มหาวิทยาลัยราชภัฏอุตรดิตถ์
สำนักงานตรวจสอบภายใน

เอกสารเลขที่ ๐๒๘/๒๕๖๙

แนวทางการตรวจสอบ
เรื่อง ตรวจสอบระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์การตรวจสอบ

๑. เพื่อให้มั่นใจว่าการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยมีประสิทธิภาพเป็นประโยชน์ในการบริหารจัดการของมหาวิทยาลัยและเป็นไปตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง

๒. เพื่อให้มั่นใจว่าหน่วยงานมีการบริหารจัดการการเข้าถึงผู้ใช้งานเป็นไปตามแนวปฏิบัติ ข้อกำหนด และหลักเกณฑ์ที่กำหนด

๓. เพื่อให้มั่นใจว่าหน่วยงานมีการควบคุมภายใน การบริหารความเสี่ยง และการกำกับดูแลที่เพียงพอ เหมาะสม

๔. เพื่อให้ทราบปัญหาและอุปสรรคในการดำเนินงาน และเสนอแนะแนวทางการแก้ไขปัญหาและอุปสรรคที่เกิดขึ้น

ขอบเขตการตรวจสอบ

เอกสารหลักฐานต่างๆ ด้านระบบเทคโนโลยีสารสนเทศ ตั้งแต่ปีงบประมาณ พ.ศ.๒๕๖๘ – พ.ศ.๒๕๖๙

กฎหมาย ระเบียบ ประกาศและหนังสือที่เกี่ยวข้อง

๑. พระราชกฤษฎีกาการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙

๒. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ.๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๓. พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๔. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ.๒๕๕๓ และฉบับที่ ๒ พ.ศ.๒๕๕๖

๕. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.๒๕๕๕

๖. แนวทางการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ การควบคุมภายในเทคโนโลยีสารสนเทศกรมบัญชีกลาง

๗. จุลสารตรวจสอบภายใน ปีที่ ๒๑ ฉบับที่ ๑๑๖ ประจำเดือน กุมภาพันธ์-มีนาคม ๒๕๖๐ แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารหลักฐานที่เกี่ยวข้อง
๑. การบริหารจัดการการเข้าถึงผู้ใช้งาน	๑.๑ ตรวจสอบว่าหน่วยงานมีการให้ความรู้ความเข้าใจกับผู้ปฏิบัติงานหรือไม่ เช่น โดยวิธีการเผยแพร่ทาง Website จัดอบรมให้ความรู้ หนังสือเวียน และวิธีอื่นๆ ๑.๒ ตรวจสอบว่าหน่วยงานมีข้อกำหนดในการลงทะเบียนสำหรับผู้เข้าใช้งานระบบหรือไม่ ๑.๓ ตรวจสอบว่าหน่วยงานมีข้อกำหนดและหลักเกณฑ์ในการอนุญาตให้ใช้งานระบบ	- หลักฐานการเผยแพร่ทาง Website - โครงการจัดอบรมให้ความรู้ - หนังสือเวียนแจ้งหน่วยงานภายใน - แนวปฏิบัติ/หลักเกณฑ์/ประกาศ - สอบถามผู้ที่เกี่ยวข้อง - หลักฐานอื่น (ถ้ามี)

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารหลักฐานที่เกี่ยวข้อง
	หรือไม่ ๑.๔ ตรวจสอบว่าหน่วยงานมีข้อกำหนดและหลักเกณฑ์ในการยกเลิก/เพิกถอนการอนุญาตให้เข้าใช้งานในระบบหรือไม่ ๑.๕ ตรวจสอบว่าหน่วยงานมีการกำหนดแนวปฏิบัติสำหรับผู้ใช้งานเกี่ยวกับ วิธีการกำหนดรหัสที่ดี การใช้รหัสผ่าน และการเปลี่ยนรหัสผ่านหรือไม่ ๑.๖ ตรวจสอบว่าหน่วยงานมีการควบคุมและจำกัดสิทธิดังนี้ หรือไม่ - มีเอกสารแสดงการกำหนดสิทธิ (ตารางกำหนดสิทธิ) - ไม่มีการสร้าง User ร่วม - สิทธิที่กำหนดให้แต่ละกลุ่มชัดเจนและเหมาะสม ๑.๗ ตรวจสอบว่ากระบวนการให้รหัสผ่านได้รับความเห็นชอบจากผู้บริหารและเป็นไปตามเงื่อนไขที่ฝ่ายบริหารกำหนดหรือไม่ ๑.๘ ตรวจสอบว่าหน่วยงานมีการดำเนินการเพิกถอนรหัสตามเงื่อนไขที่กำหนดหรือไม่ ๑.๙ ตรวจสอบว่าหน่วยงานมีการกำหนดเงื่อนไขให้ผู้ใช้งานเก็บรหัสไว้เป็นความลับหรือไม่ ๑.๑๐ ตรวจสอบการทบทวนสิทธิเข้าถึงของผู้ใช้งานว่ามีการดำเนินการอย่างต่อเนื่องเป็นระยะ โดยมีการกำหนดระยะเวลาในการทบทวนที่แน่นอนหรือไม่	
๒. การกำหนดหน้าที่ความรับผิดชอบ	๒.๑ ตรวจสอบว่าหน่วยงานมีการกำหนดแนวปฏิบัติสำหรับผู้ใช้งานเกี่ยวกับวิธีการกำหนดรหัสผ่านที่ดี การใช้รหัสผ่าน และการเปลี่ยนรหัสผ่านหรือไม่ ๒.๒ ตรวจสอบว่าผู้ใช้งานรับทราบแนวปฏิบัติเกี่ยวกับรหัส ผ่านช่องทางใด เช่น - เผยแพร่ทาง Website - จัดอบรมให้ความรู้ - หนังสือเวียน - วิธีอื่นๆ ๒.๓ ตรวจสอบว่าหน่วยงานมีการกำหนดข้อปฏิบัติสำหรับผู้ใช้งานเกี่ยวกับการป้องกันสารสนเทศ ขณะไม่มีผู้ใช้งานหรือไม่ ๒.๔ ตรวจสอบว่าหน่วยงานมีการกำหนดข้อปฏิบัติสำหรับผู้ใช้งานเกี่ยวกับการควบคุมข้อมูล สื่อ และสินทรัพย์ด้านสารสนเทศหรือไม่	- แนวปฏิบัติ/ข้อปฏิบัติ/หลักเกณฑ์ต่างๆ - สอบถามผู้ที่เกี่ยวข้อง - หลักฐานอื่น (ถ้ามี)

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารหลักฐานที่เกี่ยวข้อง
	๒.๕ ตรวจสอบว่าหน่วยงานมีการกำหนดข้อปฏิบัติและหลักเกณฑ์สำหรับการเข้าถึงข้อมูลที่เป็นความลับและข้อมูลที่สำคัญของหน่วยงานหรือไม่	
๓. การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน	๓.๑ ตรวจสอบว่าหน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการคัดเลือกระบบสารสนเทศหรือไม่ ๓.๒ ตรวจสอบว่าหน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการจัดทำระบบสำรองหรือไม่ ระบบที่หน่วยงานจัดทำกำหนดให้มีการคืนและรายงานผลได้ ๓.๓ ตรวจสอบว่าทุกระบบที่หน่วยงานจัดทำสำรองมีการรายงานผลการสำรองหรือไม่ ๓.๔ ตรวจสอบว่าหน่วยงานมีการเตรียมแผนการเตรียมความพร้อมกรณีฉุกเฉิน ดังนี้หรือไม่ - กรณีไม่สามารถดำเนินงานด้วยระบบอิเล็กทรอนิกส์ได้ - กรณีที่ Site หลักไม่ทำงาน - มีการกำหนดแผนระยะสั้น - มีการกำหนดแผนระยะยาว - มีการทบทวนแผน ๓ เดือนครั้ง ๓.๕ ตรวจสอบว่าหน่วยงานมีการกำหนดหน้าที่ความรับผิดชอบของบุคลากร ดังนี้ - ด้านระบบสารสนเทศ - ด้านระบบสำรอง - ด้านการจัดทำแผนและทบทวนแผน ๓.๖ ตรวจสอบว่าหน่วยงานมีการทดสอบระบบให้อยู่ในสภาพพร้อมใช้งานหรือไม่ - ระบบสารสนเทศ - ระบบสำรอง - แผนฉุกเฉิน	- แนวปฏิบัติ/ข้อปฏิบัติ/หลักเกณฑ์ต่างๆ - แผนเตรียมความพร้อมกรณีฉุกเฉินและแผนต่างๆ - สอบถามผู้ที่เกี่ยวข้อง - หลักฐานอื่น (ถ้ามี)
๔. ระบบการควบคุมภายใน	๔.๑ สอบทานและประเมินการควบคุมทั่วไป ๔.๒ สอบทานและประเมินการควบคุมโครงการพัฒนาระบบสารสนเทศ ๔.๓ สอบทานและประเมินการควบคุมการเปลี่ยนแปลงแก้ไขระบบ ๔.๔ สอบทานและประเมินการควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์ ๔.๕ สอบทานและประเมินการควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ ๔.๖ สอบทานและประเมินการควบคุมการเข้าถึงข้อมูล ๔.๗ สอบทานและประเมินการควบคุมระบบงาน	- แบบประเมินการควบคุมภายใน

ประเด็นการตรวจสอบ	วิธีการตรวจสอบ	เอกสารหลักฐานที่เกี่ยวข้อง
๕. การกำกับดูแล	๕.๑ สอบทานและประเมินการกำกับดูแลของผู้บังคับบัญชาและหัวหน้างาน	- แบบประเมินการกำกับดูแล
๖. การบริหารจัดการความเสี่ยง	๖.๑ สอบทานและประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ	- แบบประเมินความเสี่ยง

มหาวิทยาลัยราชภัฏอุตรดิตถ์
สำนักงานตรวจสอบภายใน

รหัสกระดาษทำการ IA ๐๒๘/๒๕๖๙

กระดาษทำการตรวจสอบ
เรื่อง ตรวจสอบระบบเทคโนโลยีสารสนเทศ

หน่วยรับตรวจ.....**ผู้รับตรวจ**.....
ตรวจสอบ ณ วันที่.....**ตำแหน่ง**.....
เกณฑ์การให้คะแนน

๑ คะแนน = ใช่/มีการปฏิบัติทั้งหมด
๐.๕๐ คะแนน = ใช่/มีการปฏิบัติบางส่วน
๐ คะแนน = ไม่ใช่/ไม่มีการปฏิบัติ

ลำดับ	วิธีการตรวจสอบ	ผลตรวจสอบ			หมายเหตุ
		ใช่/มีการปฏิบัติ ๑ คะแนน	ใช่/มีบางส่วน ๐.๕ คะแนน	ไม่ใช่/ไม่มีการปฏิบัติ ๐ คะแนน	
การบริหารจัดการการเข้าถึงผู้ใช้งาน					
๑	หน่วยงานมีการให้ความรู้ ความเข้าใจกับผู้ปฏิบัติงาน โดยวิธีการเผยแพร่ทาง Website จัดอบรมให้ความรู้ หนังสือเวียน และวิธีอื่นๆ				
๒	หน่วยงานมีข้อกำหนดในการลงทะเบียนสำหรับผู้เข้าใช้งานระบบ				
๓	หน่วยงานมีข้อกำหนดและหลักเกณฑ์ในการอนุญาตให้ใช้งานระบบ				
๔	หน่วยงานมีข้อกำหนดและหลักเกณฑ์ในการยกเลิก/เพิกถอนการอนุญาตให้เข้าใช้งานในระบบ				
๕	หน่วยงานมีการกำหนดแนวปฏิบัติสำหรับผู้ใช้งานเกี่ยวกับวิธีการกำหนดรหัสที่ดี การใช้รหัสผ่าน และการเปลี่ยนรหัสผ่าน				
๖	หน่วยงานมีการควบคุมและจำกัดสิทธิดังนี้ หรือไม่ - มีเอกสารแสดงการกำหนดสิทธิ (ตารางกำหนดสิทธิ) - ไม่มีการสร้าง User ร่วม - สิทธิที่กำหนดให้แต่ละกลุ่มชัดเจนและเหมาะสม				
๗	กระบวนการให้รหัสผ่าน ได้รับความเห็นชอบจากผู้บริหารและเป็นไปตามเงื่อนไขที่ฝ่ายบริหารกำหนดหรือไม่				
๘	หน่วยงานมีการดำเนินการเพิกถอนรหัสตามเงื่อนไขที่กำหนดหรือไม่				
๙	หน่วยงานมีการกำหนดเงื่อนไขให้ผู้ใช้งานเก็บรหัสไว้เป็นความลับหรือไม่				
๑๐	การทบทวนสิทธิเข้าถึงของผู้ใช้งาน มีการดำเนินการอย่างต่อเนื่องเป็นระยะ โดยมีการกำหนดระยะเวลาในการทบทวนที่แน่นอนหรือไม่				

ลำดับ	วิธีการตรวจสอบ	ผลตรวจสอบ			หมายเหตุ
		ใช่/มีการปฏิบัติ ๑ คะแนน	ใช่/มีบางส่วน ๐.๕ คะแนน	ไม่ใช่/ไม่มีการปฏิบัติ ๐ คะแนน	
การกำหนดหน้าที่ความรับผิดชอบ					
๑๑	หน่วยงานมีการกำหนดแนวปฏิบัติสำหรับผู้ใช้งานเกี่ยวกับวิธีการกำหนดรหัสผ่านที่ดี การใช้รหัสผ่าน และการเปลี่ยนรหัสผ่าน				
๑๒	ผู้ใช้งานรับทราบแนวปฏิบัติเกี่ยวกับรหัส ผ่านช่องทางดังนี้ - เผยแพร่ทาง Website - จัดอบรมให้ความรู้ - หนังสือเวียน - วิธีอื่นๆ ระบุ.....				
๑๓	หน่วยงานกำหนดข้อปฏิบัติสำหรับผู้ใช้งานเกี่ยวกับการป้องกันสารสนเทศ ขณะไม่มีผู้ใช้งานหรือไม่				
๑๔	หน่วยงานมีการกำหนดข้อปฏิบัติสำหรับผู้ใช้งานเกี่ยวกับการควบคุมข้อมูล สื่อ และสินทรัพย์ด้านสารสนเทศหรือไม่				
๑๕	หน่วยงานมีการกำหนดข้อปฏิบัติและหลักเกณฑ์สำหรับการเข้าถึงข้อมูลที่เป็นความลับและข้อมูลที่สำคัญของหน่วยงานหรือไม่				
การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน					
๑๖	หน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการคัดเลือกระบบสารสนเทศหรือไม่				
๑๗	หน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการจัดทำระบบสำรองหรือไม่				
๑๘	ระบบที่หน่วยงานจัดทำกำหนดให้มีการคืนและรายงานผลได้				
๑๙	ทุกระบบที่จัดทำสำรองมีการรายงานผลการสำรองหรือไม่				
๒๐	หน่วยงานมีการเตรียมแผนการเตรียมความพร้อมกรณีฉุกเฉิน ดังนี้ - กรณีไม่สามารถดำเนินงานด้วยระบบอิเล็กทรอนิกส์ได้ - กรณีที่ Site หลักไม่ทำงาน - มีการกำหนดแผนระยะสั้น - มีการกำหนดแผนระยะยาว - มีการทบทวนแผน ๓ เดือนครั้ง				
๒๑	หน่วยงานมีการกำหนดหน้าที่ความรับผิดชอบของบุคลากรดังนี้ - ด้านระบบสารสนเทศ - ด้านระบบสำรอง - ด้านการจัดทำแผนและทบทวนแผน				
๒๒	หน่วยงานจัดให้มีการทดสอบระบบให้อยู่ในสภาพพร้อมใช้งานดังนี้ หรือไม่ - ระบบสารสนเทศ - ระบบสำรอง - แผนฉุกเฉิน				ทดสอบครั้งสุดท้ายเมื่อ ....

ลำดับ	วิธีการตรวจสอบ	ผลตรวจสอบ			หมายเหตุ
		ใช่/มีการปฏิบัติ ๑ คะแนน	ใช่/มีบางส่วน ๐.๕ คะแนน	ไม่ใช่/ไม่มีการปฏิบัติ ๐ คะแนน	
	รวม				
	ผลรวมคะแนน				
	(ผลรวมคะแนน x ๕) / ๒๒ จำนวนข้อทั้งหมด				
	คิดเป็นร้อยละ (ผลรวมคะแนน x ๑๐๐) / ๒๒ จำนวนข้อทั้งหมด				

สรุปผลการตรวจสอบ

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

ลงชื่อ.....ผู้ตรวจสอบ
(.....)
วันที่.....

ลงชื่อ.....ผู้สอบทาน
(.....)
วันที่.....

มหาวิทยาลัยราชภัฏอุตรดิตถ์
สำนักงานตรวจสอบภายใน

รหัสกระดาษทำการ IC ๐๒๘/๒๕๖๙

แบบประเมินการควบคุมภายใน
ด้านระบบเทคโนโลยีสารสนเทศ

หน่วยรับตรวจ.....

เกณฑ์การให้คะแนน

๑ คะแนน = เพียงพอ
๐.๕๐ คะแนน = พอใช้
๐ คะแนน = ต้องปรับปรุง

ลำดับ	วิธีการตรวจสอบ	ผลการประเมิน			หมายเหตุ
		เพียงพอ ๑ คะแนน	พอใช้ ๐.๕ คะแนน	ต้องปรับปรุง ๐ คะแนน	
การควบคุมทั่วไป					
๑	มีการกำหนดนโยบายในการใช้ข้อมูลสารสนเทศที่ชัดเจนว่าใครต้องการเข้าถึงข้อมูลอะไร เมื่อไหร่ ในระบบงานใด				
๒	มีการกำหนดการให้สิทธิในการเข้าถึงข้อมูล				
๓	มีการแบ่งแยกหน้าที่งานในระบบสารสนเทศ ดังนี้หรือไม่ ■ มีการแยกหน้าที่การพัฒนาระบบออกจากผู้ปฏิบัติการคอมพิวเตอร์ ■ ผู้บริหารฐานข้อมูล (Database Administrator)ต้องไม่ทำหน้าที่อื่น ■ มีการแยกหน้าที่ผู้พัฒนาระบบออกจากผู้ดูแลบำรุงรักษาระบบ				
การควบคุมโครงการพัฒนาระบบสารสนเทศ					
๔	มีการกำหนดแผนระยะยาว				
๕	มีการกำหนดแผนงานพัฒนาระบบ				
๖	มีการกำหนดการประมวลผลข้อมูล				
๗	มีการมอบหมายหน้าที่และความรับผิดชอบ				
๘	มีการประเมินผลงานระหว่างการดำเนินโครงการ				
๙	มีการสอบทานภายหลังการติดตั้งระบบและนำระบบมาใช้งาน				
๑๐	มีการวัดผลการดำเนินงานของระบบ				
การควบคุมการเปลี่ยนแปลงแก้ไขระบบ					
๑๑	มีการกำหนดระเบียบวิธีปฏิบัติในการแก้ไขระบบไว้เป็นลายลักษณ์อักษร				
๑๒	มีการศึกษาผลกระทบต่างๆ ในการเปลี่ยนแปลงแก้ไขระบบ				
๑๓	มีการทดสอบระบบที่แก้ไขแล้วก่อนนำไปใช้				
๑๔	มีการจัดทำเอกสารคู่มือประกอบการแก้ไขระบบ				
๑๕	มีการประเมินผลและสอบทานระบบงานภายหลังเริ่มใช้				
การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์					
๑๖	มีการประมวลผลข้อมูลของระบบงานต่างๆ ให้มีความถูกต้องครบถ้วน				
๑๗	มีการกู้ระบบและการสำรองข้อมูล				

ลำดับ	วิธีการตรวจสอบ	ผลการประเมิน			หมายเหตุ
		เพียงพอ ๑ คะแนน	พอใช้ ๐.๕ คะแนน	ต้องปรับปรุง ๐ คะแนน	
๑๘	มีการจัดการปัญหาของระบบ เช่น จัดทำแผนสำรอง				
การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์					
๑๙	มีสถานที่จัดเก็บอุปกรณ์คอมพิวเตอร์มิดชิด ไม่มีอากาศร้อน ชื้น และแม่เหล็ก				
๒๐	มีการรักษาความปลอดภัยหนาแน่น				
๒๑	มีการกำหนดการเข้าออกได้เฉพาะผู้เกี่ยวข้อง				
๒๒	มีการกำหนดนโยบายการรักษาความปลอดภัยของระบบที่ชัดเจน				
๒๓	มีการติดตั้งระบบเตือนภัยกรณีมีผู้บุกรุก				
๒๔	มีการจำกัดให้ใช้โทรศัพท์เฉพาะเรื่องที่เกี่ยวกับงาน				
๒๕	มีการติดอุปกรณ์ป้องกันเครื่องคอมพิวเตอร์				
การควบคุมการเข้าถึงข้อมูล					
๒๖	มีการกำหนดผู้ใช้ (User Views or Subschema)				
๒๗	มีการกำหนดสิทธิ (ตารางกำหนดสิทธิ) ในการเข้าถึงฐานข้อมูล (Database Authorization Table)				
๒๘	มีการกำหนดการเข้ารหัสข้อมูล (Data Encryption)				
๒๙	มีการควบคุมเข้าถึงระบบงาน ดังนี้ ▪ การพิสูจน์ตัวจริงโดยการกำหนดรหัสผ่าน (Password) ▪ การกำหนดสิทธิ์ (Authorization) ▪ การบันทึกกิจกรรมต่างๆ ในระบบเพื่อการตรวจสอบ (Audit Logging)				
การควบคุมระบบงาน					
๓๐	มีการควบคุมการนำเข้าข้อมูล ดังนี้ ▪ การควบคุมเกี่ยวกับงานจัดทำข้อมูลก่อนป้อนเข้าสู่ระบบคอมพิวเตอร์ ▪ การเตรียมข้อมูลนำเข้า ▪ การป้องกันข้อผิดพลาด ▪ การค้นหาข้อผิดพลาดและการแก้ไขข้อผิดพลาด เช่น การตรวจสอบตัวเลขตรวจสอบ (Check digit) ว่าเป็นตัวเลขที่ถูกหรือไม่ (เลขรหัสวัสดุ และรหัสครุภัณฑ์)				
๓๑	มีการควบคุมการทำรายการป้อนเข้าสู่ระบบงาน โดยข้อมูลที่ป้อนเข้าสู่ระบบจะต้องถูกหลักเกณฑ์ในการทำรายการ รวมถึงการกระทบยอดข้อมูลนำเข้าเพื่อพิสูจน์ความถูกต้อง				
๓๒	มีการควบคุมการสื่อสารข้อมูลให้มีความถูกต้องและครบถ้วน ซึ่งจะต้องคำนึงถึง Hardware และ Software ที่ใช้ในการสื่อสารข้อมูล การมอบอำนาจ				
๓๓	มีการควบคุมการประมวลผลด้วยคอมพิวเตอร์ ให้มีความแม่นยำ ถูกต้อง และครบถ้วนเป็นไปตามหลักเกณฑ์การใช้แฟ้มข้อมูล การชี้แนะให้เห็นข้อผิดพลาด และการรายงาน				
๓๔	มีการควบคุมการจัดเก็บข้อมูลไว้ในระบบ เช่น การกำหนดสิทธิการใช้ข้อมูล การรักษาความปลอดภัย การแก้ไขข้อผิดพลาด การสำรองข้อมูล และการกำหนดอายุการจัดเก็บแฟ้มข้อมูล				

ลำดับ	วิธีการตรวจสอบ	ผลการประเมิน			หมายเหตุ
		เพียงพอ ๑ คะแนน	พอใช้ ๐.๕ คะแนน	ต้องปรับปรุง ๐ คะแนน	
๓๕	มีการควบคุมผลลัพธ์ การกระทบยอดข้อมูลนำเข้าและผลลัพธ์ เพื่อพิสูจน์ความถูกต้องด้วยระบบ Manual				
	รวม				
	ผลรวมคะแนน				
	(ผลรวมคะแนน x ๕) / ๓๕ จำนวนข้อทั้งหมด				
	คิดเป็นร้อยละ (ผลรวมคะแนน x ๑๐๐) / ๓๕ จำนวนข้อทั้งหมด				

สรุปผลการประเมิน

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

ลงชื่อ.....ผู้ประเมิน

(.....)

วันที่.....

มหาวิทยาลัยราชภัฏอุตรดิตถ์
สำนักงานตรวจสอบภายใน

รหัสกระดาษทำการ Gov ๐๒๘/๒๕๖๙

แบบประเมินการกำกับดูแล
ด้านระบบเทคโนโลยีสารสนเทศ

หน่วยรับตรวจ.....

เกณฑ์การให้คะแนน

๑ คะแนน = เพียงพอ
๐.๕๐ คะแนน = พอใช้
๐ คะแนน = ต้องปรับปรุง

ลำดับ	วิธีการตรวจสอบ	ผลการประเมิน			หมายเหตุ
		เพียงพอ ๑ คะแนน	พอใช้ ๐.๕ คะแนน	ต้องปรับปรุง ๐ คะแนน	
ผู้บังคับบัญชา					
๑	มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security Policy) และระเบียบวิธีปฏิบัติที่ชัดเจน เพื่อให้บุคลากรและนักศึกษาปฏิบัติตามอย่างเคร่งครัด				
๒	มีการอนุมัตินโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี และจัดให้มีการกำหนดขั้นตอน วิธีปฏิบัติงานและกระบวนการที่เกี่ยวข้องให้เป็นไปตามนโยบายดังกล่าว				
๓	มีการสื่อสารนโยบายการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศ รวมทั้งขั้นตอน วิธีการปฏิบัติงานและกระบวนการที่เกี่ยวข้อง ให้บุคลากรรับทราบ และสนับสนุนให้มีการปฏิบัติตามนโยบายดังกล่าว				
๔	มีการควบคุมดูแลให้การใช้งานระบบเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) และกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์				
๕	มีการประเมินและจัดการความเสี่ยงด้านเทคโนโลยี เช่น การป้องกันภัยคุกคามทางไซเบอร์ การสำรองข้อมูล และแผนกู้คืนระบบเมื่อเกิดเหตุฉุกเฉิน (Disaster Recovery Plan)				
๖	มีการจัดสรรทรัพยากรและงบประมาณให้สอดคล้องกับแผนยุทธศาสตร์ดิจิทัล เพื่อพัฒนาโครงสร้างพื้นฐานและบริการที่ตอบโจทย์การเรียนการสอน				
๗	มีการกำหนดทิศทางและงบประมาณในการจัดหา จัดซื้อ หรืออัปเกรดโครงสร้างพื้นฐาน (เช่น ระบบเครือข่าย Wi-Fi, เซิร์ฟเวอร์, ระบบคลาวด์) ให้สอดคล้องกับยุทธศาสตร์ของมหาวิทยาลัย				
๘	มีการบังคับใช้นโยบาย IT Security เพื่อป้องกันการรั่วไหลของข้อมูล เช่น ข้อมูลผลการเรียนของนักศึกษา งานวิจัย และประวัติบุคลากร ให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)				
๙	มีการกำกับดูแลระบบสนับสนุนการเรียนการสอนออนไลน์ ระบบทะเบียนนักศึกษาและจัดการทีมช่างเทคนิคหรือ Helpdesk เพื่อแก้ปัญหาหน้างานให้แก่ผู้ใช้งาน				

ลำดับ	วิธีการตรวจสอบ	ผลการประเมิน			หมายเหตุ
		เพียงพอ ๑ คะแนน	พอใช้ ๐.๕ คะแนน	ต้องปรับปรุง ๐ คะแนน	
๑๐	มีการดูแลและติดตามเพื่อให้มั่นใจว่ากิจกรรมในการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศมีการดำเนินการอย่างมีประสิทธิภาพและมีประสิทธิผล				
๑๑	มีการทบทวนหรือปรับปรุงนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีอย่างน้อยปีละหนึ่งครั้ง				
	รวม				
	ผลรวมคะแนน				
	(ผลรวมคะแนน x ๕) / ๑๑ จำนวนข้อทั้งหมด				
	คิดเป็นร้อยละ (ผลรวมคะแนน x ๑๐๐) / ๑๑ จำนวนข้อทั้งหมด				

สรุปผลการประเมิน

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

ลงชื่อ.....ผู้ประเมิน

(.....)

วันที่.....

มหาวิทยาลัยราชภัฏอุตรดิตถ์
สำนักงานตรวจสอบภายใน

รหัส Risk ๐๒๘/๒๕๖๙

แบบประเมินความเสี่ยง
ด้านระบบเทคโนโลยีสารสนเทศ

หน่วยรับตรวจ.....

ขั้นตอน/กระบวนการ/ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	ระดับคะแนน	ระดับความเสี่ยง
๑. การเข้าถึงข้อมูลโดยบุคคลอื่น	การให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน หรือมีการพยายามเข้าถึงระบบสารสนเทศโดยผู้ไม่มีสิทธิ				
	การเข้าถึงข้อมูล เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต				
๒. ข้อมูลสูญหาย เสียหาย ไม่ครบถ้วน	มีความผิดพลาดในการสำรองข้อมูล หรือระบบสำรองข้อมูลล้มเหลว หรือไม่สามารถกู้คืนข้อมูลได้ในยามฉุกเฉิน				
	การไม่สามารถเข้าถึงข้อมูลที่จำเป็นได้ การขาดการบริหารจัดการข้อมูลที่เหมาะสมทำให้ไม่สามารถนำข้อมูลที่เก็บไว้มาใช้งานได้				
๓. เกิดภัยคุกคามทางไซเบอร์	การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ การถูกแฮก การโจมตีด้วยมัลแวร์ สปายแวร์ การถูกขโมยข้อมูลสำคัญโดยผู้ไม่หวังดี				
๔. การทำงานของระบบขัดข้อง	ระบบล่ม ฮาร์ดแวร์เสียหาย หรือปัญหาซอฟต์แวร์ผิดพลาด จนทำให้งานหยุดชะงัก				
	โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง หรือความผิดพลาดเกิดจากการเขียนโปรแกรม และถูกผู้ไม่หวังดีทำลายระบบ เป็นต้น				
	การเคลื่อนย้ายตัวเครื่อง อุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม				
๕. การรั่วไหลหรือการสูญหายของข้อมูล	ฐานข้อมูลต่างๆ ในระบบสารสนเทศเสียหาย สูญหาย ไม่ครบถ้วน ข้อมูลถูกทำลายจากผู้บุกรุกข้อมูล การโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล				
๖. การละเลยไม่ปฏิบัติตามนโยบายและแผนด้านเทคโนโลยีสารสนเทศ	บุคคลากรขาดความรู้ความเข้าใจเกี่ยวกับกฎหมาย หลักเกณฑ์ ประกาศ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งกฎหมายคุ้มครองข้อมูลส่วนบุคคล				
๗. ขาดแคลนบุคลากรผู้ปฏิบัติงานด้านสารสนเทศ	จำนวนบุคลากรที่ไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ				

ขั้นตอน/กระบวนการ/ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	ระดับคะแนน	ระดับความเสี่ยง
๘. เกิดภัยธรรมชาติ	เหตุการณ์ภัยธรรมชาติ เช่น แผ่นดินไหว วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้				
	การไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย (Network Operation Center) และการก่อการร้าย				

สรุปผลการประเมิน

.....

.....

.....

.....

.....

.....

.....

.....

ลงชื่อ.....ผู้ประเมิน

(.....)

วันที่.....

๑. เกณฑ์การประเมินความเสี่ยง

๑.๑ โอกาสที่จะเกิดความเสี่ยง (likelihood)

คะแนน	โอกาสที่จะเกิดความเสี่ยง	เชิงคุณภาพ	เชิงปริมาณ
๕	สูงมาก	มีโอกาสเกิดขึ้นเป็นประจำหรือเกิดต่อเนื่องตลอดเวลา	๕ ครั้ง/ปี
๔	สูง	มีโอกาสเกิดขึ้นบ่อยครั้ง	๔ ครั้ง/ปี
๓	ปานกลาง	มีโอกาสเกิดขึ้นบางครั้ง	๓ ครั้ง/ปี
๒	ต่ำ	มีโอกาสเกิดขึ้นน้อย แต่มีโอกาสเป็นไปได้	๒ ครั้ง/ปี
๑	ต่ำมาก	แทบไม่เคยเกิดขึ้น หรือมีโอกาสเกิดขึ้นน้อยมาก	ไม่เกิน ๑ ครั้ง/ปี

๑.๒ ระดับความรุนแรงของผลกระทบความเสี่ยง (Impact)

คะแนน	ผลกระทบ/ความรุนแรง/ความเสียหาย	ด้านการดำเนินงาน	ด้านการเงิน
๕	สูงมาก	ระบบหยุดทำงานถาวรหรือเสียหายหนักมาก ข้อมูลสูญหายถาวร	มูลค่ามากกว่า ๑๐ ล้านบาท
๔	สูง	ระบบหลักล่ม ไม่สามารถให้บริการได้ กระทบผู้ใช้งานจำนวนมาก หรือข้อมูลสำคัญรั่วไหล	มูลค่า ๕ ล้านบาท – ๑๐ ล้านบาท
๓	ปานกลาง	ระบบหยุดชะงักเป็นชั่วโมง กระทบต่อหน่วยงานหรือผู้ใช้งานบางส่วน	มูลค่า ๑ ล้านบาท – ๕ ล้านบาท
๒	ต่ำ	การทำงานติดขัดชั่วคราว สามารถกู้คืนได้ทันที	มูลค่า ๕ แสนบาท – ๑ ล้านบาท
๑	ต่ำมาก	กระทบผู้ใช้กลุ่มเล็ก แก้ไขได้รวดเร็ว ไม่เสียหายร้ายแรง	มูลค่าน้อยกว่า ๕ แสนบาท

๒. การจัดลำดับความเสี่ยง

ระดับความเสียง	ระดับความเสียง	เกณฑ์การประเมิน
สูงมาก	๒๐-๒๕	ไม่สามารถยอมรับได้ และต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ในทันที
สูง	๑๕-๑๖	ไม่สามารถยอมรับได้ และต้องจัดการความเสี่ยงให้อยู่ในระดับความเสี่ยงที่ยอมรับได้โดยเร็ว
ปานกลาง	๕-๑๒	ยอมรับได้โดยต้องมีการติดตามเฝ้าระวังอย่างสม่ำเสมอเพื่อให้มั่นใจว่าระดับความเสี่ยงไม่ได้เพิ่มขึ้น
ต่ำ	๓-๔	ยอมรับได้โดยอาจมีการติดตามเฝ้าระวังเป็นระยะเพื่อให้มั่นใจว่าระดับความเสี่ยงไม่ได้เพิ่มขึ้น
ต่ำมาก	๑-๒	ยอมรับได้โดยไม่ต้องมีการจัดการเพิ่มเติม