ข้อเสนอแนะมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ

Information Security Recommendation

จุฬาลงกรณ์มหาวิทยาลัย

ประวัติการแก้ไขเอกสาร

เวอร์ชัน	รายละเอียดการแก้ไข	มีผลบังคับใช้วันที่
01	เอกสารเวอร์ชันตั้งต้น	15 พฤศจิกายน 2567

การอนุมัติเอกสาร

ผู้ตรวจทานเอกสาร	
ชื่อ นายรุ่งโรจน์ กิตติถาวรกุล ตำแหน่ง ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ วันที่ 15 พฤศจิกายน 2567	ลงชื่อ ..... (นายรุ่งโรจน์ กิตติถาวรกุล)
ผู้อนุมัติเอกสาร	
ชื่อ รองศาสตราจารย์ ดร.ชัยเชษฐ์ สายวิจิตร ตำแหน่ง ผู้ช่วยอธิการบดี วันที่ 15 พฤศจิกายน 2567	ลงชื่อ ..... (รองศาสตราจารย์ ดร.ชัยเชษฐ์ สายวิจิตร)

สารบัญ

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้เป็นข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ส่วนงานของจุฬาลงกรณ์มหาวิทยาลัย มีแนวทางในการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศแก่ข้อมูลและระบบสารสนเทศที่สำคัญ เพื่อสามารถลดความเสี่ยงหรือบรรเทาความเสี่ยงได้อย่างเป็นรูปธรรม และรักษาซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

2. คำนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 “ส่วนงาน” หมายความว่า ส่วนงานตามประกาศจุฬาลงกรณ์มหาวิทยาลัย ว่าด้วย ส่วนงานของมหาวิทยาลัย

2.2 “หัวหน้าส่วนงาน” หมายความว่า คณบดี ผู้อำนวยการสถาบัน หรือหัวหน้าส่วนงานที่เรียกชื่ออย่างอื่น

2.3 “พนักงาน” หมายความว่า พนักงานมหาวิทยาลัย หรือผู้ปฏิบัติงานในมหาวิทยาลัย และลูกจ้างของมหาวิทยาลัย

2.4 “หน่วยงานภายนอก” หมายความว่า หน่วยงานภายนอกมหาวิทยาลัย

2.5 “ผู้ให้บริการภายนอก” หมายความว่า หน่วยงานภายนอกหรือบุคคลของหน่วยงานภายนอกที่รับจ้างปฏิบัติงานตามความต้องการของส่วนงาน

2.6 “ผู้ใช้งาน” หมายความว่า พนักงาน และผู้ให้บริการภายนอกที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหารจัดการหรือดูแลรักษาระบบสารสนเทศของส่วนงาน

2.7 “ผู้ให้บริการคลาวด์” หมายความว่า หน่วยงานของรัฐ หรือเอกชนที่ทำให้บริการคลาวด์ (Cloud Service) สามารถใช้ได้ตามความต้องการของส่วนงาน

2.8 “ความมั่นคงปลอดภัยสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ

3. ภาพรวม

ข้อเสนอแนะมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศฉบับนี้ จัดทำขึ้นโดยคณะทำงานจัดทำแนวปฏิบัติด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย (กรกฎาคม พ.ศ. 2567) โดยอ้างอิงมาตรฐาน ข้อเสนอแนะมาตฐาน และแนวคิด ดังต่อไปนี้

3.1 ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls

3.2 ขมธอ. 35-2566 ของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม "ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์"

3.3 แนวคิด The 7 Layers of Cybersecurity ในการจัดการและวางแผนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุมในทุกมิติสอดคล้องกับแบบจำลอง OSI Model (Open Systems Interconnection Model) ที่อธิบายการทำงานของการสื่อสารข้อมูลในระบบเครือข่ายคอมพิวเตอร์ ซึ่งพัฒนาโดย International Organization for Standardization (ISO)

4. ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศประกอบด้วย การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

4.1 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

4.1.1 ส่วนงานต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (information security risk assessment) ของระบบงานหรือบริการที่สำคัญ ดังนี้

- การกำหนดเกณฑ์ความเสี่ยง ซึ่งประกอบด้วย เกณฑ์การยอมรับความเสี่ยง (risk acceptance criteria) และเกณฑ์การประเมินความเสี่ยง (risk assessment criteria)
- การระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (risk identification) ได้แก่ การใช้กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อระบุความเสี่ยงที่เกี่ยวกับ การถูกเปิดเผยข้อมูล ความถูกต้องครบถ้วน และความพร้อมใช้งานของสารสนเทศภายในขอบเขต ของระบบงานหรือบริการที่สำคัญ รวมถึงการระบุผู้เป็นเจ้าของความเสี่ยง
- การวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (risk analysis) โดยการประเมินผล กระทบและโอกาสที่อาจจะเกิดขึ้นจากความเสี่ยง รวมถึงการกำหนดระดับค่าความเสี่ยง
- การเปรียบเทียบผลลัพธ์จากการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยง และการจัดลำดับ ความเสี่ยงเพื่อการจัดการความเสี่ยง (risk treatment)

4.1.2 ส่วนงานต้องกำหนดแผนจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (information security risk treatment plan) และต้องเก็บรักษาเอกสารแสดงผลลัพธ์จากการจัดการความเสี่ยง

4.1.3 ส่วนงานต้องทบทวนการประเมินความเสี่ยงและการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของระบบงานหรือบริการที่สำคัญอย่างสม่ำเสมอ

4.2 มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ อ้างอิง มาตรการควบคุม (control) และแนวปฏิบัติ (guidance) จากมาตรฐาน ISO/IEC 27002:2022 โดยพิจารณาตามข้อกำหนด และระดับความจำเป็นในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้

4.2.1	มาตรการควบคุมด้านองค์กร (organizational controls)	จำนวน	8	ข้อ
4.2.2	มาตรการควบคุมด้านบุคลากร (people controls)	จำนวน	2	ข้อ
4.2.3	มาตรการควบคุมด้านกายภาพ (physical controls)	จำนวน	2	ข้อ
4.2.4	มาตรการควบคุมด้านเทคโนโลยี (technological controls)	จำนวน	11	ข้อ

โดยแบ่งเป็นมาตรการควบคุมตามระดับความจำเป็น ดังนี้

- มาตรการควบคุมที่จำเป็น (mandatory controls) จำนวน 19 ข้อ
- มาตรการควบคุมที่เฉพาะกรณี (conditional controls) จำนวน 4 ข้อ

ทั้งนี้ เพื่อให้สอดคล้องตามข้อเสนอแนะมาตรฐานฉบับนี้ ส่วนงานต้องปฏิบัติตามมาตรการควบคุมที่จำเป็นทุกข้อ และปฏิบัติตามมาตรการควบคุมที่เฉพาะกรณีหากระบบของส่วนงานเป็นไปตามเงื่อนไขที่ระบุไว้ในข้อนั้น ๆ เช่น กรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน กรณีที่ใช้บริการคลาวด์ หรือกรณีที่ส่วนงานเป็นผู้พัฒนาระบบเอง

4.2.1 มาตรการควบคุมด้านองค์กร (organizational controls)

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวทางปฏิบัติ	ISO/IEC 27002:2022
1.	**นโยบายความมั่นคงปลอดภัยสารสนเทศ (policies for information security)** ส่วนงานกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศซึ่งได้รับการอนุมัติโดยหัวหน้าส่วนงาน รวมถึงเผยแพร่และสื่อสารให้พนักงานที่เกี่ยวข้องรับทราบ	จำเป็น	- **จัดทำ**นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ และนโยบายนี้ได้รับอนุมัติจากหัวหน้าส่วนงาน - มีการทบทวนนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ อย่างน้อย 1 ครั้งต่อปี หรือตามความเหมาะสม	Clause 5.1
2.	**การกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (information security roles and responsibilities)** ส่วนงานกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ และจัดสรรให้มีความเหมาะสมตามความต้องการของส่วนงาน	จำเป็น	- **กำหนดหน้าที่**ความรับผิดชอบของพนักงานในการดูแลด้านความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจน	Clause 5.2
3.	**บัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ (inventory of information and other associated assets)** ส่วนงานต้องจัดทำและเก็บทะเบียนทรัพย์สินเพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อทรัพย์สินอย่างเหมาะสม	จำเป็น	- **จัดทำ**ทะเบียนทรัพย์สิน และปรับปรุงแก้ไขข้อมูลให้มีความถูกต้องอยู่เสมอ	Clause 5.9
4.	**สิทธิการเข้าถึง (access rights)** ส่วนงานมีการจัดเตรียม ทบทวน แก้ไข หรือลบสิทธิการเข้าถึงข้อมูล และสินทรัพย์ที่เกี่ยวข้องอื่น ๆ ตามนโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศและกฎระเบียบของส่วนงาน	จำเป็น	- **ทบทวน**สิทธิการเข้าถึงของผู้ใช้งาน โดยต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิการเข้าถึง ทั้งการให้สิทธิและการถอดถอนสิทธิ และการทบทวนสิทธิอย่างเหมาะสม	Clause 5.18
5.	**การวางแผนและเตรียมการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (information security incident management planning and preparation)** ส่วนงานมีการวางแผนและเตรียมการสำหรับการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (information security incident) โดยมีการกำหนดและสื่อสารกระบวนการการจัดการ บทบาทและหน้าที่ความรับผิดชอบสำหรับการบริหารจัดการ สถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	จำเป็น	- **จัดทำ**เอกสารขั้นตอนปฏิบัติในการรับมือกับเหตุขัดข้อง (Incident Management Procedure)	Clause 5.24

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวทางปฏิบัติ	ISO/IEC 27002:2022
6.	**ความมั่นคงปลอดภัยสารสนเทศเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก และการระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (information security in supplier relationships and addressing information security within supplier agreements)** เพื่อให้มีการป้องกันทรัพย์สินของส่วนงานที่มีการเข้าถึงโดยผู้ให้บริการภายนอก ส่วนงานจะต้องกำหนดให้มีการจัดทำข้อกำหนดหรือสัญญาร่วมกันระหว่างส่วนงานกับผู้ให้บริการภายนอก และต้องกำหนดให้มีการลงนามในข้อตกลงด้านการรักษาความลับที่ของข้อมูลที่สอดคล้องกับนโยบายฯ ซึ่งรวมถึงระบุความรับผิดชอบของผู้ให้บริการภายนอก หากเกิดความเสียหายขึ้น	เฉพาะในกรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน	- **จัดทำ**ข้อกำหนด หรือสัญญาร่วมกันระหว่างส่วนงานกับผู้ให้บริการภายนอก - ผู้ให้บริการภายนอกต้อง**ลงนาม**ในหนังสืออินยอมรับเงื่อนไขนโยบายเกี่ยวกับความปลอดภัยระบบสารสนเทศ (Acceptable Use Policy : AUP) และข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยสารสนเทศและระดับการให้บริการตามที่ตกลงกันไว้	Clause 5.19, Clause 5.20
7.	**ข้อกำหนดทางกฎหมาย ข้อบังคับและสัญญา (legal, statutory, regulatory and contractual requirements) และ การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศของส่วนงาน (compliance with policies, rules and standards for information security)** เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับรวมทั้งสัญญาต่าง ๆ และเพื่อให้มีการปฏิบัติอย่างสอดคล้องกับนโยบาย กฎระเบียบ และ มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ	จำเป็น	- ส่วนงานต้องมีการ**ศึกษา ทำความเข้าใจ และปฏิบัติตาม**รายการของนโยบาย กฎระเบียบข้อบังคับ กฎหมาย ที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เช่น การปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) - ส่วนงานต้องมีการ**ตรวจสอบและทบทวน**การปฏิบัติตามนโยบาย กฎระเบียบ และ มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ	Clause 5.31, Clause 5.36
8.	**ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (information security for use of cloud services)** เพื่อให้แน่ใจว่าข้อมูลที่จัดเก็บหรือประมวลผลบนคลาวด์มีความปลอดภัยตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศของส่วนงาน หรือตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	เฉพาะในกรณีที่ใช้บริการคลาวด์	- ส่วนงานต้อง**กำหนดมาตรการ**และการปฏิบัติที่เหมาะสม ซึ่งครอบคลุมถึงกระบวนการในการจัดหา การใช้บริการ การบริหารจัดการ และการยกเลิกการใช้บริการคลาวด์ - **กำกับดูแลผู้ให้บริการคลาวด์** ดำเนินการตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศของส่วนงาน หรือตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	Clause 5.23

4.2.2 มาตรการควบคุมด้านบุคลากร (people controls)

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวทางปฏิบัติ	ISO/IEC 27002:2022
9.	**การสร้างความตระหนัก การศึกษา และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (information security awareness, education and training)** พนักงานของส่วนงานและผู้ที่เกี่ยวข้องได้รับการสร้างความตระหนัก ได้รับการศึกษาและการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสม รวมถึงได้รับรู้ถึงนโยบายความมั่นคงปลอดภัยสารสนเทศ และ นโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน้าที่ ความรับผิดชอบ ที่มีความเป็นปัจจุบันอย่างสม่ำเสมอ	จำเป็น	- จัดอบรมให้ความรู้กับพนักงานอย่างน้อยปีละ1 ครั้ง เพื่อให้ตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ และเพื่อรับทราบถึงนโยบายความมั่นคงปลอดภัยสารสนเทศของส่วนงานที่มีการประกาศใช้	Clause 6.3
10.	**การทำงานจากระยะไกล (remote working)** ส่วนงานต้องมีมาตรการด้านความมั่นคงปลอดภัยสารสนเทศเมื่อพนักงานทำงานจากระยะไกลเพื่อป้องกันการเข้าถึง การประมวลผล หรือ การจัดเก็บข้อมูลจากภายนอก	จำเป็น	- กำกับไม่ให้มีการเข้าถึงอย่างอิสระ โดยส่วนงานจะต้องพิจารณาตามมาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ดังนี้ 1) อนุญาตในการเข้าถึงเฉพาะผู้ที่มีสิทธิหรือได้รับอนุญาตในการเข้าถึงเท่านั้น 2) ผู้มีสิทธิใช้งานจากระยะไกลต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อเพิ่มความปลอดภัย เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น 3) ในการเข้าถึงจากระยะไกลจะต้องสามารถบันทึกข้อมูลการเข้าถึง และข้อมูลจราจรทางคอมพิวเตอร์เพื่อตรวจสอบกิจกรรมภายหลังได้	Clause 6.7

4.2.3 มาตรการควบคุมด้านกายภาพ (physical controls)

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวทางปฏิบัติ	ISO/IEC 27002:2022
11.	**การเข้าออกทางกายภาพ (physical entry)** ส่วนงานมีการควบคุมการเข้าออกทางกายภาพของพื้นที่ควบคุมพิเศษ เช่น ห้อง Server โดยอนุญาตให้บุคคลผ่านเข้า-ออกพื้นที่ควบคุมพิเศษได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น	จำเป็น	- ส่วนงานต้อง**กำหนดมาตรการ**ควบคุมและป้องกันที่เหมาะสมในการควบคุมการเข้า – ออกพื้นที่ อาทิ **การออกระเบียบ วิธีปฏิบัติ หรือจัดเตรียมอุปกรณ์รักษาความปลอดภัย** ดังนี้ 1) มีการติดตั้งกล้องวงจรปิด ที่สามารถดูข้อมูลการเข้า - ออกพื้นที่ย้อนหลังได้ 2) ห้องระบบคอมพิวเตอร์และศูนย์คอมพิวเตอร์ (ห้อง Server หรือ Data Center) เป็นห้องที่มีกุญแจล็อค หรือมีระบบที่สามารถตรวจสอบการระบุตัวตน ซึ่งจำกัดสิทธิการเข้าถึงเฉพาะผู้ที่ได้รับการอนุญาตเท่านั้น	Clause 7.2
12.	**การบำรุงรักษาอุปกรณ์ (equipment maintenance)** ส่วนงานมีการบำรุงรักษาอุปกรณ์อย่างถูกต้องเพื่อให้มีสภาพพร้อมใช้งาน รักษาความถูกต้องครบถ้วนและมีการรักษาความลับของข้อมูล	จำเป็น	- **ต้องบำรุงรักษาอุปกรณ์**อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงอย่างน้อยปีละ 1 ครั้ง หรือตามที่เจ้าของผลิตภัณฑ์แนะนำ เป็นต้น	Clause 7.13

4.2.4 มาตรการควบคุมด้านเทคโนโลยี (technological controls)

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวทางปฏิบัติ	ISO/IEC 27002:2022
13.	**การยืนยันตัวตนอย่างปลอดภัย (secure authentication)** ส่วนงานมีการใช้เทคโนโลยีและกระบวนการยืนยันตัวตนที่มีความมั่นคงปลอดภัย โดยสอดคล้องกับข้อจำกัดการเข้าถึงข้อมูลและนโยบายควบคุมการเข้าถึง	จำเป็น	- ต้องมีการ**พิสูจน์ยืนยันตัวตน**ด้วยการใช้รหัสผ่าน หรือระบบยืนยันตัวตนเพิ่มเติมที่มีความมั่นคงปลอดภัย	Clause 8.5
14.	**การสำรองข้อมูล (information backup)** ส่วนงานต้องมีการดำเนินการสำรองข้อมูล และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอ เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ	จำเป็น	- **จัดทำ**แผนสำรองข้อมูลพร้อมกู้คืนระบบ และกำหนดให้มีการสำรองข้อมูลที่เหมาะสมในแต่ละระบบงาน	Clause 8.13

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวทางปฏิบัติ	ISO/IEC 27002:2022
15.	**การเฝ้าติดตามเหตุการณ์ (monitoring activities)** เครือข่าย ระบบ และแอพพลิเคชันต้องมีการเฝ้าระวังการทำงานเพื่อตรวจหาพฤติกรรมที่ผิดปกติ และดำเนินการเพื่อประเมินความเป็นไปได้ของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น	จำเป็น	- **กำหนดกระบวนการหรือรูปแบบ**ในการเฝ้าระวังการทำงานของเครือข่าย ระบบ และแอปพลิเคชันเพื่อตรวจหาพฤติกรรมที่ผิดปกติที่อาจเกิดขึ้นกับระบบสารสนเทศ	Clause 8.16
16.	**การตั้งค่าเทียบเวลา (clock synchronization)** ส่วนงานตั้งค่าเทียบเวลาระบบประมวลผลที่ส่วนงานใช้ให้สอดคล้องกับแหล่งเวลาที่น่าเชื่อถือ	จำเป็น	- **ตั้งค่า**เวลาในอุปกรณ์เครือข่ายให้ตรงตามเวลามาตรฐานสากล หรือ NTP Server ของมหาวิทยาลัย (ntp.chula.ac.th)	Clause 8.17
17.	**สิทธิการเข้าถึงของสิทธิระดับสูง (privileged access rights)** ส่วนงานมีการจัดสรรและจำกัดการเข้าถึงของสิทธิระดับสูง	จำเป็น	- **ควบคุมและจัดการสิทธิ**การเข้าถึงของผู้ใช้งานอย่างเหมาะสม ดังนี้ 1) ต้องกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบด้วย 2) ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ	Clause 8.2
18.	**การจำกัดการเข้าถึงข้อมูลสารสนเทศ (information access restriction)** ส่วนงานมีการจำกัดการเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ให้สอดคล้องกับนโยบายควบคุมการเข้าถึง	จำเป็น	- การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการ**จำกัด**ให้สอดคล้องกับนโยบาย**ควบคุมการเข้าถึง** ดังนี้ 1) ผู้ใช้งานทุกคนต้องมีรหัสผู้ใช้งาน (User Account) เฉพาะบุคคล เพื่อสามารถระบุและติดตามการใช้งานของแต่ละคนได้ 2) ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน เช่น เขียน อ่าน ลบ ได้ เป็นต้น	Clause 8.3
19.	**การบันทึกข้อมูลเหตุการณ์ (logging)** ข้อมูล Log ที่มีการบันทึกกิจกรรมต่าง ๆ ข้อมูลเหตุการณ์ (logging) ข้อยกเว้น (exceptions) ข้อผิดพลาด (faults) และเหตุการณ์ที่เกี่ยวข้องอื่น ๆ ของระบบ ต้องมีการจัดเตรียมระบบไว้เพื่อให้สามารถตรวจสอบ สอบทาน และนำมาวิเคราะห์ข้อมูลได้	จำเป็น	- **จัดเก็บ**บันทึกข้อมูล Log กิจกรรมต่าง ๆ ของระบบ	Clause 8.15

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวทางปฏิบัติ	ISO/IEC 27002:2022
20.	**ความมั่นคงปลอดภัยของระบบเครือข่าย (networks security)** ส่วนงานมีการจัดการ ควบคุม และรักษาความมั่นคงปลอดภัยระบบเครือข่ายและอุปกรณ์เครือข่าย เพื่อปกป้องข้อมูลในระบบสารสนเทศ และแอปพลิเคชัน	จำเป็น	- **กำหนดมาตรการ**บริหารจัดการและควบคุมระบบเครือข่ายให้มีความปลอดภัย ดังนี้ 1) จัดทำแผนผังการเชื่อมต่อ 2) จำกัดการเชื่อมต่อระบบ และเปิดใช้งาน service port ที่เชื่อมต่อตามความจำเป็นเท่านั้น 3) ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router, Switch และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด	Clause 8.2
21.	**การแบ่งแยกเครือข่าย (segregation of networks)** ส่วนงานแบ่งแยกกลุ่มการบริการข้อมูล กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศต้องมีการแบ่งแยกออกจากกันในเครือข่ายของส่วนงาน	จำเป็น	- **แบ่งแยก**เครือข่ายออกจากกันอย่างชัดเจน เช่น แบ่งตามกลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และ โซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ	Clause 8.22
22.	**การจ้างหน่วยงานภายนอกพัฒนาระบบ (outsourced development)** การกำหนดขอบเขตในการจ้างพัฒนาระบบ และควบคุมให้หน่วยงานภายนอกพัฒนาซอฟต์แวร์ให้เป็นไปตามเงื่อนไขหรือข้อกำหนดในสัญญา	**เฉพาะในกรณีที่ส่วนงานเป็นผู้พัฒนาระบบเอง**	- ในการทำสัญญาว่าจ้างการพัฒนาระบบส่วนงาน**ต้องมีความชัดเจนและครอบคลุม**ถึงสัญญาทางด้านลิขสิทธิ์ ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ	Clause 8.3
23.	**การแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการให้บริการ ออกจากกัน (separation of development, test and production environments)** ส่วนงานมีการแยกสภาพแวดล้อมและรักษาความมั่นคงปลอดภัยในสภาพแวดล้อมของการพัฒนา การทดสอบ และการให้บริการ	**เฉพาะในกรณีที่ส่วนงานเป็นผู้พัฒนาระบบเอง**	- ต้องมีการ**แยกเครื่องมือ**ในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ควรมีการแยกเครื่องที่ใช้ในการพัฒนาและทดสอบ ออกจากกับเครื่องที่ใช้งานจริง หากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริงด้วย	Clause 8.31