วัตถุประสงค์การตรวจประเมิน (Objective) :	เพื่อตรวจประเมินความสอดคล้องของการดำเนินงานด้านการรรักษาความมมั่นคงปลอดภัยไซเบอร์ที่มีต่อ: ๑) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ๒) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ ๒๕๖๔ ๓) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ ๒๕๖๕ ๔) นโยบาย ISMS ของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ตามแนวทางการปฏิบัติต่อข้อกำหนดของมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓(ถ้ามี)
เกณฑ์/มาตรฐานที่ใชjในการตรวจประเมิน (Audit Criteria) :	๑) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ๒) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ ๒๕๖๔ ๓) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ ๒๕๖๕ ๔) มาตรฐานสากลอื่นๆ เช่น ISO/IEC ๒๗๐๐๑:๒๐๑๓ (ถ้ามี)

ขอบเขตที่ตรวจประเมิน (Scope of Audit) :	การรักษาความมั่นคงปลอดภัยไซเบอร์ของ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ซึ่งประกอบไปด้วยขอบเขตบริการที่สำคัญดังต่อไปนี้ (อ้างอิงแอกสาร แนบ ๑ : ผลผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ๑. บริการระบบสารสนเทศทั่วไป โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ๒. บริการระบบนักศึกษาและอาจารย์ โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ สำนักส่งเสริมวิชาการและงานทะเบียน ๓. บริการระบบการเงินและพัสดุ โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ กองคลัง กองกลาง รวมถึงสิ่งอำนวยความสะดวกพื้นฐาน (Facilities) ระบบเครือข่าย (Network) ที่สนับสนุนการให้บริการดังกล่าวของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ อาคาร วิทยบริการ(๒๑) เลขที่ ๖๐ หมู่ ๓ ถ.สายเอเชีย (กรุงเทพฯ - นครสวรรค์) ต.หันตรา อ.พระนครศรีอยุธยา จ.พระนครศรีอยุธยา ๑๓๐๐๐

แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(Cyber Security Audit Plan)

ประจำปี ....๒๕..... ครั้งที่ .....

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
	๐๙.๐๐ - ๐๙.๑๕	Opening Meeting (ประชุมชี้แจงแผนการตรวจ)	All participants	All participants	
	๐๙.๑๕ - ๐๙.๓๐	**สัมภาษณ์ผู้บริหารระดับสูงขององค์กร** . ทิศทางการบริหารจัดการ . วิสัยทัศน์ พันธกิจ กลยุทธ์ และวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ . บทบาท หน้าที่ และความรับผิดชอบ - การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) - การบริหารความเสี่ยง (Risk Management) - นโยบาย และแนวปฏิบัติ (Policies and Guidelines)	All Auditors	ผู้บริหารด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	มาตรา ๔๒, ๔๓, ๔๔, ๔๕, ๔๖, ๕๒, ๕๔, ๕๕, ๕๖, ๕๗, ๕๘ ประมวลข้อ ๑๗, ๑๘, ๑๙ นโยบายข้อ ๑, ๒, ๓

แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(Cyber Security Audit Plan)

ประจำปี ....๒๕..... ครั้งที่ .....

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
	๐๙.๓๐ - ๑๑.๐๐	สอบถามแนวทางปฏิบัติขององค์กร ตาม พรบ.ฯ ตามประมวลฯ และตามนโยบายฯ โดยมีหัวข้อ ดังนี้ ๑. การจัดทำแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - องค์กรมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้งหรือไม่ - องค์กรมีการส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จ หรือไม่ - องค์กรมีการจัดทำแผนดำเนินการแก้ไขอย่างไร - องค์กรมีขั้นตอนการปรับปรุงแผนหรือไม่หากมีการทักท้วงจากคกก. - องค์กรมีการดำเนินการแก้ไขให้อยู่ในกรอบระยะเวลาอย่างไร และมีการติดตามผลอย่างไร ๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - องค์กรมีการประเมินความเสี่ยง (Risk Assessment) อย่างไร	All Auditors	ผู้บริหารด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	มาตรา ๔๒, ๔๓, ๔๔, ๔๕, ๔๖, ๕๒, ๕๔, ๕๕, ๕๖, ๕๗, ๕๘ ประมวลข้อ ๑๗, ๑๘, ๑๙ นโยบายข้อ ๑, ๒, ๓

แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(Cyber Security Audit Plan)

ประจำปี ....๒๕..... ครั้งที่ .....

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
		- องค์กรมีการจัดการความเสี่ยง (Risk Treatment) อย่างไร - องค์กรมีการติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) อย่างไร - องค์กรมีการรายงานความเสี่ยง (Risk Reporting) อย่างไร ๓. การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ - องค์กรมีการจัดทำแผน มีการสื่อสาร และมีการทบกวนแผนการรับมืออย่างไร ๔. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) - องค์กรมีการกำกับดูแลที่ดี ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างไร ๕. นโยบาย และแนวปฏิบัติ (Policies and Guidelines) - องค์กรมีการจัดทำ นโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างไร			

แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(Cyber Security Audit Plan)

ประจำปี ....๒๕..... ครั้งที่ .....

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
	๑๑.๐๐ - ๑๒.๐๐	**การระบุความเสี่ยงขององค์กร (Identify)** - การจัดการทรัพย์สิน (Asset Management) - การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy) - การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) - การจัดการผู้ให้บริการภายนอก (Third Party Management)	K. _____ (Auditor)	ผู้บริหารด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	มาตรา ๕๔, ๕๕ ประมวลข้อ ๒๑ นโยบายข้อ ๒
	๑๒.๐๐ - ๑๓.๐๐	<u>พักกลางวัน</u>		-	
	๑๓.๐๐ - ๑๔.๐๐	**มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้นขององค์กร (Protect)** - การควบคุมการเข้าถึง (Access Control) - การทำให้ระบบมีความแข็งแกร่ง (System Hardening) - การเชื่อมต่อระยะไกล (Remote Connection)	K. _____ (Auditor)	ผู้บริหารด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และสำนักวิทยบริการ	มาตรา ๕๔, ๕๕ ประมวลข้อ ๒๒ นโยบายข้อ ๓

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
		- สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) - การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) - การแบ่งปันข้อมูล (Information Sharing)		และเทคโนโลยีสารสนเทศ	
	๑๔.๐๐ – ๑๕.๐๐	**มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)** - การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	K. _____ (Auditor)	ผู้บริหารด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	มาตรา ๕๖, ๕๗, ๕๘ ประมวลข้อ ๒๓ นโยบายข้อ ๑

แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(Cyber Security Audit Plan)

ประจำปี ....๒๕..... ครั้งที่ .....

วันที่	เวลา	ขjอกำหนดในการตรวจประเมิน (Area of Audit)	ผูjตรวจประเมิน	ผูjรับการตรวจ ประเมิน	หมายเหตุ
	๑๕.๐๐ – ๑๖.๐๐	**มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)** - แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) - แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) - การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	K. _____ (Auditor)	ผู้บริหารด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	มาตรา ๕๖, ๕๗, ๕๘ ประมวลข้อ ๒๔ นโยบายข้อ ๑
	๑๖.๐๐ – ๑๗.๐๐	**มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)** - การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) . การรายงานผลต่อคณะกรรมการการรักษาความ มั่นคงปลอดภัยไซเบอร์แห่งชาติ	K. _____ (Auditor)	ผู้บริหารด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	มาตรา ๕๖, ๕๗, ๕๘ ประมวลข้อ ๒๕ นโยบายข้อ ๑

แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(Cyber Security Audit Plan)

ประจำปี ....๒๕..... ครั้งที่ .....

วันที่	เวลา	ขอบกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
	๑๗.๐๐ - ๑๗.๑๐	Auditor Time ประชุมคณะผู้ตรวจประเมิน	All Auditors	-	
	๑๗.๑๐ - ๑๗.๓๐	สรุปผลการตรวจประเมินภายใน ร่วมกับทีมผู้ตรวจประเมินและผู้ที่เกี่ยวข้อง	All participants	All participants	

ผู้จัดทำ / ตรวจสอบ	ผู้อนุมัติ
ลงนาม : ( )	ลงนาม : ( )
หัวหน้าคณะผู้ตรวจสอบภายใน (Lead Internal Auditor)	ผู้บริหารด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security)
วันที่ :	วันที่ :

หมายเหตุ เวลาอาจมีการปรับเปลี่ยนตามความเหมาะสม