รายการตรวจสอบนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีสุรนารี

(ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม รวมทั้ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

หน่วยงานหลัก สำนักวิชาวิทยาศาสตร์ **ฝ่าย/งาน** .....

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
1	มีการจัดทำนโยบายหรือข้อปฏิบัติเป็นลายลักษณ์อักษร						- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
2	มีนโยบายเกี่ยวกับการเข้าถึงระบบสารสนเทศ/ระบบเครือข่าย / ระบบปฏิบัติการ / โปรแกรมประยุกต์ (Application)						- ต้องมีการจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศอย่างน้อยครอบคลุม 4 เรื่อง ระบบสารสนเทศ/ ระบบเครือข่าย / ระบบปฏิบัติการ /

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติ
							โปรแกรมประยุกต์ (Application)
3	มีการกำหนดนโยบายเกี่ยวข้องกับการจัดทำระบบสำรอง โดยมีเนื้อหาอย่างน้อย 2 เรื่อง (1) การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน (2) การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน						- ต้องมีการจัดทำนโยบายเกี่ยวกับการสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน และการจัดทำแผนเตรียมความพร้อม
4	มีการกำหนดนโยบายให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศไว้ด้วย						- ต้องมีการจัดทำนโยบายเกี่ยวกับการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ
5	มีการประกาศเผยแพร่นโยบายให้ผู้ใช้งานทราบทาง Website และ/หรือแจ้งเวียน						- ต้องมีการประกาศนโยบาย ซึ่งลงนามโดยผู้บริหารของหน่วยงาน พร้อมทั้งให้ระบุวิธีประกาศและควรระบุไว้เป็นส่วนหนึ่งของนโยบาย - กรณีหน่วยงานมีผู้รับบริหารทางอิเล็กทรอนิกส์ ต้องประกาศนโยบายและแนวปฏิบัติฯ ให้ผู้บริการทราบด้วย - หากหน่วยงานเห็นว่าเป็นความลับ แยกส่วนที่สามารถเปิดเผยได้ขึ้นอีกฉบับ เพื่อแจ้งให้ผู้บริการทราบด้วย
6	หน่วยงานมีการกำหนดผู้รับผิดชอบตามนโยบายที่ชัดเจน						- ต้องมีการกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติที่

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติ
							กำหนดผู้รับผิดชอบ ชัดเจน โดยเชื่อมโยงทั้งบุคคล ตำแหน่ง และภารกิจที่รับผิดชอบ
7	หน่วยงานมีการทบทวนนโยบาย/ข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ โดยฉบับที่ใช้ในปัจจุบัน คือ ฉบับลงวันที่.....						- ต้องมีการกำหนดระยะเวลาในการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน ระบุมีความถี่อย่างไร

ข้อคิดเห็น_____

_____

ผู้ให้ข้อมูล (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

ผู้สอบทาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

หัวหน้าหน่วยงาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

มหาวิทยาลัยเทคโนโลยีสุรนารี

(ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560)

หน่วยงานหลัก **สำนักวิชาวิทยาศาสตร์** **ฝ่าย/งาน**

.....

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
1	มีการประกาศ ไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันเข้าถึงโดย โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน (ม.5)						
2	มีการประกาศ ผู้ล่วงรู้มาตรการป้องกันเข้าถึงระบบคอมพิวเตอร์ ไม่ให้เปิดเผยมาตรการป้องกันโดยมิชอบในประการที่น่าจะเกิด ความเสียหายแก่ผู้อื่น (ม.6)						
3	มีการประกาศ ไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบ ซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน (ม.7)						
4	มีการประกาศ ไม่ให้ผู้ใช้บริการกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่ง ข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้ บุคคลทั่วไปใช้ประโยชน์ (ม.8)						
5	มีการประกาศ ไม่ให้ผู้ใช้บริการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงหรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (ม.9)						

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
6	มีการประกาศ ไม่ให้ผู้ใช้บริการกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ (ม.10)						
7	มีการประกาศ ไม่ให้ผู้ใช้บริการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคล อื่นโดยปกติสุข (ม.11)						
8	มีการประกาศ ไม่ให้ผู้ใช้บริการกระทำโดยประการที่ น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือ ระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคง ปลอดภัยของประเทศชาติ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือการ บริการสาธารณะหรือเป็นการกระทำต่อข้อมูล คอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อ ประโยชน์สาธารณะ (ม.12)						
9	มีการประกาศไม่ให้ผู้ใช้บริการจำหน่วยหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม พ.ร.บ. คอมพิวเตอร์ (ม.11)						
10	มีการประกาศ ไม่ให้นำเข้าหรือสนับสนุนการนำเข้าข้อมูลเท็จ หรือลามก เผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ (ม.14 และ 15)						

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
11	มีการประกาศ ไม่ให้นำเข้าหรือเผยแพร่ หรือส่งต่อสู่ระบบคอมพิวเตอร์ ภาพของผู้อื่น และภาพนั้นเป็นภาพที่ เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการใด ๆ ที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง (ม.16)						
12	มีการประกาศ ห้ามเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลจราจรคอมพิวเตอร์ของผู้ใช้บริการให้แก่บุคคลใด ยกเว้นเพื่อประโยชน์ในการดำเนินคดี (ม.16)						
13	ฝ่าย IT มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ (ม.26)						- มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ตามที่กฎหมายกำหนด

ข้อคิดเห็น_____

_____

ผู้ให้ข้อมูล (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

ผู้สอบทาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

หัวหน้าหน่วยงาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

From SUT.IAU.IT.A3

รายการตรวจสอบการปฏิบัติตามพรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
มหาวิทยาลัยเทคโนโลยีสุรนารี

หน่วยงานหลัก สำนักวิชาวิทยาศาสตร์ **ฝ่าย/งาน**

.....

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
1	การสั่งการจากผู้บริหารให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562						- โครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล บทบาท และหน้าที่ความรับผิดชอบ
2	การศึกษาข้อมูล พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562						- มีความตระหนักในการปฏิบัติตามนโยบายและแนวปฏิบัติสำหรับการคุ้มครองข้อมูลส่วนบุคคล - มีความตระหนักรู้ในการให้ข้อมูลส่วนบุคคลแก่ผู้อื่นด้วยความระมัดระวัง และป้องกันมิให้มีการเปิดเผยโดยมิได้รับอนุญาต - มีความรู้ความเข้าใจในเรื่องการของการแจ้งเพื่อเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
							- มีความรู้ความเข้าใจ ในเรื่องการขอความยินยอม ก่อนเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่ - มีความรู้ความเข้าใจในสิทธิตามกฎหมาย คุ้มครองข้อมูลส่วนบุคคลหรือไม่
3	การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพื่อเก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล (ม. 19) ได้กระทำดังข้อต่อไปนี้						- มีการกำหนดขั้นตอนการปฏิบัติสำหรับการรับเรื่องการขอใช้สิทธิโดยเจ้าของข้อมูลส่วนบุคคล - กรณีมีการปฏิเสธการร้องขอใช้สิทธิ มีการบันทึกเหตุผลของการปฏิเสธไว้หรือไม่ - ได้กำหนดให้มีวิธีการอย่างเป็นรูปธรรมสำหรับการตรวจสอบและทำลายข้อมูลส่วนบุคคลเมื่อพ้นระยะเวลาจัดเก็บ - มีการดูแลคุณภาพของข้อมูล
	3.1 ทำเป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์						
	3.2 แจ้งวัตถุประสงค์ที่ต้องขอความยินยอม						
4	ผู้เก็บข้อมูลส่วนบุคคล ต้องรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ที่แจ้งไว้ตามข้อ 3.2 เท่านั้น (ม.21)						
5	การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ที่มิใช่จากเจ้าของข้อมูลโดยตรง (ม.25)						
6	หน่วยงานได้มีมาตรการหรือแนวทางในการรักษาความปลอดภัยของข้อมูล						- กำหนดให้มีมาตรการหรือแนวทางที่เหมาะสมกับข้อมูล รวมทั้งมีความรู้ความเข้าใจนโยบายและขั้นตอน
7	การเตรียมความพร้อมระดับองค์กร 15 ด้าน						
	7.1 มีการกำหนดหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจน						- โครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล บทบาท และหน้าที่ความรับผิดชอบ

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของ
							- มีการบันทึกกิจกรรมการประมวลผลของข้อมูลส่วนบุคคล - มีความตระหนักรู้ ความเข้าใจตลอดจนความตระหนักในหน้าที่และความรับผิดชอบ
	7.2 การจัดทำสัญญาหรือข้อตกลงการประมวลผลกับผู้ใช้งานภายนอกมีการกำหนดหรือระบุประเด็นดังกล่าว (Third Party Access Management)						- กำหนดให้ผู้ให้บริการภายนอกปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด - กำหนดวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลลงในสัญญาหรือข้อตกลงการจ้างงานให้ชัดเจน พร้อมทั้งกำหนดให้ปฏิบัติตามวัตถุประสงค์การประมวลผลที่กำหนดไว้เคร่งครัด
	7.3 มีการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน						- มีการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่มีประเด็นครบถ้วน
	7.4 มีการบันทึกกิจกรรมการประมวลผล ROPA						- มีการทบทวนและปรับปรุงบันทึกกิจกรรมการประมวลผลอย่างสม่ำเสมอ
	7.4.1 การเลือกฐานทางกฎหมายเพื่อเก็บรวบรวมข้อมูลส่วนบุคคล						- มีการกำหนดฐานการประมวลผลหรือฐานทางกฎหมายของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
	7.4.2 มีการดำเนินการในการขอความยินยอมสำหรับการใช้ข้อมูลที่มีความอ่อนไหว						- มีการจัดเก็บข้อมูลที่มีความอ่อนไหวตามที่กฎหมาย เช่น ศาสนา เชื้อชาติ ประวัติสุขภาพ

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
							หรือการรักษาความลับ หรือข้อมูลที่ คกก.คุ้มครองข้อมูลส่วนบุคคลประกาศเพิ่มเติม
	7.4.3 การขอความยินยอมสำหรับการใช้ข้อมูลส่วนบุคคลของผู้เยาว์ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ						- มีความรู้ ความเข้าใจเกี่ยวกับประเภทของบุคคลดังนี้หรือไม่ ผู้เยาว์ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ ปละมีการขอความยินยอมก่อนการใช้ข้อมูลของบุคคลเหล่านี้
	7.4.4 การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับการจัดเก็บรวบรวมข้อมูลส่วนบุคคล						- มีการกำหนดหัวข้อตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้หรือไม่ (ในเอกสารแจ้งเก็บรวบรวมข้อมูลส่วนบุคคล)
	7.5 มีการประเมินผลกระทบด้านความคุ้มครองข้อมูลส่วนบุคคล						- มีการประเมินความเสี่ยหรือประเมินผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลหรือไม่ มีแผนการจัดการความเสี่ยงหรือไม่
	7.6 มีการดำเนินการต่างๆ สำหรับการใช้และเปิดเผยข้อมูลส่วนบุคคล						- มีการใช้ข้อมูลส่วนบุคคลตามประสงค์ที่กำหนดไว้เท่านั้น - การเปิดเผยเพื่อให้เป็นไปตามของการประมวลที่กำหนดไว้ วัตถุประสงค์ที่กำหนดไว้ในสัญญาหรือข้อตกลงตามที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
บ	7.7 มีหลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปต่างประเทศหรือองค์การระหว่างประเทศที่เกี่ยวข้อง						- ประเทศหรือองค์การระหว่างประเทศที่ได้รับข้อมูลส่วนบุคคลที่มีมาตรการในการคุ้มครองขอมูลส่วนบุคคล
	7.7.1 กรณีเป็นหน่วยงานในต่างประเทศที่มีอำนาจหน้าที่ที่เกี่ยวข้องร้องขอให้จัดส่ง						- มีการระบุวัตถุประสงค์ของการจัดส่งข้อมูล - มีการดำเนินการพิสูจน์ตัวตนหน่วยงาน - การแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบเกี่ยวกับการจัดส่งข้อมูลนั้น
	7.8 มีการร้องขอข้อมูลจากหน่วยงนภายนอก						- หน่วยงานภายนอกที่ร้องขอข้อมูลส่วนข้อมูลส่วนบุคคลเป็นหน่วยงาน - การแจ้งให้ทราบหรือพิจารณาการร้องขอข้อมูลจากหน่วยงานภายนอก
	7.9 การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล						- มีการแจ้งบันทึกการแจ้งเหตุละเมิดความมั่นคงปลอดภัยข้อมูลส่วนบุคคลไว้หรือไม่ บันทึกรายละเอียดของการดำเนินการไว้หรือไม่ - มีการวิเคราะห์หาสาเหตุที่เกิดขึ้นและแนวทางนการรับมือกับเหตุที่เกิดขึ้น

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
บ	7.10 การจัดเก็บรักษาและระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคล						
	7.10.1 การจัดเก็บและระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคล						- ข้อมูลที่เก็บรักษาไว้ จัดเก็บไว้เท่าที่จำเป็นหรือไม่ - ให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบในช่วงที่เก็บรวบรวม - มีการกำหนดระยะเวลาสำหรับการตรวจสอบเพื่อทำลายข้อมูลส่วนบุคคลหรือไม่
	7.10.2 การจำหน่ายออกและลบทำลายข้อมูลส่วนบุคคล						- เมื่อครบระยะการจัดเก็บที่ได้แจ้งให้เจ้าข้อมูลได้รับทราบ หรือตามที่ระบุไว้ในสัญญา - เมื่อครบระยะเวลาการจัดเก็บที่กำหนดไว้

ข้อคิดเห็น_____

_____

ผู้ให้ข้อมูล (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

ผู้สอบทาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

หัวหน้าหน่วยงาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

From SUT.IAU.IT.B1

รายการตรวจสอบการควบคุมการเข้าถึงและควบคุมการใช้งาน
มหาวิทยาลัยเทคโนโลยีสุรนารี

หน่วยงานหลัก สำนักวิชาวิทยาศาสตร์ **ฝ่าย/งาน**

.....

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
1	การควบคุมทางกายภาพ						
	1.1 พื้นที่ของหน่วยงานเป็นพื้นที่เฉพาะสำหรับ บุคคลที่ได้รับอนุญาตเท่านั้น						ต้องมีข้อปฏิบัติ/หลักเกณฑ์ที่เกี่ยวข้องกับการป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต
	1.2 หน่วยงาน รวมถึงห้องเก็บสารสนเทศภายใน และห้องทำงานปิดล็อก เมื่อไม่มีการใช้งาน						
	1.3 หน่วยงานมีการควบคุมเพื่อป้องกันภัย จากขโมย						
	1.4 หน่วยงานมีการควบคุมเพื่อป้องกันภัย จากไฟไหม้						
	1.5 หน่วยงานมีการควบคุมเพื่อป้องกันภัย จากน้ำท่วม						
	1.6 มีนโยบายไม่ให้กิน ดื่ม และสูบบุหรี่ภายในหน่วยงาน						
	1.7 มีอุปกรณ์ UPS สำรองไฟ เพื่อป้องกันข้อมูลสารสนเทศเสียหายกรณีไฟฟ้าดับ/ตก/ไม่สม่ำเสมอ						
	1.8 อุปกรณ์ UPS มีระยะเวลาการใช้งานเพียงพอ ที่จะสำรองข้อมูลได้						
2	มีการกำหนดสิทธิในการเข้าถึงสอดคล้องกับการอนุญาตและการมอบอำนาจ						ต้องมีขั้นตอนปฏิบัติที่แสดงถึงการกำหนด

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
							สิทธิ เช่น มีสิทธิอย่างไร มีการอนุญาตอย่างไร หรือมีการมอบอำนาจในเรื่องใดบ้าง
3	มีการดำเนินการเกี่ยวกับข้อมูลและสารสนเทศต่างๆ ในเรื่องต่อไปนี้						ต้องมีรายละเอียดที่แสดงถึงการกำหนดในเรื่องต่อไปนี้ครบทุกประเด็น - ระบุประเภทของข้อมูลให้ชัดเจน - ระบุการจัดลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลให้ชัดเจน - ระบุลำดับชั้นการเข้าถึงว่าใครเป็นผู้มีสิทธิหรือไม่มีสิทธิในการเข้าถึงข้อมูลได้ - ระบุ เวลา หากมีการกำหนดเป็นช่วงวันเวลาที่สามารถเข้าถึงได้
	3.1 จัดประเภทของข้อมูลและสารสนเทศ						
	3.2 จัดชั้นความลับของข้อมูลและสารสนเทศ						
	3.3 จัดชั้นการเข้าถึง						
	3.4 กำหนดเวลาในการเข้าถึง						
	3.5 กำหนดช่องทางในการเข้าถึง						

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
							- รวมถึงระบุช่องทางที่สามารถเข้าถึงข้อมูลได้

ข้อคิดเห็น_____

_____

ผู้ให้ข้อมูล (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

ผู้สอบทาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

หัวหน้าหน่วยงาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

From SUT.IAU.IT.B2

รายการตรวจสอบการบริหารจัดการการเข้าถึงผู้ใช้งาน
มหาวิทยาลัยเทคโนโลยีสุรนารี

(ตรวจสอบความพร้อมใช้งานของระบบสารสนเทศฯ)

หน่วยงานหลัก ____**สำนักวิชาวิทยาศาสตร์**____ **ฝ่าย/งาน**

.....

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ผลคะแนนประเมิน
		ใช่	ใช่บางส่วน	ไม่ใช่			
1	หน่วยงานจัดให้มีการให้ความรู้ ความเข้าใจกับ กับผู้ปฏิบัติงานอย่างต่อเนื่อง โดยวิธีการ ต่อไปนี้						สร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตะหนัก ต้องมีการกำหนดขั้นตอนการปฏิบัติ 2 เรื่อง - การบริหารจัดการการเข้าถึงของผู้ใช้งาน - การฝึกอบรมหลักสูตรการสร้างความตะหนักเรื่องความมั่นคงปลอดภัยไซเบอร์
	1.1 เผยแพร่ทาง Website						
	1.2 จัดอบรม						
	1.3 วิธีอื่น ๆ ระบุ.....						
2	มีการให้ลงทะเบียนสำหรับผู้เข้าใช้งาน					-	- ต้องแสดงขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน - ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ในการอนุญาติเข้าถึงระบบสารสนเทศ - ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ
	2.1 มีข้อกำหนดในการลงทะเบียน						
	2.2 มีข้อกำหนดและหลักเกณฑ์ในการอนุญาตให้ใช้งาน						
	2.3 มีข้อกำหนดและหลักเกณฑ์ในการยกเลิก/เพิกถอนการ อนุญาตให้เข้าใช้งานในระบบ						

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ผลคะแนนประเมิน
		ใช่	ใช่บางส่วน	ไม่ใช่			
3	มีการควบคุมและจำกัดสิทธิ					-	- ต้องมีรายละเอียดแสดงถึงการควบคุมสิทธิการใช้งาน - ต้องแสดงกระบวนการในการมอบหมายกำหนดสิทธิใช้งานให้แก่ผู้ใช้งาน - ต้องมีการกำหนดระดับสิทธิในการเข้าถึงระบบงานที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็น
	3.1 มีเอกสารแสดงการกำหนดสิทธิ (ตารางกำหนดสิทธิ)						
	3.2 ไม่มีการใช้ User ร่วมกัน						
	3.3 สิทธิที่กำหนดในแต่ละกลุ่มชัดเจนและเหมาะสม						
4	มีการกำหนดเงื่อนไขการให้รหัสและเพิกถอนการให้รหัสโดยผ่านกระบวนการด้านการบริหาร					-	- ต้องมีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
	4.1 กระบวนการให้รหัสผ่านความเห็นชอบตามเงื่อนไขที่ฝ่ายบริหารกำหนด						
	4.2 มีการดำเนินการเพิกถอนรหัสตามเงื่อนไขที่กำหนด						
	4.3 มีการกำหนดเงื่อนไขให้ผู้ใช้งานเก็บรหัสไว้เป็นความลับ						
5	มีการทบทวนสิทธิเข้าถึงของผู้ใช้งานเป็นระยะ ๆ โดยกำหนดระยะเวลาในการทบทวนที่แน่นอน หรือไม่						
6	หน่วยงานสามารถระบุอุปกรณ์บนเครือข่ายได้						

ข้อคิดเห็น_____

_____

ผู้ให้ข้อมูล (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

ผู้สอบทาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

หัวหน้าหน่วยงาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

From SUT.IAU. IT.B3

รายการตรวจสอบการเข้าถึงโปรแกรมประยุกต์ หรือ Application และสารสนเทศ มหาวิทยาลัยเทคโนโลยีสุรนารี

(ตรวจสอบความพร้อมใช้งานของระบบสารสนเทศฯ)

หน่วยงานหลัก **สำนักวิชาวิทยาศาสตร์** **ฝ่าย/งาน**

.....

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
1	หน่วยงานมีการจำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์จากผู้ใช้งาน 1.1 หน่วยงานกำหนดการจำกัดหรือการควบคุมการใช้งาน โปรแกรมอรรถประโยชน์						- ต้องมีขั้นตอนปฏิบัติที่แสดงถึงการควบคุมการเข้าถึงข้อมูลหรือการเข้าใช้ของผู้ใช้งาน หรือบุคลากร โดยใช้

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
2	หน่วยงานมีการจำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์จากบุคลากรฝ่ายสนับสนุน						สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่กำหนดไว้ - ต้องมีมาตรการควบคุม outsource กรณีมีการจ้างเหมาดำเนินการเกี่ยวกับระบบสารสนเทศของหน่วยงาน
4	หน่วยงานมีข้อกำหนดในการควบคุมคอมพิวเตอร์เคลื่อนที่การเข้าถึงสารสนเทศ						- ต้องมีข้อปฏิบัติในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่
5	หน่วยงานมีข้อกำหนดในการควบคุมโทรศัพท์เคลื่อนที่การเข้าถึงสารสนเทศ						
6	หน่วยงานมีข้อกำหนดในการควบคุมการใช้จากภายนอกผ่านคอมพิวเตอร์เคลื่อนที่และโทรศัพท์เคลื่อนที่						- ต้องมีข้อปฏิบัติ/แผนงาน และขั้นตอนปฏิบัติ สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน
7	หน่วยงานมีข้อปฏิบัติหรือข้อกำหนดและมาตรการเพื่อป้องกันความเสี่ยงจากการใช้คอมพิวเตอร์เคลื่อนที่และ โทรศัพท์เคลื่อนที่						- ต้องมีข้อปฏิบัติในควบคุมการใช้อุปกรณ์คอมพิวเตอร์เคลื่อนที่และโทรศัพท์เคลื่อนที่
8	หน่วยงานมีการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบหรือทำงานอัตโนมัติได้อย่างมั่นคง						- ต้องมีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อ
--9	หน่วยงานแจ้งข้อปฏิบัติในการให้เครื่องยุติการใช้งาน หากว่างเว้นการใช้งานใด ๆ ระยะเวลาหนึ่ง ให้ผู้ใช้งานทราบ						- ต้องมีข้อปฏิบัติในการปฏิบัติของหน่วยงาน กำหนดให้ยุติการใช้งานระบบสารสนเทศ เมื่อเว้นว่างจากการใช้งานในระยะเวลาหนึ่ง - ระบุระยะเวลาที่ชัดเจน

ข้อคิดเห็น_____

_____

ผู้ให้ข้อมูล (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

ผู้สอบทาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

หัวหน้าหน่วยงาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

รายการตรวจสอบการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน
มหาวิทยาลัยเทคโนโลยีสุรนารี

(ตรวจสอบความพร้อมใช้งานของระบบสารสนเทศฯ)

หน่วยงานหลัก สำนักวิชาวิทยาศาสตร์ **ฝ่าย/งาน**

.....

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
1	หน่วยงานมีการพิจารณาคัดเลือกและจัดทำระบบสำรองโดย					-	- ต้องมีการคัดเลือกระบบสารสนเทศ - ต้องมีการจัดทำระบบสำรองที่เหมาะสมให้อยู่ให้อยู่ในสภาพพร้อมใช้งาน
	1.1 หน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการคัดเลือกระบบ สารสนเทศ					-	
	1.2 หน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการจัดทำระบบ สำรอง						
	1.3 ระบบที่จัดทำกำหนดให้มีการกู้คืนและรายงานผลได้						
	1.4 ทุกระบบที่จัดทำสำรองมีการรายงานผลการสำรอง						
2	หน่วยงานมีการเตรียมแผนการเตรียมความพร้อมกรณีฉุกเฉิน ดังนี้					-	- ต้องมีแผนเตรียมพร้อมความพร้อมกรณีฉุกเฉินในกรณีไม่สามารถดำเนินการด้วย
	2.1 กรณีที่ไม่สามารถดำเนินงานด้วยระบบอิเล็กทรอนิกส์ได้						
	2.2 กรณีที่ Site หลักไม่ทำงาน						

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
	2.3 มีการกำหนดแผนระยะสั้น						วิธีการทางอิเล็กทรอนิกส์ - ต้องมีการปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้ได้เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
	2.4 มีการกำหนดแผนระยะยาว						
	2.5 มีการทบทวนแผน 3 เดือนครั้ง						
3	หน่วยงานกำหนดหน้าที่ความรับผิดชอบของบุคลากรดังนี้						ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรในเรื่องต่อไปนี้ - ระบบสารสนเทศ - ระบบสำรอง - การจัดทำแผนเตรียมความพร้อมฉุกเฉิน
	3.1 ด้านระบบสารสนเทศ						
	3.2 ด้านระบบสำรอง						
	3.3 ด้านการจัดทำแผนและทบทวนแผน						
4	หน่วยงานจัดให้มีการทดสอบระบบให้อยู่ในสภาพพร้อมใช้งาน					-	- ต้องมีความถี่ในการทดสอบสภาพพร้อมใช้งาน
	4.1 ระบบสารสนเทศ ทดสอบครั้งสุดท้าย เมื่อ.....						
	4.2 ระบบสำรอง ทดสอบครั้งสุดท้าย เมื่อ.....						

ลำดับ	รายการ	ผลคะแนนประเมิน			ผู้รับผิดชอบหลัก	รายละเอียดเอกสาร/หลักฐานที่เกี่ยวข้อง	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		ใช่	ใช่บางส่วน	ไม่ใช่			
	4.3 แผนฉุกเฉิน ทดสอบครั้งสุดท้าย เมื่อ.....						

ข้อคิดเห็น_____

_____

ผู้ให้ข้อมูล (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

ผู้สอบทาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....

หัวหน้าหน่วยงาน (ลงนาม) ..... ชื่อ-นามสกุล

(.....) วันที่ .....