
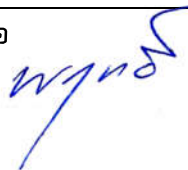


	<b>ชื่อเอกสาร : นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ</b> <b>ของศูนย์ข้อมูลสารสนเทศ</b>		<b>วันที่บังคับใช้</b> 14 ก.พ. 2566
	<b>ชั้นความลับ</b> สาธารณะ	<b>รหัสเอกสาร PLC-SSI-001-V6</b>	

**รายละเอียดเอกสาร**

<b>ชื่อเอกสาร (ไทย)</b>	นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของศูนย์ข้อมูลสารสนเทศ
<b>ชื่อเอกสาร (English)</b>	ISMS for information security of Information Technology Center
<b>วันที่มีผลบังคับใช้</b>	14 กุมภาพันธ์ 2566
<b>รอบการทบทวนเอกสาร</b>	ทบทวนปีละ 1 ครั้ง


**การอนุมัติเอกสาร**

<b>ผู้จัดทำเอกสาร</b>	ลงชื่อ 	<b>ชื่อ</b> นายวิทศักดิ์ นามเมืองรักษ์ <b>ตำแหน่ง</b> นักวิชาการคอมพิวเตอร์ <b>วันที่</b> 14 กุมภาพันธ์ 2566
<b>ผู้ตรวจทานเอกสาร</b>	ลงชื่อ 	<b>ชื่อ</b> นายพฤษดิ์ เกษกระโทก <b>ตำแหน่ง</b> ผู้อำนวยการกลุ่มบริหารจัดการเทคโนโลยีสารสนเทศและเครือข่าย <b>วันที่</b> 14 กุมภาพันธ์ 2566
<b>ผู้อนุมัติเอกสาร</b>	ลงชื่อ 	<b>ชื่อ</b> นางสาวจันทนา วงศ์เยาว์ฟ้า <b>ตำแหน่ง</b> ผู้อำนวยการกองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์วิจัยและนวัตกรรม <b>วันที่</b> 14 กุมภาพันธ์ 2566


	<b>ชื่อเอกสาร : นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ</b> <b>ของศูนย์ข้อมูลสารสนเทศ</b>		<b>วันที่บังคับใช้</b> 14 ก.พ. 2566
	<b>ชั้นความลับ</b> สาธารณะ	<b>รหัสเอกสาร PLC-SSI-001-V6</b>	

**ประวัติปรับปรุงเอกสาร**

เวอร์ชัน	ผู้จัดทำเอกสาร	วันที่มีผลบังคับใช้	รายละเอียดการแก้ไข
1	นายพฤทธิ แกะกระโทก	4 ตุลาคม 2561	<b>เอกสารอนุมัติใช้ครั้งแรก</b>
2	นายพฤทธิ แกะกระโทก	6 มีนาคม 2563	<ul style="list-style-type: none"> <li>- ปรับปรุงชื่อหน่วยงาน</li> <li>- ปรับปรุงสัญลักษณ์หน่วยงาน</li> <li>- ปรับปรุงชื่อศูนย์ข้อมูลระบบสารสนเทศ (MHESI Data Center) แก้ไขคำประกาศนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ</li> </ul>
3	นายทวีศักดิ์ นาเมืองรักษ์	29 มกราคม 2564	<ul style="list-style-type: none"> <li>- ปรับปรุงสัญลักษณ์หน่วยงาน</li> <li>- แก้ไขคำจำกัดความ หน้าที่ 4 ข้อที่ 3 ลำดับที่ 1 เพิ่มเติม (ด้าน ววน.)</li> </ul>
4	นายทวีศักดิ์ นาเมืองรักษ์	1 ธันวาคม 2564	<ul style="list-style-type: none"> <li>- ปรับปรุงชื่อหน่วยงาน</li> <li>- ปรับปรุงสัญลักษณ์หน่วยงาน</li> <li>- ปรับปรุงรหัสเอกสาร อ้างอิงชื่อย่อภาษา English ของหน่วยงานตามโครงสร้างใหม่</li> <li>- ปรับปรุงคำจำกัดความ ลำดับที่ 1 – 3 (หน้าที่ 5 ข้อที่ 3)</li> <li>- แก้ไขคำประกาศนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (หน้าที่ 5 ข้อที่ 4) จากเดิม ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม</li> </ul>


	<b>ชื่อเอกสาร :</b> นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของศูนย์ข้อมูลสารสนเทศ	<b>วันที่บังคับใช้</b> 14 ก.พ. 2566	
<b>ชั้นความลับ</b>	สาธารณะ	<b>รหัสเอกสาร</b> PLC-SSI-001-V6	<b>เลขหน้า</b> 3/7

เวอร์ชัน	ผู้จัดทำเอกสาร	วันที่มีผลบังคับใช้	รายละเอียดการแก้ไข
			เป็น “กองระบบและบริหารข้อมูล เชิงยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม สำนักงานปลัดกระทรวงการ อุดมศึกษา วิทยาศาสตร์ วิจัยและ นวัตกรรม”
5	นายทวีศักดิ์ นาเมืองรักษ์	9 มกราคม 2566	<ul style="list-style-type: none"> <li>- ตัดข้อความ (อาคารพระจอมเกล้า)                ในขอบเขต (หน้าที่ 5 ข้อที่ 2)</li> <li>- ปรับปรุงคำจำกัดความ ลำดับที่                2 – 3 (หน้าที่ 5 ข้อที่ 3)</li> <li>- ตัด OBJ03: กิจกรรมด้านความ                มั่นคงปลอดภัยสารสนเทศเป็นไป                ตามกฎ ระเบียบ นโยบาย และ                กฎหมาย (หน้าที่ 7) แผน</li> </ul>
6	นายทวีศักดิ์ นาเมืองรักษ์	20 กุมภาพันธ์ 2566	<ul style="list-style-type: none"> <li>- เพิ่ม OBJ06 -กิจกรรมด้านความ                มั่นคงปลอดภัยสารสนเทศเป็นไป                ตามกฎ ระเบียบ นโยบาย และ                กฎหมาย (หน้าที่ 6 ข้อที่ 4)</li> <li>- แก้ไขข้อความ หน้าที่ 7 ข้อที่ 4                จาก “คณะกรรมการ/                คณะทำงาน” เป็น “ทีมบริหาร                จัดการ/ทีมทำงาน”</li> </ul>

	<b>ชื่อเอกสาร :</b> นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของศูนย์ข้อมูลสารสนเทศ	<b>วันที่บังคับใช้</b> 14 ก.พ. 2566	
<b>ชั้นความลับ</b> สาธารณะ	<b>รหัสเอกสาร</b> PLC-SSI-001-V6		<b>เลขหน้า</b> 4/7

## สารบัญ

1.	วัตถุประสงค์.....	5
2.	ขอบเขต .....	5
3.	คำจำกัดความ.....	5
4.	นโยบายและวัตถุประสงค์ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System policy and objectives) .....	6

	<b>ชื่อเอกสาร : นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ</b> <b>ของศูนย์ข้อมูลสารสนเทศ</b>	<b>วันที่บังคับใช้</b> <b>14 ก.พ. 2566</b>
<b>ชั้นความลับ</b>	<b>สาธารณะ</b>	<b>รหัสเอกสาร PLC-SSI-001-V6</b>
		<b>เลขหน้า 5/7</b>

### 1. วัตถุประสงค์


เอกสารนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของศูนย์ข้อมูลสารสนเทศ เป็นเอกสารแสดงความมุ่งมั่นและความคาดหวังในการดำเนินการ ISMS ของผู้บริหาร รวมถึงการชี้แจง วัตถุประสงค์ของระบบ ISMS ให้เป็นไปตามมาตรฐาน ISO/IEC 27001:2013

### 2. ขอบเขต

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ของศูนย์ข้อมูลสารสนเทศ สำนักงานปลัดกระทรวงการอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม ครอบคลุมขอบเขต และหลักเกณฑ์การดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อขอการรับรองตามมาตรฐาน ISO/IEC 27001:2013 ของหน่วยงาน

### 3. คำจำกัดความ

ลำดับที่	คำศัพท์	คำจำกัดความ
1	กรข.สป.อว.	กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม สำนักงานปลัดกระทรวงการ อุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
2	ศูนย์ข้อมูลสารสนเทศ	ศูนย์ข้อมูลสารสนเทศ (อาคารพระจอมเกล้า และอาคารอุดมศึกษา 2)
3	Data Center	Data Center (Phrachomklao Building and Udom Building 2)
4	ทรัพย์สินสารสนเทศ	ครอบคลุมถึง 1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงาน คอมพิวเตอร์ และระบบสารสนเทศ 2) อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และ ข้อมูลคอมพิวเตอร์
5	อุปกรณ์โครงสร้างพื้นฐาน	เครื่องปรับอากาศแบบควบคุมความชื้น เครื่องสำรองไฟฟ้า (UPS) และชุดแบตเตอรี่สำรองไฟฟ้า ระบบตรวจจัดการรั่วซึม ของน้ำ ระบบฝ้าดูด และระบบแจ้งเตือนอัตโนมัติ ระบบดับเพลิง อัตโนมัติ ระบบตรวจจับควันความไวสูง อุปกรณ์เครือข่าย
6	บุคลากร	ผู้ใช้งานที่เกี่ยวข้อง และผู้ดูแลระบบของ สป.อว.

	<b>ชื่อเอกสาร :</b> นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของศูนย์ข้อมูลสารสนเทศ	<b>วันที่บังคับใช้</b> 14 ก.พ. 2566
<b>ชั้นความลับ</b>	สาธารณะ	<b>รหัสเอกสาร</b> PLC-SSI-001-V6
		<b>เลขหน้า</b> 6/7


#### 4. นโยบายและวัตถุประสงค์ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System policy and objectives)

เป้าหมายของนโยบายเพื่อป้องกันทรัพย์สินสารสนเทศ (Information Assets) ที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศและการสื่อสารของศูนย์ข้อมูลสารสนเทศ จากภัยคุกคามภายในและภายนอกที่อาจเกิดขึ้นทั้งที่โดยเจตนาหรือไม่เจตนาก็ตาม และเพื่อแสดงถึงข้อผูกพันด้านคุณภาพและความมุ่งมั่นของหน่วยงาน ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จึงได้ประกาศนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้

“กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม มุ่งมั่นในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์ข้อมูลสารสนเทศ จะเป็นไปอย่างต่อเนื่อง มีเสถียรภาพ มั่นคงปลอดภัย และมีความสอดคล้องตามมาตรฐาน ISO/IEC 27001:2013 ตลอดจนดำเนินการพัฒนาอย่างต่อเนื่อง”

วัตถุประสงค์ของการดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีดังนี้

- OBJ01 - บุคลากรของ สป.อว. มีความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและสามารถปฏิบัติ ตามกฎ ระเบียบ นโยบาย และขั้นตอนปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ
- OBJ02 - นโยบาย และแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศมีการทบทวนตามความถี่ที่กำหนดไว้
- OBJ03 - ระบบบริการเครื่องแม่ข่ายแบบเสมือนมีความมั่นคงปลอดภัยและพร้อมใช้ตามที่กำหนด
- OBJ04 - โครงสร้างพื้นฐานของศูนย์ข้อมูลสารสนเทศมีความมั่นคงปลอดภัยและพร้อมใช้ตามที่กำหนด
- OBJ05 - ระบบเครือข่ายมีความมั่นคงปลอดภัยและพร้อมใช้ตามที่กำหนด
- OBJ06 - กิจกรรมด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปตามกฎ ระเบียบ นโยบาย และกฎหมาย

	<b>ชื่อเอกสาร :</b> นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ <b>ของศูนย์ข้อมูลสารสนเทศ</b>	<b>วันที่บังคับใช้</b> 14 ก.พ. 2566
<b>ชั้นความลับ</b>	<b>สาธารณะ</b>	<b>รหัสเอกสาร</b> PLC-SSI-001-V6
		<b>เลขหน้า</b> 7/7

เพื่อให้บรรลุตามนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังกล่าว กรข.สป.อว. จะดำเนินการดังนี้

1. กำหนดนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และให้การสนับสนุนในเรื่องนโยบาย งบประมาณ ทรัพยากรและอื่นๆ ที่จำเป็นเพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีการพัฒนาและปรับปรุงอย่างต่อเนื่อง
2. นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องสร้างความมั่นใจดังนี้
  - ทรัพย์สินสารสนเทศ จะต้องถูกรักษาสถานภาพด้านความลับ (Confidentiality)
  - ทรัพย์สินสารสนเทศ จะต้องถูกรักษาสถานภาพด้านความถูกต้องสมบูรณ์ (Integrity)
  - การเข้าถึงทรัพย์สินสารสนเทศ จะต้องมีความพร้อมใช้งาน (Availability)
  - ทรัพย์สินสารสนเทศ จะต้องถูกป้องกันจากผู้ไม่มีสิทธิ์ในการเข้าถึง (Unauthorized access)
  - นโยบาย ขั้นตอน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารต่างๆ จะต้องถูกกำหนดเพื่อสนับสนุนนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
  - มีการปฏิบัติตามคำสั่ง ระเบียบ ข้อบังคับ กฎหมาย และข้อตกลงที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศ
  - บุคลากรซึ่งเป็นผู้ใช้และผู้ดูแลระบบของ สป.อว. จะต้องได้รับการฝึกอบรมด้านความตระหนักและความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ
  - ทุกเหตุการณ์ที่เกิดขึ้นที่มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศจะต้องถูกบันทึก ตรวจสอบ จัดการ และรายงาน
  - แผนบริหารจัดการความต่อเนื่องของธุรกิจจะต้องถูกพัฒนา ปรับปรุง และทดสอบ
  - ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จะต้องมีการตรวจสอบ การประเมิน และมีกระบวนการปรับปรุงอย่างต่อเนื่องให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป
3. การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ตามขั้นตอนปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Management Procedure) ที่ได้รับการอนุมัติ
4. ต้องมีการแต่งตั้งทีมบริหารจัดการ/ทีมงาน เพื่อรับผิดชอบในการขับเคลื่อนและธำรงไว้ซึ่งระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
5. นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จะต้องถูกนำไปปฏิบัติอย่างเคร่งครัด