องของผู้ใช้งานยังไม่มีโปรแกรมตรวจสอบไวรัสให้ดาวน์โหลดโปรแกรมTrendMicro OfficeScan และคู่มือการติดตั้งที่ http://www.moph.go.th/download/	- อ่านคู่มือก่อนติดตั้ง จากนั้นดำเนินการตรวจสอบตามข้อ 1	หน้าจอแสดงไอคอนTrendMicro ที่ Taskbar
3.	Scan Virus ที่ Removable Drive ทุกครั้งที่มีการเชื่อมต่อ	ใช้โปรแกรม Scan Removable Drive	
4.	กรณีพบ Virus แต่โปรแกรม Anti Virus ไม่สามารถกำจัดได้ ให้รีบแจ้งคณะทำงานของหน่วยงานดำเนินการทันที หากยังไม่สามารถกำจัดได้ ให้คณะทำงานของหน่วยงานแจ้งศูนย์เทคโนโลยีสารสนเทศ ฯ โดยใช้แบบแจ้งซ่อมครุภัณฑ์คอมพิวเตอร์ เพื่อดำเนินการแก้ไขต่อไป	สังเกตหรือตรวจสอบไวรัสในเครื่องผู้ใช้และดำเนินการกำจัดไวรัส	หน้าจอแสดงผลการจัดการกับไวรัสที่พบ

ระเบียบปฏิบัติสำหรับการป้องกันการละเมิดลิขสิทธิ์และสิทธิทางปัญญา

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1.	ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น	ตรวจสอบการติดตั้งโปรแกรมในเครื่องของผู้ใช้งาน	-ไม่พบว่ามีโปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้องถูกติดตั้งในเครื่องของผู้ใช้งาน
2.	ระมัดระวังการใช้งานเอกสารหรือข้อมูลต่างๆ ซึ่งอยู่ในรูปแบบใดก็ตาม และได้มีการกำหนดเงื่อนไขการใช้งานเอาไว้ ต้องปฏิบัติตามเงื่อนไขดังกล่าวอย่างเคร่งครัด เพื่อไม่ให้เป็นการละเมิดทรัพย์สินทางปัญญาของบุคคลอื่น	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน

ระเบียบปฏิบัติสำหรับการใช้งานอินเทอร์เน็ต

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1.	ห้ามทำการดาวน์โหลด หรือส่งไฟล์ประเภทสื่อลามกอนาจาร	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
2.	ห้ามเล่นเกมส์ ดูภาพยนต์ หรือฟังเพลง ผ่านทางอินเทอร์เน็ตในเวลาทำงาน	-ใช้วิธีทางอ้อมเพื่อไม่อนุญาตกิจกรรมดังกล่าว สามารถใช้วิธีทางเทคนิค เช่น ไฟร์วอลล์ เพื่อป้องกันการเข้าถึงกิจกรรมดังกล่าว -ตรวจสอบว่าไฟร์วอลล์ได้มีการป้องกันไว้อย่างไรบ้าง	-ไฟร์วอลล์ได้มีการป้องกันการเข้าถึงกิจกรรมดังกล่าวไว้บ้าง -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
3.	ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้ -การพนัน -วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และพระมหากษัตริย์ -ลามก อนาจาร -อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม	-ใช้วิธีทางอ้อมเพื่อไม่อนุญาตการเข้าเว็บไซต์ดังกล่าว สามารถใช้วิธีทางเทคนิค เช่น ไฟร์วอลล์ เพื่อป้องกันการเข้าถึงได้ -ตรวจสอบว่าไฟร์วอลล์ได้มีการป้องกันการเข้าเว็บไซต์เหล่านั้นไว้อย่างไรบ้าง	-ไฟร์วอลล์ได้มีการป้องกันการเข้าถึงเว็บไซต์ดังกล่าวไว้บ้าง -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
4.	ห้ามใช้งานข้อมูลที่ได้รับโดยผ่านทางอินเทอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของข้อมูลนั้น	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
5.	ห้ามใช้อินเทอร์เน็ตเพื่อส่ง กระจาย หรือแจกจ่าย ดังต่อไปนี้ -ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต -ข้อมูลที่เป็นความลับขององค์กรไปยังบุคคลที่ไม่ได้รับอนุญาต	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
6.	ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงขององค์กร	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน

ระเบียบปฏิบัติสำหรับการใช้งานอีเมล์

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	ห้ามมิให้เข้าถึงข้อมูลอีเมล์ของบุคคลอื่นโดยไม่ได้รับอนุญาต	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
2	ห้ามลงทะเบียนด้วย E-mail Address ที่องค์กรมอบให้ไว้ตามที่อยู่เว็บไซต์ต่างๆ ที่ไม่เกี่ยวข้องกับงานขององค์กร	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
3	ห้ามทำการส่งอีเมล์ที่เกี่ยวข้องกับงานขององค์กรด้วย E-mail Address อื่นที่นอกเหนือจากที่องค์กรจัดให้	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
4	ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนเรื่องการส่งจดหมายขยะโดยเจ้าหน้าที่ขององค์กร -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
5	ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนเรื่องการส่งจดหมายลูกโซ่โดยเจ้าหน้าที่ขององค์กร -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
6	ห้ามส่งอีเมล์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการฟ้องร้องเรื่องการละเมิดสิทธิของบุคคลอื่น -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
7	ห้ามส่งอีเมล์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา	-ใช้วิธีทางอ้อมเพื่อไม่อนุญาตการกระทำดังกล่าว สามารถใช้วิธีทางเทคนิค เช่น โปรแกรมป้องกันไวรัสบนเมล์เซิร์ฟเวอร์เพื่อดักจับไวรัสที่มาทางอีเมล์ -สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-มีการติดตั้งโปรแกรมป้องกันไวรัสบนเมล์เซิร์ฟเวอร์ -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
8	ห้ามปลอมแปลงอีเมล์ของบุคคลอื่น	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนหรือการฟ้องร้องเรื่องการส่งจดหมายเท็จโดยเจ้าหน้าที่ขององค์กร -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
9	ห้ามรับ หรือส่งอีเมล์แทนบุคคลอื่นโดยไม่ได้รับอนุญาต	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่สังเกตพบการส่งอีเมล์แทนกัน -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
10	ห้ามส่งอีเมล์ที่มีขนาดใหญ่เกินกว่า 8 เมกกะไบต์ หรือตามที่องค์กรระบุไว้	-ใช้วิธีทางอ้อมเพื่อไม่อนุญาตการกระทำดังกล่าว โดยปรับแต่งเมล์เซิร์ฟเวอร์เพื่อจำกัดขนาดของอีเมล์ที่ส่งไป	-ผู้ดูแลระบบเครือข่ายได้ปรับแต่งอีเมล์เซิร์ฟเวอร์เพื่อจำกัดขนาดของอีเมล์ที่ส่งออกไป
11	ห้ามส่งอีเมล์ที่เป็นความลับขององค์กร เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลอีเมล์ที่องค์กรกำหนดไว้	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนหรือการแจ้งเกี่ยวกับเรื่องการเปิดเผยข้อมูลต่างๆ ซึ่งรวมถึงความลับขององค์กร -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
12	ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่อีเมล์ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบเหตุการณ์ที่ผู้ใช้งานส่งอีเมล์ผิดตัวผู้รับ
13	ให้ใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับอีเมล์เท่าที่มีความจำเป็นต้องรับรู้รับทราบในข้อมูลที่ส่งไป	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบเหตุการณ์การส่งข้อมูลลับของเจ้าหน้าที่ให้แก่บุคคลที่ไม่มีความจำเป็นต้องรับทราบ
14	ให้ใช้คำที่สุภาพในการส่งอีเมล์	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนเรื่องการใช้วาจาไม่เหมาะสม หรือการฟ้องร้องการหมิ่นประมาทผู้อื่น -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
15	ให้ระบุชื่อของผู้ส่งในอีเมล์ทุกฉบับที่ส่งไป	-ใช้วิธีทางอ้อมเพื่อไม่อนุญาตการกระทำดังกล่าว โดยปรับแต่งเมล์เซิร์ฟเวอร์เพื่อบังคับให้มีการกำหนด E-mail Address ของอีเมล์ทุกฉบับที่ส่งไป	-ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน -ผู้ดูแลระบบเครือข่ายได้ปรับแต่งอีเมล์เซิร์ฟเวอร์เพื่อบังคับให้มีการกำหนด E-mail Address ของอีเมล์ทุกฉบับ
16	ให้ทำการสำรองข้อมูลอีเมล์ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าองค์กรจะทำการสำรองข้อมูลอีเมล์ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้นอีเมล์ที่เก่ามากๆ และจำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องขอข้อมูลอีเมล์ที่เก่ามากๆ และเกินกว่าระยะเวลาที่ผู้ดูแลระบบเครือข่ายได้สำรองข้อมูลไว้ให้

ระเบียบปฏิบัติสำหรับการป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
เจ้าหน้าที่จะต้องไม่ใช้ระบบเครือข่าย โดยมีวัตถุประสงค์ดังต่อไปนี้			
1	เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการฟ้องร้องเรื่องการกระทำผิดกฎหมายหรือการสร้างความเสียหายแก่บุคคลอื่น -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
2	เพื่อการกระทำที่ขัดต่อ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการฟ้องร้องเรื่องการละเมิด พ.ร.บ. ดังกล่าว -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
3	เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
4	เพื่อการค้าขาย หรือผลประโยชน์ส่วนตัว หรือผลประโยชน์ทางการเมือง	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนจากบุคคลภายนอกเกี่ยวกับการทำการค้าดังกล่าว -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
5	เพื่อการเข้าถึง แสดง จัดเก็บ แจกจ่าย แก้ไข จัดทำ หรือบันทึกข้อมูลที่มีเนื้อหาไม่เหมาะสม เช่น ข้อมูลอันเป็นเท็จ	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนหรือฟ้องร้องในเรื่องข้อมูลที่มีเนื้อหาไม่เหมาะสมดังกล่าว

	ข้อมูลที่มีผลต่อความมั่นคงของสถาบันชาติ ศาสนาและพระมหากษัตริย์ ภาพลามกอนาจาร ภาพตัดต่อของบุคคลอื่น หรือข้อมูลที่ก่อให้เกิดความเสื่อมเสียอับอายแก่องค์กรหรือบุคคลอื่น เป็นต้น		-ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
6	เพื่อทำการเผยแพร่ข้อมูล หรืออนุญาตให้ผู้อื่นเผยแพร่ข้อมูลเพื่อการกล่าวร้าย หมิ่นประมาทหรือพาดพิง บุคคลอื่นจนทำให้องค์กรถูกฟ้องร้องหรือก่อให้เกิดความเสียหายแก่องค์กร	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการฟ้องร้องเรื่องการหมิ่นประมาทหรือพาดพิงจนทำให้องค์กรเกิดความเสียหาย -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
7	เพื่อการเปิดเผยข้อมูลลับซึ่งได้มาจากการปฏิบัติงานให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กรหรือบุคคลภายนอกก็ตาม	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนหรือการแจ้งเกี่ยวกับเรื่องการเปิดเผยข้อมูลต่างๆ ซึ่งรวมถึงความลับขององค์กร -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
8	เพื่อขัดขวางหรือโจมตี การใช้งานระบบเครือข่ายขององค์กรหรือของหน่วยงานภายนอกอื่น	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนหรือฟ้องร้องเรื่องการขัดขวางหรือโจมตีระบบเครือข่ายขององค์กรหรือของผู้อื่น -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
9	เพื่อแพร่กระจายไวรัส หนอน ม้าโทรจัน สปายแวร์ สแปมเมล์ หรือโปรแกรมไม่ประสงค์ดีอื่นๆ	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนหรือฟ้องร้องเรื่องการแพร่กระจายโปรแกรมไม่ประสงค์ดีดังกล่าว -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
10	เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กรไปยังที่อยู่เว็บ หรือห้องสนทนาใดๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนหรือแจ้งเกี่ยวกับการแสดงความคิดเห็นที่เกี่ยวข้องกับการดำเนินงานขององค์กร ซึ่งคลาดเคลื่อนไปจากความเป็นจริง -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
11	เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อองค์กร	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	-ไม่พบการร้องเรียนหรือฟ้องร้องเกี่ยวกับการสร้างความเสียหายแก่องค์กร -ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน

ระเบียบปฏิบัติสำหรับการใช้งานเครื่องคอมพิวเตอร์โน้ตบุ๊ก

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	ในกรณีที่เป็นเครื่องโน้ตบุ๊คที่ใช้ร่วมกันให้ทำการกรอก **แบบฟอร์มยืม-คืนสำหรับเครื่องคอมพิวเตอร์โน้ตบุ๊ค**นั้น เพื่อขออนุมัติการนำไปใช้งาน และป้องกันการสูญหาย	ตรวจสอบเครื่องโน้ตบุ๊คกลางว่ามีการขออนุมัติทุกครั้งที่นำออกไปใช้งานนอกสถานที่	-แบบฟอร์มยืม-คืนสำหรับเครื่องคอมพิวเตอร์โน้ตบุ๊คบันทึกข้อมูลผู้ยืมไว้อย่างครบถ้วน -ในระหว่างที่ยืมไปนั้นต้องมีการบันทึกแบบฟอร์มไว้อย่างครบถ้วน -ไม่พบกรณีที่เครื่องคอมพิวเตอร์โน้ตบุ๊คไม่อยู่แต่ไม่มีการลงบันทึกใดๆ ไว้
2	ตรวจสอบอย่างสม่ำเสมอว่าโปรแกรมป้องกันไวรัสที่ใช้งานอยู่ได้รับการปรับปรุงฐานข้อมูลรูปแบบไวรัสอย่างสม่ำเสมอ	ตรวจสอบการปรับปรุงฐานข้อมูลไวรัสจากเมนูการใช้งานของโปรแกรมป้องกันไวรัสบนเครื่องนั้น	หน้าจอแสดงผลการปรับปรุงฐานข้อมูลครั้งล่าสุด (ภายหลังจากเลือกเมนูนั้น)
3	ให้ระมัดระวังและรักษาเครื่องคอมพิวเตอร์โน้ตบุ๊คเมื่อมีการนำไปใช้งานนอกสถานที่ เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	-ตรวจสอบการสูญหายของเครื่องคอมพิวเตอร์โน้ตบุ๊ค -ตรวจสอบพฤติกรรมการใช้งานเครื่องคอมพิวเตอร์โน้ตบุ๊ค เช่น มีการปล่อยเครื่องทิ้งไว้โดยไม่มีผู้ดูแล เป็นต้น	-ไม่พบว่าเครื่องคอมพิวเตอร์โน้ตบุ๊คมีการสูญหาย -ไม่พบว่ามีการปล่อยให้เครื่องคอมพิวเตอร์โน้ตบุ๊คทิ้งไว้โดยไม่มีผู้ดูแล
4	เมื่ออยู่ในที่สาธารณะหรือในห้องประชุม ห้ามปล่อยเครื่องทิ้งไว้โดยไม่มีผู้ดูแล	สังเกตการป้องกันเครื่องคอมพิวเตอร์โน้ตบุ๊คเมื่อจำเป็นต้องทิ้งไว้ในที่สาธารณะหรือห้องประชุม	-ไม่พบว่าเครื่องคอมพิวเตอร์โน้ตบุ๊คมีการสูญหาย -ไม่พบว่ามีการปล่อยให้เครื่องคอมพิวเตอร์โน้ตบุ๊คทิ้งไว้โดยไม่มีผู้ดูแล
5	ตรวจสอบว่าได้มีการตั้งค่า Screen Saver เพื่อให้ทำการล็อกหน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาที	ตรวจสอบการตั้งค่า Screen Saver ดังกล่าวบนเครื่องคอมพิวเตอร์โน้ตบุ๊ค	-ไม่พบว่าเครื่องคอมพิวเตอร์โน้ตบุ๊คไม่ได้รับการตั้งค่า Screen Saver ไว้

ระเบียบปฏิบัติสำหรับการกำหนดและป้องกันรหัสผ่าน

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	เก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น	สังเกตพฤติกรรมการใช้งานรหัสผ่านของพนักงาน ซึ่งรวมถึงการบอกรหัสผ่าน	-ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
2	กำหนดรหัสผ่านให้มีคุณสมบัติ ตาม**ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน**	-ใช้วิธีทางอ้อมเพื่อไม่อนุญาตการกระทำดังกล่าว โดยพัฒนาหรือปรับแต่งระบบรุ่นใหม่เพื่อให้สามารถตั้งรหัสผ่านตามระเบียบปฏิบัติดังกล่าว -ตรวจสอบความยาวรหัสผ่านโดยนับจากจำนวนสัญลักษณ์ที่ปรากฏเพื่อปกปิดรหัสผ่านบนหน้าจอ	-ระบบงานใหม่ๆ (นับจากปี พ.ศ. 2551)ได้รับการพัฒนาให้เป็นไปตามระเบียบดังกล่าวโดยสามารถทดลองใส่รหัสผ่านเพื่อดูความสอดคล้องกับระเบียบปฏิบัติฯ -ไม่พบรหัสผ่านที่มีความยาวน้อยกว่าความยาวขั้นต่ำที่กำหนดไว้
3	กำหนดรหัสผ่านสำหรับการใช้ไฟล์ข้อมูลร่วมกันบนเครือข่าย	ตรวจสอบการกำหนดรหัสผ่านสำหรับไฟล์ข้อมูลที่มีการใช้งานร่วมกัน	ไม่พบไฟล์ข้อมูลที่มีการใช้งานร่วมกันบนเครือข่ายไม่ได้รับการกำหนดรหัสผ่าน
4	ห้ามบันทึกรหัสผ่านไว้ในโปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านของตน (เช่น ในโปรแกรมเว็บบราวเซอร์จะสามารถเลือกให้โปรแกรมช่วยจำรหัสผ่านไว้ให้)	สังเกตพฤติกรรมการบันทึกรหัสผ่านไว้ในโปรแกรมที่ใช้งานนั้นเพื่อให้ในภายหลังสามารถย้อนกลับมาใช้ได้โดยง่าย โดยไม่ต้องมีการใส่รหัสผ่านอีกครั้ง	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน
5	ต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น	สังเกตพฤติกรรมการเก็บรหัสผ่านของผู้ใช้งานว่าเก็บไว้อย่างปลอดภัยหรือไม่	ไม่พบว่ามีการจด บันทึก หรือเก็บรหัสผ่านไว้ในที่ที่สามารถสังเกตเห็นได้โดยง่าย
6	ในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน

ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
	กำหนดรหัสผ่านให้มีคุณสมบัติ ดังต่อไปนี้		
1	มีความยาวไม่น้อยกว่า 6 ตัวอักษร ยกเว้นระบบเก่าๆ ที่ไม่สามารถดำเนินการได้	-ใช้วิธีทางอ้อมเพื่อบังคับให้ผู้ใช้งานตั้งรหัสผ่านตามความยาวดังกล่าว โดยพัฒนาหรือปรับแต่งระบบรุ่นใหม่เพื่อให้สามารถตั้งรหัสผ่านตามระเบียบการตั้งรหัสผ่านนี้ -ตรวจสอบความยาวรหัสผ่านโดยนับจากจำนวนสัญลักษณ์ที่ปรากฏเพื่อปกปิดรหัสผ่านบนหน้าจอ	-ระบบงานใหม่ๆ (นับจากปี พ.ศ. 2551) ได้รับการพัฒนาให้เป็นไปตามระเบียบการตั้งรหัสผ่านนี้ โดยสามารถทดลองใส่รหัสผ่านเพื่อดูความสอดคล้องกับระเบียบปฏิบัติฯ -ไม่พบรหัสผ่านที่มีความยาวน้อยกว่าความยาวขั้นต่ำที่กำหนดไว้
2	มีการผสมผสานกันระหว่างตัวอักษรที่เป็นตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน	ใช้วิธีทางอ้อมเพื่อบังคับให้ผู้ใช้งานตั้งรหัสผ่านโดยผสมผสานตัวอักษรต่างๆ โดยพัฒนาหรือปรับแต่งระบบรุ่นใหม่เพื่อให้สามารถตั้งรหัสผ่านตามระเบียบการตั้งรหัสผ่านนี้	-ระบบงานใหม่ๆ (นับจากปี พ.ศ. 2551) ได้รับการพัฒนาให้เป็นไปตามระเบียบการตั้งรหัสผ่านนี้ โดยสามารถทดลองใส่รหัสผ่านเพื่อดูความสอดคล้องกับระเบียบปฏิบัติฯ
3	ไม่กำหนดรหัสผ่านจากคำศัพท์ที่ปรากฏในพจนานุกรม	ใช้วิธีทางอ้อมเพื่อบังคับให้ผู้ใช้งานตั้งรหัสผ่านโดยไม่ใช้คำจากพจนานุกรม โดยพัฒนาหรือปรับแต่งระบบรุ่นใหม่เพื่อให้สามารถตั้งรหัสผ่านตามระเบียบการตั้งรหัสผ่านนี้	-ระบบงานใหม่ๆ (นับจากปี พ.ศ. 2551) ได้รับการพัฒนาให้เป็นไปตามระเบียบการตั้งรหัสผ่านนี้ โดยสามารถทดลองใส่รหัสผ่านเพื่อดูความสอดคล้องกับระเบียบปฏิบัติฯ
4	เปลี่ยนรหัสผ่านทุกๆ 6 เดือนสำหรับเจ้าหน้าที่ทั่วไปและทุกๆ 3 เดือนสำหรับเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ	ใช้วิธีทางอ้อมเพื่อบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดไว้ โดยพัฒนาหรือปรับแต่งระบบรุ่นใหม่เพื่อให้สามารถตั้งรหัสผ่านตามระเบียบการตั้งรหัสผ่านนี้	-ระบบงานใหม่ๆ (นับจากปี พ.ศ. 2551) ได้รับการพัฒนาให้เป็นไปตามระเบียบการตั้งรหัสผ่านนี้ โดยสามารถทดลองใส่รหัสผ่านเพื่อดูความสอดคล้องกับระเบียบปฏิบัติฯ

ระเบียบปฏิบัติสำหรับการใช้งานห้องเครื่อง

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	ห้ามเจ้าหน้าที่เข้าไปในบริเวณห้องเครื่องโดยไม่มีกิจที่เกี่ยวข้อง	สังเกตบุคคลที่เข้าออกห้องเครื่องโดยต้องมีผู้ดูแลจากศูนย์เทคโนโลยีสารสนเทศคอยติดตามดูแลโดยตลอด	-ไม่พบเจ้าหน้าที่จากกองอื่นๆ เข้าไปในบริเวณห้องเครื่องโดยไม่มีผู้ดูแล
2	ห้ามใส่รองเท้าเข้าห้องเครื่อง	สังเกตดูว่ามีการใส่รองเท้าเข้าไปในห้องเครื่องหรือไม่	ไม่พบว่ามีการใส่รองเท้าเข้าไปในห้องเครื่อง
3	ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้องเครื่อง	สังเกตดูว่ามีการนำอาหารหรือเครื่องดื่มเข้าไปในห้องเครื่องหรือไม่	ไม่พบว่ามีการนำอาหารหรือเครื่องดื่มเข้าไปในห้องเครื่อง
4	หากพบเห็นความผิดปกติในห้องเครื่อง เช่น มีทรัพย์สินหาย มีร่องรอยการบุกรุก เป็นต้น ให้รีบแจ้งเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์การละเลยไม่แจ้ง เมื่อพบเหตุความผิดปกติ
5	ให้ปฏิบัติตามคำแนะนำของเจ้าหน้าที่ที่ดูแลห้องเครื่องอย่างเคร่งครัด	สังเกตดู หรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ความเสียหายในห้องเครื่องเนื่องจากการไม่ปฏิบัติตามคำแนะนำของผู้ดูแลห้อง

ระเบียบปฏิบัติสำหรับการลงทะเบียนเข้าใช้ระบบงาน
ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	เมื่อเจ้าหน้าที่ใหม่เข้ามาปฏิบัติหน้าที่ ให้กรอกแบบฟอร์มเพื่อขออนุมัติใช้งานระบบงาน ตามแบบฟอร์มลงทะเบียนผู้ใช้งาน และนำเสนอต่อผู้บังคับบัญชาเพื่อขอการอนุมัติ	-ตรวจสอบความสอดคล้องระหว่างแบบฟอร์มลงทะเบียนกับบัญชีผู้ใช้งานของระบบงาน -ตรวจการกรอกรายละเอียดของผู้ใช้งานในแบบฟอร์มให้ครบถ้วน	-บัญชีผู้ใช้งานในระบบสอดคล้องกับแบบฟอร์มลงทะเบียนผู้ใช้งาน -แบบฟอร์มมีการกรอกรายละเอียดที่ครบถ้วนและชัดเจน
2	ห้ามเจ้าหน้าที่ใหม่ใช้ระบบงานขององค์กรจนกว่าจะได้รับการอนุมัติให้ใช้งานโดยผ่านการลงทะเบียนก่อน	ตรวจสอบความสอดคล้องระหว่างแบบฟอร์มลงทะเบียนกับบัญชีผู้ใช้งานของระบบงาน	บัญชีผู้ใช้งานในระบบสอดคล้องกับแบบฟอร์มลงทะเบียนผู้ใช้งาน

ระเบียบปฏิบัติสำหรับการจัดซื้อจัดจ้างทางด้าน ICT
ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของกรม

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1	ในการจัดซื้อจัดจ้างที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ให้ทำเรื่องผ่านทางศูนย์เทคโนโลยีสารสนเทศเพื่อดูความเข้ากันได้กับโครงสร้างพื้นฐานสารสนเทศขององค์กร และความเหมาะสมในการใช้งาน ก่อนการจัดซื้อจัดจ้าง	-ตรวจสอบเรื่องที่ผ่านการพิจารณาจัดซื้อจัดจ้างทางด้าน ICT ว่ามีรายละเอียดที่ครบถ้วนหรือไม่ -สังเกตการจัดซื้ออุปกรณ์ ICT ใหม่ๆ และขอตรวจสอบว่าได้มีการพิจารณาโดยศูนย์เทคโนโลยีสารสนเทศหรือไม่	-เรื่องที่ผ่านการพิจารณาต้องมีรายละเอียดต่อไปนี้เป็นอย่างน้อย - ความเข้ากันได้กับโครงสร้างพื้นฐานปัจจุบัน - ความเหมาะสมในการใช้งาน -ไม่พบการจัดซื้อจัดจ้างทางด้าน ICT ที่ไม่ผ่านการพิจารณาจากศูนย์เทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติสำหรับการนำข้อมูลเผยแพร่สู่สาธารณะ

ระเบียบปฏิบัติสำหรับการนำข้อมูลเผยแพร่สู่สาธารณะ
ผู้รับผิดชอบ : ผู้รับผิดชอบข้อมูลที่ต้องนำเผยแพร่สู่สาธารณะ

ที่	ระเบียบปฏิบัติ	วิธีตรวจสอบ	ตัวอย่าง หลักฐานการปฏิบัติ
1.	ให้ผู้ที่เป็นเจ้าของข้อมูลที่ต้องการนำข้อมูลนั้นขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของกรม จะต้องทำการตรวจสอบความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น	-ตรวจสอบหรือสังเกตความถูกต้องของข้อมูลที่นำขึ้นเว็บไซต์ของกรม -ตรวจสอบแบบฟอร์มการขออนุมัตินำข้อมูลขึ้นเว็บไซต์ขององค์กร	-ไม่พบข้อมูลบนเว็บไซต์ที่มีเนื้อหาผิดพลาดหรือไม่เหมาะสมต่อการนำเสนอ -ไม่พบข้อมูลบนเว็บไซต์ที่ไม่มีการขออนุมัติผ่านทางแบบฟอร์มการนำข้อมูลขึ้นเว็บไซต์ขององค์กร -แบบฟอร์มฯ มีการกรอกข้อมูลที่ครบถ้วนและถูกต้อง
2.	ให้ผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของกรมจะต้องดำเนินการด้วยตนเอง โดยห้ามมิให้ผู้อื่นดำเนินการแทน	สังเกตดูหรือคอยรับข้อมูลข่าวสารเกี่ยวกับระเบียบนี้ เช่น การไม่ปฏิบัติตาม	ไม่พบเหตุการณ์ที่ผู้ใช้งานฝ่าฝืน