ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย
เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

---

เพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย จึงกำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

จึงอาศัยอำนาจตามความในมาตรา ๒๔ และมาตรา ๒๗ แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล พ.ศ. ๒๕๔๘ กำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ข้อ ๔ ให้อธิการบดีเป็นผู้รักษาการตามประกาศนี้ กรณีที่มีปัญหาจากการปฏิบัติตามประกาศนี้หรือที่ประกาศนี้มิได้กำหนดไว้ ให้อธิการบดีเป็นผู้วินิจฉัยและคำวินิจฉัยนั้นให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๑๐ มิถุนายน พ.ศ.๒๕๖๙

(ศาสตราจารย์สุวัจน์ ธัญรส)
อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย
เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

---

เพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย จึงกำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

จึงอาศัยอำนาจตามความในมาตรา ๒๔ และมาตรา ๒๗ แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล พ.ศ. ๒๕๔๘ กำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ข้อ ๔ ให้อธิการบดีเป็นผู้รักษาการตามประกาศนี้ กรณีที่มีปัญหาจากการปฏิบัติตามประกาศนี้ หรือที่ประกาศนี้มิได้กำหนดไว้ ให้อธิการบดีเป็นผู้วินิจฉัยและคำวินิจฉัยนั้นให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๓๐ มิถุนายน พ.ศ.๒๕๖๙

(ศาสตราจารย์สุวัจน์ ธัญรส)
อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

ร่าง/พิมพ์.....

ตรวจ.....

30/06/2569
09:55:27 +07'00'
DID-8E210FA38


# ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

# (Guideline and Cybersecurity Framework)

# มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

**โดย**

**สำนักวิทยบริการและเทคโนโลยีสารสนเทศ**

**มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย**

**มิถุนายน ๒๕๖๙**

# สารบัญ

# สารบัญ (ต่อ)

# ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
# (Guideline and Cybersecurity Framework)

## ๑. บทนำ

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) มีหน้าที่จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้เป็นข้อกำหนดขั้นต่ำในการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรการดังกล่าวครอบคลุมถึงการกำหนดแนวทางการประเมินความเสี่ยง การเฝ้าระวัง และการเตรียมความพร้อมเพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบหรือสร้างความเสียหายต่อระบบสารสนเทศของประเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ในฐานะหน่วยงานของรัฐที่มีพันธกิจสำคัญในการให้บริการข้อมูลองค์ความรู้ และการเผยแพร่งานวิจัยผ่านระบบเทคโนโลยีสารสนเทศที่หลากหลาย ทั้งในรูปแบบเครือข่ายภายใน สื่อสังคมออนไลน์ และโมบายแอปพลิเคชัน (Mobile Application) ตระหนักถึงความสำคัญในการปกป้องข้อมูลและระบบคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย จึงได้จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ขึ้น โดยอ้างอิงจาก **ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔** จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

การดำเนินการตามกรอบมาตรฐานนี้ มีวัตถุประสงค์หลักเพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยสามารถปฏิบัติได้อย่างปลอดภัย มีประสิทธิภาพ และสอดคล้องกับมาตรฐานสากล นอกจากนี้ยังมุ่งเน้นการสร้างความเชื่อมั่นให้กับผู้รับบริการและผู้มีส่วนได้ส่วนเสีย ผ่านกระบวนการเฝ้าระวังภัยคุกคามที่มีมาตรฐานที่เป็นไปตามแนวทางของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อยกระดับความมั่นคงปลอดภัยสารสนเทศของประเทศอย่างยั่งยืน

**๒. วัตถุประสงค์**

๒.๑ เพื่อกำหนดกรอบแนวคิด แนวทาง และวิธีปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ให้มีความมั่นคงปลอดภัยและมีประสิทธิภาพ

๒.๒ เพื่อให้การปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยสอดคล้องกับข้อกำหนดตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (คปส.) ที่เกี่ยวข้อง

๒.๓ เพื่อป้องกัน ลดความเสี่ยง และรับมือกับภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และบริการที่สำคัญของมหาวิทยาลัย

๒.๔ เพื่อสร้างความเชื่อมั่นให้กับผู้รับบริการและผู้มีส่วนได้ส่วนเสีย ผ่านการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

**๓. ขอบเขต**

กรอบมาตรฐานและประมวลแนวทางปฏิบัติฉบับนี้ มีขอบเขตการบังคับใช้และครอบคลุมการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย โดยอ้างอิงตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งครอบคลุมถึงองค์ประกอบดังต่อไปนี้

**๓.๑ สารสนเทศที่สำคัญและบริการที่สำคัญ (Critical Services)** ครอบคลุมระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ และโครงสร้างพื้นฐานสารสนเทศที่สนับสนุนภารกิจหลักของมหาวิทยาลัยทั้งในส่วนงานบริหาร ส่วนงานวิจัย และการบริการการศึกษา

**๓.๒ บุคลากรและผู้เกี่ยวข้อง** ครอบคลุมถึงบุคลากรสายวิชาการ สายสนับสนุน เจ้าหน้าที่จ้างเหมา นักศึกษา รวมถึงผู้ให้บริการภายนอก (Third Party) ที่ได้รับสิทธิ์ในการเข้าถึงหรือเชื่อมต่อกับระบบสารสนเทศของมหาวิทยาลัย

**๓.๓ ทรัพย์สินทางเทคโนโลยีสารสนเทศ** ครอบคลุมทรัพย์สินที่ระบุไว้ในทะเบียนทรัพย์สิน (Asset Inventory) ของหน่วยงาน ทั้งในรูปแบบที่จับต้องได้ (Hardware) และระบบนามธรรม (Software/Data) ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) ต่อบริการที่สำคัญ

**๓.๔ พื้นที่ปฏิบัติงานและการเชื่อมต่อ** ครอบคลุมระบบเครือข่ายภายในและภายนอก การเชื่อมต่อระยะไกล (Remote Connection) และการสื่อสารข้อมูลระหว่างมหาวิทยาลัยกับหน่วยงานภายนอกที่เกี่ยวข้อง

**๔. คำนิยาม**

**๔.๑ มหาวิทยาลัย หรือ หน่วยงาน** หมายถึง มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

**๔.๒ คณะกรรมการ** หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) หรือคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (คปส.) ตามแต่บริบทของกฎหมาย

**๔.๓ บริการที่สำคัญ (Critical Services)** หมายถึง ภารกิจหลักหรือบริการเทคโนโลยีสารสนเทศของมหาวิทยาลัยที่หากเกิดการขัดข้องจะส่งผลกระทบต่อการดำเนินงานหรือภาพลักษณ์ของสถาบันอย่างรุนแรง

**๔.๔ ภัยคุกคามทางไซเบอร์ (Cyber Threat)** หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของระบบ

**๔.๕ เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident)** หมายถึง เหตุการณ์ที่มีผลเชิงลบซึ่งเกิดจากภัยคุกคามทางไซเบอร์ ทำให้ระบบหรือข้อมูลได้รับความเสียหายหรือทำงานผิดปกติ

**๔.๖ ผู้ให้บริการภายนอก (Third Party)** หมายถึง บุคคลหรือนิติบุคคลภายนอกที่ให้บริการด้านเทคโนโลยีสารสนเทศ หรือมีการเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยและสามารถเข้าถึงข้อมูลสำคัญ ได้

**๔.๗ ตัวชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators: KRI)** หมายถึง เครื่องมือที่ใช้วัดกิจกรรมหรือสัญญาณเตือนที่บ่งบอกว่าระดับความเสี่ยงขององค์กรกำลังเพิ่มขึ้น เพื่อให้สามารถเตรียมมาตรการป้องกันได้ทันท่วงที

**๔.๘ Recovery Time Objective (RTO)** หมายถึง ระยะเวลาเป้าหมายที่ต้องกู้คืนระบบให้กลับมาใช้งานได้ตามปกติ

**๔.๙ Recovery Point Objective (RPO)** หมายถึง ระยะเวลาสูงสุดของข้อมูลที่ยอมให้สูญหายได้ (จุดที่ต้องสำรองข้อมูลล่าสุด)

**๔.๑๐ Maximum Tolerance Period of Disruption (MTPD)** หมายถึง ระยะเวลาสูงสุดที่หน่วยงานสามารถทนต่อการหยุดชะงักของบริการสำคัญได้ก่อนจะเกิดความเสียหายที่ไม่อาจยอมรับได้

**๔.๑๑ เหตุการณ์ (Event)** หมายถึง สิ่งที่เกิดขึ้นและสังเกตได้ในระบบเครือข่ายหรือกระบวนการทำงาน ซึ่งอาจส่งผลเชิงบวกหรือเชิงลบก็ได้

**๕. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีระบบและครอบคลุมทุกมิติ มหาวิทยาลัยจึงกำหนดกรอบมาตรฐานการดำเนินงานซึ่งประกอบด้วย ๖ หัวข้อหลัก ดังนี้

**๕.๑ การระบุความเสี่ยง (Identify)** มุ่งเน้นการทำความเข้าใจในบริบทของหน่วยงาน การระบุทรัพย์สินสารสนเทศที่สำคัญ และการประเมินความเสี่ยง เพื่อวางรากฐานในการจัดการความมั่นคงปลอดภัยที่เหมาะสมกับทรัพยากรที่มีอยู่

**๕.๒ มาตรการป้องกันความเสี่ยง (Protect)** การกำหนดมาตรการควบคุมและป้องกันทางเทคนิคและด้านบริหารจัดการ เพื่อจำกัดหรือลดผลกระทบจากภัยคุกคามไซเบอร์ รวมถึงการสร้างความตระหนักรู้ให้แก่บุคลากร

**๕.๓ มาตรการตรวจสอบและเฝ้าระวัง (Detect)** การจัดให้มีกลไกและกระบวนการตรวจจับเหตุการณ์ที่ผิดปกติหรือเหตุภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที เพื่อให้สามารถวิเคราะห์และจำแนกประเภทของภัยคุกคามได้อย่างแม่นยำ

**๕.๔ มาตรการเผชิญเหตุ (Respond)** การกำหนดขั้นตอนและวิธีปฏิบัติเมื่อตรวจพบเหตุภัยคุกคาม รวมถึงการจัดทำแผนรับมือและแผนการสื่อสารในภาวะวิกฤต เพื่อให้สามารถแก้ไขสถานการณ์ได้อย่างมีประสิทธิภาพ

**๕.๕ มาตรการรักษาและฟื้นฟูความเสียหาย (Recover)** การเตรียมความพร้อมในการกู้คืนระบบและบริการสำคัญให้กลับมาดำเนินงานได้อย่างต่อเนื่อง (Resilience) และการปรับปรุงแผนความต่อเนื่องทางธุรกิจ (BCP) ให้ทันต่อสถานการณ์

**๕.๖ แผนการตรวจสอบ (Audit Plan)** แผนการจัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน สำหรับตรวจสอบว่าหน่วยงาน ปฏิบัติตามกฎหมายและมาตรฐาน (Compliance) หรือไม่ และเพื่อประเมินความพร้อมและประสิทธิภาพในการป้องกันภัยคุกคาม รวมถึงความเหมาะสมของมาตรการควบคุมที่ใช้ในการป้องกันความเสี่ยง

**หัวข้อหลักที่ ๑** การระบุความเสี่ยง (Identify)

เพื่อให้มหาวิทยาลัยสามารถบริหารจัดการและประเมินความเสี่ยงที่อาจเกิดขึ้นต่อระบบคอมพิวเตอร์ ข้อมูล และทรัพย์สินสำคัญได้อย่างมีประสิทธิภาพ มหาวิทยาลัยต้องปฏิบัติตามกรอบมาตรฐานดังต่อไปนี้

**กรอบมาตรฐาน**

๑.๑ การจัดการทรัพย์สิน (Asset Management)

๑.๑.๑ การจัดทำทะเบียนทรัพย์สิน (Inventory) ต้องจัดทำและรักษาทะเบียนทรัพย์สินของบริการที่สำคัญให้เป็นปัจจุบัน โดยต้องระบุรายละเอียดอย่างน้อย ดังนี้

ก) ชื่อและคำอธิบายของทรัพย์สินที่เกี่ยวข้องกับบริการที่สำคัญ

ข) ฟังก์ชันที่สำคัญของทรัพย์สินของบริการที่สำคัญของหน่วยงาน

ค) การระบุและจัดลำดับความสำคัญของทรัพย์สินต่อภารกิจของหน่วยงาน

ง) ระบุเจ้าของ (Asset Owner) หรือผู้รับผิดชอบดูแลทรัพย์สิน

จ) ระบุตำแหน่งทางกายภาพ (Physical Location) ของทรัพย์สินแต่ละรายการ

ฉ) ระบุความเชื่อมโยง (Dependencies) ของทรัพย์สินกับระบบหรือเครือข่าย ทั้งภายในและภายนอกหน่วยงาน

๑.๑.๒ การกำหนดขอบเขต ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) ให้ชัดเจน

๑.๑.๓ การตรวจสอบและทบทวน ต้องตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง และต้องปรับปรุงทันทีเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อบริการที่สำคัญ

๑.๑.๔ ภาระหน้าที่ตามกฎหมาย ตามมาตรา ๕๔ แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญและทรัพย์สินที่ระบุไว้ในทะเบียน อย่างน้อย ปีละ ๑ ครั้ง

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๑.๒.๑ รอบการประเมินความเสี่ยง มหาวิทยาลัยต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญและทรัพย์สินที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่มีผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๒.๒ ระดับของความเสี่ยงพิจารณาจากความสัมพันธ์ระหว่าง แนวโน้มหรือโอกาส (Likelihood) ที่จะเกิดเหตุการณ์ภัยคุกคาม และผลกระทบที่อาจเกิดขึ้น (Impact) โดยใช้เกณฑ์เมทริกซ์ความเสี่ยงขนาด ๓x๓ ดังนี้

ก) แนวโน้มหรือโอกาส (Likelihood) แบ่งเป็น ๓ ระดับ ประกอบด้วย สูง (๓) ปานกลาง (๒) และ ต่ำ (๑) โดยพิจารณาจากความสามารถในการค้นพบช่องโหว่ ความสามารถในการใช้ประโยชน์ และความสามารถในการทำซ้ำ

ข) ผลกระทบที่อาจเกิดขึ้น (Impact) แบ่งเป็น ๓ ระดับ ประกอบด้วย สูง (๓) ปานกลาง (๒) และ ต่ำ (๑) โดยพิจารณาจากความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมถึงผลกระทบด้านการเงิน การดำเนินงาน และชื่อเสียงของมหาวิทยาลัย

๑.๒.๓ มหาวิทยาลัยต้องกำหนดเกณฑ์การยอมรับความเสี่ยงเพื่อให้ฝ่ายบริหารตัดสินใจจัดการความเสี่ยงได้อย่างชัดเจน

ก) ความเสี่ยงระดับสูง (High) ไม่สามารถยอมรับได้ ต้องดำเนินการตามกลยุทธ์การลดความเสี่ยงหรือโอนย้ายความเสี่ยงทันที

ข) ความเสี่ยงระดับกลาง (Medium) ไม่สามารถยอมรับได้ ต้องมีแผนดำเนินการตอบสนองความเสี่ยงเพื่อลดระดับความเสี่ยงให้อยู่ในระดับต่ำภายในระยะเวลา ๓ - ๖ เดือน

ค) ความเสี่ยงระดับต่ำ (Low) เป็นระดับความเสี่ยงที่ ยอมรับได้ แต่มหาวิทยาลัยต้องมีการติดตามและเฝ้าระวังการเปลี่ยนแปลงของสถานการณ์เป็นระยะ

๑.๒.๔ ทะเบียนความเสี่ยง (Risk Register) ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยทะเบียนความเสี่ยงมีรายละเอียดอย่างน้อย ดังต่อไปนี้

ก) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

ข) คำอธิบายของความเสี่ยง (Description of the Risk)

ค) ระดับโอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

ง) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

จ) การจัดการความเสี่ยง (Risk Treatment)

ฉ) เจ้าของความเสี่ยง (Risk Owner)

ช) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) และ

ซ) ความเสี่ยงที่เหลือ (Residual Risk)

๑.๒.๕ กลยุทธ์ในการจัดการความเสี่ยง (Risk Response Options) เมื่อพบความเสี่ยงที่สูงกว่าระดับที่ยอมรับได้ มหาวิทยาลัยต้องเลือกดำเนินการอย่างใดอย่างหนึ่ง ได้แก่ การลดความเสี่ยง (Mitigate) การหลีกเลี่ยงความเสี่ยง (Avoid) การโอนย้ายความเสี่ยง (Transfer) หรือการยอมรับความเสี่ยง (Accept) โดยแผนจัดการความเสี่ยงทั้งหมดต้องได้รับการอนุมัติอย่างเป็นทางการจากผู้บริหารระดับสูง

๑.๒.๖ ดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) มหาวิทยาลัยต้องกำหนด KRI ที่วัดผลได้เพื่อใช้เป็นสัญญาณเตือนภัยล่วงหน้าและติดตามแนวโน้มความเสี่ยงอย่างต่อเนื่อง โดยต้องได้รับการอนุมัติจากผู้บริหารของหน่วยงานหรือผู้ที่ได้รับมอบหมาย

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (VA and Penetration Testing)

๑.๓.๑ ขอบเขตการประเมิน (VA) ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ ครอบคลุมทั้งระบบเทคโนโลยีสารสนเทศ (IT) และระบบควบคุมเครื่องจักร (ICS) โดยต้องประกอบด้วยการประเมินความปลอดภัยของโฮสต์ (Host) เครือข่าย (Network) และสถาปัตยกรรม (Architecture)

๑.๓.๒ การทดสอบก่อนเริ่มระบบ ต้องประเมินช่องโหว่ก่อนการทดสอบระบบใหม่ หรือก่อนการเปลี่ยนแปลงระบบที่สำคัญ เช่น การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๓ การทดสอบเจาะระบบ (Pentest) ควรดำเนินการอย่างน้อยปีละ ๑ ครั้ง ตามระดับความเสี่ยง โดยเน้นระบบที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing)

๑.๓.๔ คุณสมบัติผู้ทดสอบ ผู้ทดสอบเจาะระบบต้องมีการรับรอง (Certifications) ที่เป็นที่ยอมรับ และต้องเป็นอิสระจากระบบที่ทำการทดสอบ

๑.๓.๕ การรายงานผลตามกฎหมาย หากได้รับการร้องขอจากหน่วยงานกำกับดูแล ต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบภายใน ๓๐ วัน นับแต่วันที่ได้รับหนังสือร้องขอ

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

๑.๔.๑ ภาระรับผิดชอบ มหาวิทยาลัยต้องเป็นผู้รับผิดชอบ (Responsible) และ มีภาระรับผิดชอบ (Accountable) ต่อความปลอดภัยของโครงสร้างพื้นฐานสำคัญ แม้จะมีการจ้างงานภายนอก (Outsource) ก็ตาม

๑.๔.๒ ข้อกำหนดในสัญญา (Service Level Agreement: SLA) ต้องระบุข้อกำหนดด้านความปลอดภัยในสัญญาหรือ SLA อย่างชัดเจน เช่น ประเภทการเข้าถึงทรัพย์สิน ภาระหน้าที่ในการป้องกันภัยคุกคาม และสิทธิ์ของมหาวิทยาลัยในการตรวจสอบ (Audit) ความมั่นคงปลอดภัยของผู้ให้บริการ

**หัวข้อหลักที่ ๒** มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

เพื่อจำกัดหรือลดผลกระทบจากภัยคุกคามทางไซเบอร์ มหาวิทยาลัยต้องกำหนดมาตรการป้องกันที่เข้มงวด ดังต่อไปนี้

**กรอบมาตรฐาน**

๒.๑ การควบคุมการเข้าถึง (Access Control)

๒.๑.๑ การจำกัดสิทธิ์ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญถูกจำกัดไว้เฉพาะบุคลากร กิจกรรม อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตเท่านั้น

๒.๑.๒ การพิสูจน์ตัวตน ต้องใช้เทคนิคการตรวจสอบสิทธิ์ (Authentication) ที่แข็งแกร่งและสอดคล้องกับโปรไฟล์ความเสี่ยงของแต่ละโหมดการเข้าถึง

๒.๑.๓ การเก็บบันทึกและตรวจสอบ (Logs) ต้องเก็บรักษาบันทึกการเข้าถึง (Logs) ทั้งหมด รวมถึงความพยายามในการเข้าถึงที่ล้มเหลว และต้องตรวจสอบกิจกรรมที่ผิดปกติเป็นประจำอย่างต่อเนื่อง ซึ่งต้องเก็บรักษาไว้อย่างน้อย ๙๐ วัน เพื่อให้สอดคล้องกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๒.๑.๔ การกำกับดูแลการเชื่อมต่อ การเข้าถึงอินเทอร์เฟซทางกายภาพ (เช่น USB) หรือทางลอจิคอล (Logical) ของบริการที่สำคัญ ต้องกระทำภายใต้การดูแลของมหาวิทยาลัยและดำเนินการในสถานที่ที่กำหนดหากเป็นไปได้

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ มาตรฐานการกำหนดค่าขั้นต่ำ (Security Baseline) ต้องจัดทำมาตรฐาน Security Baseline สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ

๒.๒.๒ หลักการรักษาความมั่นคงปลอดภัย มาตรฐานข้างต้นต้องประกอบด้วยหลักการสำคัญดังต่อไปนี้

ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

ข) การแบ่งแยกหน้าที่ (Separation of Duties)

ค) การบังคับใช้นโยบายรหัสผ่านที่ซับซ้อน และการลบบัญชีที่ไม่ได้ใช้งาน

ง) การปิดพอร์ตเครือข่าย ลบบริการ และแอปพลิเคชันที่ไม่จำเป็น (เช่น คอมไพเลอร์)

จ) การป้องกันมัลแวร์ และการปรับปรุงซอฟต์แวร์/แพตช์ (Patch) อย่างทันการณ์

๒.๒.๓ การทบทวนและจัดการเปลี่ยนแปลง ต้องทบทวนมาตรฐาน Security Baseline อย่างน้อยปีละ ๑ ครั้ง และต้องมีกระบวนการจัดการการเปลี่ยนแปลง (Change Management Process) เพื่อควบคุมการแก้ไขระบบทุกครั้ง

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๒.๓.๑ การควบคุมการเปิดใช้งาน เปิดการเชื่อมต่อระยะไกลเฉพาะเมื่อจำเป็นเท่านั้น และใช้เทคนิคการพิสูจน์ตัวตนที่แข็งแกร่ง

๒.๓.๒ การเข้ารหัสข้อมูล ต้องใช้การเข้ารหัส (Encryption) สำหรับการเชื่อมต่อเครือข่ายทั้งหมด (เช่น HTTPS, SSH, SCP) เพื่อรักษาความสมบูรณ์ของข้อมูล

๒.๓.๓ ข้อจำกัดทางเทคนิค ไม่อนุญาตให้ใช้คำสั่งระบบ (System Commands) ผ่านการเชื่อมต่อระยะไกลที่ส่งผลกระทบต่อบริการสำคัญ เว้นแต่จะได้รับอนุญาตและจำเป็นทางธุรกิจ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ มาตรการควบคุมพอร์ต ปิดการใช้งานพอร์ตเชื่อมต่อภายนอก (เช่น USB) ทั้งหมด และเปิดใช้งานเฉพาะเมื่อจำเป็นด้วยอุปกรณ์ที่ได้รับอนุญาตเท่านั้น

๒.๔.๒ การตรวจสอบมัลแวร์ ต้องตรวจสอบมัลแวร์ก่อนการเชื่อมต่อทุกครั้ง และต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนที่อยู่บนสื่อบันทึกข้อมูลแบบถอดได้เสมอ

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒.๕.๑ กลุ่มเป้าหมาย จัดแผนงานสร้างความตระหนักรู้ให้ครอบคลุม เจ้าหน้าที่ใหม่ ผู้บริหาร เจ้าหน้าที่สนับสนุน (IT/ICS) ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

๒.๕.๒ เนื้อหาและการทบทวน สื่อสารข้อมูลภัยคุกคามและผลกระทบอย่างสม่ำเสมอ และต้องทบทวนแผนงานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

กำหนดขั้นตอนการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ภัยคุกคามและมาตรการบรรเทาผลกระทบให้กับบุคคลที่ได้รับผลกระทบ เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้ทันท่วงทีตามหลักเกณฑ์ที่ สกมช. กำหนด เพื่อความเป็นมาตรฐานในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

**หัวข้อหลักที่ ๓** มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

เพื่อให้สามารถตรวจพบเหตุการณ์ผิดปกติได้อย่างรวดเร็วและแม่นยำ มหาวิทยาลัยต้องดำเนินการดังต่อไปนี้

**กรอบมาตรฐาน**

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๓.๑.๑ การสร้างกลไกเฝ้าระวัง ต้องจัดให้มีระบบและกระบวนการที่สามารถตรวจจับเหตุการณ์ (Events) ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ได้ครอบคลุมทุกบริการที่สำคัญ

๓.๑.๒ การวิเคราะห์และจัดประเภท เมื่อตรวจพบเหตุการณ์ ต้องมีขั้นตอนการจัดประเภท (Classification) และวิเคราะห์เพื่อระบุว่าเป็นภัยคุกคามทางไซเบอร์ (Cyber Threat) หรือเหตุภัยคุกคาม (Incident) ที่ส่งผลกระทบต่อมหาวิทยาลัยหรือไม่

๓.๑.๓ การทบทวนประสิทธิภาพ ต้องทบทวนกลไกและกระบวนการตรวจจับอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าระบบเฝ้าระวังยังคงมีประสิทธิภาพต่อรูปแบบการโจมตีใหม่ ๆ

**หัวข้อหลักที่ ๔** มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

เมื่อเกิดเหตุการณ์ภัยคุกคาม ต้องมีกระบวนการตอบโต้ที่รวดเร็วเพื่อระงับความเสียหาย ซึ่งมหาวิทยาลัยต้องปฏิบัติตามกรอบมาตรฐาน ดังต่อไปนี้

**กรอบมาตรฐาน**

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๔.๑.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ที่เป็นลายลักษณ์อักษร และมีการสื่อสารให้บุคลากรที่เกี่ยวข้องทราบ โดยหากเกิดภัยคุกคามในระดับร้ายแรงหรือระดับวิกฤต มหาวิทยาลัยต้องรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน ๒๔ ชั่วโมง หลังจากการตรวจพบ

๔.๑.๒ ดำเนินการฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนสามารถดำเนินการได้อย่างมีประสิทธิผลและทันต่อสถานการณ์ปัจจุบัน

๔.๑.๓ จัดตั้งคณะทำงาน CIRT ประกอบด้วยผู้บัญชาการรับมือเหตุการณ์ และสมาชิกทีมจากฝ่ายโครงสร้างพื้นฐานและฝ่ายระบบสารสนเทศ โดยกำหนดช่องทางติดต่อสื่อสารผ่านสายด่วนภายในและกลุ่มสื่อสารฉุกเฉินที่สามารถใช้งานได้ตลอด ๒๔ ชั่วโมงในภาวะวิกฤต เพื่อให้การประสานงานรับมือเหตุการณ์เป็นไปอย่างรวดเร็วและเป็นระบบ

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๒.๑ ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต ประกอบด้วย

ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์แต่ละประเภท

ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

จ) ระบุแพลตฟอร์ม หรือช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๔.๒.๓ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต อย่างน้อยปีละหนึ่ง ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๔.๓.๑ ตามมาตรา ๒๒ วรรคหนึ่ง (๑๓) มหาวิทยาลัยต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าว อาจดำเนินการได้ทั้งในระดับชาติ หรือระดับภาคส่วนหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

๔.๓.๒ ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของมหาวิทยาลัย เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นตามข้อ ๔.๑ และข้อ ๔.๒ ที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของมหาวิทยาลัย

**หัวข้อหลักที่ ๕** มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

เพื่อให้มหาวิทยาลัย มั่นใจว่าบริการที่สำคัญจะสามารถกู้คืนสถานะและกลับมาดำเนินงานได้ตามปกติอย่างต่อเนื่องแม้เกิดเหตุภัยคุกคามทางไซเบอร์ที่รุนแรง มหาวิทยาลัยต้องปฏิบัติตามกรอบมาตรฐานดังต่อไปนี้

**กรอบมาตรฐาน**

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๕.๑.๑ มหาวิทยาลัยต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เป็นลายลักษณ์อักษร เพื่อรองรับเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก รวมถึงต้องสอบทานแผนของผู้ให้บริการภายนอก (Third Party) ให้สอดคล้องกับแผนของมหาวิทยาลัย ในเรื่องของขอบเขตและระยะเวลาการกู้คืน

๕.๑.๒ การจัดทำผลวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) มหาวิทยาลัยต้องระบุระยะเวลาเป้าหมายที่ต้องกู้คืนระบบให้กลับมาใช้งานได้ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดของข้อมูลที่ยอมให้สูญหายได้ (Recovery Point Objective: RPO) ของแต่ละบริการสำคัญให้ชัดเจน ได้แก่

ก) ระยะเวลาเป้าหมายในการกู้คืนระบบ (RTO) ไม่เกิน 48 ชั่วโมง

ข) ระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหายได้ (RPO) ไม่เกิน 4 ชั่วโมง

ค) บริการระบบสารสนเทศกลางต้องมีค่าระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerable Downtime: MTD) ไม่เกิน 24 ชั่วโมง

๕.๑.๓ มหาวิทยาลัยต้องกำหนดแนวทางการสำรองข้อมูล (Backup System) ที่สอดคล้องกับค่าระยะเวลาสูงสุดของข้อมูลที่ยอมให้สูญหายได้ และเลือกใช้เทคโนโลยีที่สามารถกู้คืนข้อมูลได้อย่างถูกต้องและรวดเร็ว โดยอาจพิจารณาจัดตั้งศูนย์ปฏิบัติงานสำรอง (Alternate Site) สำหรับบริการที่มีความเสี่ยงสูง

๕.๑.๔ มหาวิทยาลัยต้องดำเนินการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิผลของแผนและกลยุทธ์การกู้คืน รวมถึงเพื่อให้บุคลากรที่เกี่ยวข้องเข้าใจบทบาทหน้าที่และสามารถปฏิบัติงานได้จริงในภาวะวิกฤต

๕.๑.๕ มหาวิทยาลัยต้องทบทวนผลการวิเคราะห์ BIA อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงของระบบสารสนเทศอย่างมีนัยสำคัญ เพื่อให้ข้อกำหนดในการกู้ระบบและลำดับความสำคัญของการตอบสนองให้มีความทันสมัยและเหมาะสม

**หัวข้อหลักที่ ๖** แผนการตรวจสอบ (Audit Plan)

เพื่อให้มหาวิทยาลัยสามารถประเมินประสิทธิผลและความเหมาะสมของมาตรการควบคุมความเสี่ยง รวมถึงเพื่อให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สอดคล้องกับข้อกำหนดของกฎหมายและมาตรฐานสากล มหาวิทยาลัยต้องปฏิบัติตามกรอบมาตรฐานดังต่อไปนี้

**กรอบมาตรฐาน**

๖.๑ การวางแผนและการจัดให้มีการตรวจสอบ (Audit Planning and Engagement)

๖.๑.๑ มหาวิทยาลัยต้องจัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

๖.๑.๒ ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งอย่างเป็นทางการจากมหาวิทยาลัย โดยอาจเป็นผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบอิสระภายนอก (External Auditor)

๖.๑.๓ ผู้ตรวจสอบต้องมีความเป็นอิสระ ไม่มีผลประโยชน์ทับซ้อนกับระบบหรือส่วนงานที่ถูกตรวจสอบ และต้องมีความสามารถทางเทคนิคหรือใบรับรองวิชาชีพที่จำเป็นต่อการดำเนินการตรวจสอบ

๖.๑.๔ การดำเนินการตรวจสอบต้องยึดหลักความซื่อสัตย์ การนำเสนอผลตามข้อเท็จจริง ความรอบคอบเป็นมืออาชีพ และการรักษาความลับของข้อมูลอย่างเคร่งครัด

๖.๒ ขอบเขตและเกณฑ์การตรวจสอบ (Audit Scope and Criteria)

๖.๒.๑ ขอบเขตการตรวจสอบขั้นต่ำต้องครอบคลุมองค์ประกอบดังนี้

ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (BIA)

ข) บริการที่สำคัญ และทรัพย์สินสารสนเทศที่เกี่ยวข้องที่ระบุไว้ในทะเบียนทรัพย์สิน

ค) มาตรการควบคุมตามหัวข้อหลักที่ ๑-๕ ของประมวลแนวทางปฏิบัติฉบับนี้

ง) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองที่เกี่ยวข้อง

๖.๒.๒ นอกจากการตรวจสอบตามข้อกำหนดแล้ว ผู้ตรวจสอบควรประเมินความเหมาะสมของมาตรการควบคุมโดยอิงจากระดับความเสี่ยง และสถิติเหตุภัยคุกคามที่เคยเกิดขึ้นกับมหาวิทยาลัย

๖.๓ รายงานการตรวจสอบและการดำเนินการแก้ไข (Audit Reporting and Remediation)

๖.๓.๑ ผู้ตรวจสอบต้องจัดทำรายงานรายงานสรุปผลการตรวจสอบที่มีเนื้อหาอย่างน้อย ประกอบด้วย บทสรุปผู้บริหาร วัตถุประสงค์และขอบเขต สิ่งที่พบจากการตรวจสอบ (Audit Findings) และระดับความสอดคล้อง (Conformity/Non-Conformity)

๖.๓.๒ มหาวิทยาลัยต้องจัดทำแผนปฏิบัติการและเป้าหมายการดำเนินงาน เพื่อแก้ไขสิ่งที่พบว่าไม่สอดคล้องตามข้อกำหนด โดยต้องระบุมาตรการแก้ไข ผู้รับผิดชอบ และระยะเวลาดำเนินการให้ชัดเจน

๖.๓.๓ มหาวิทยาลัยต้องมีกระบวนการติดตามผลการแก้ไขความไม่สอดคล้องเพื่อให้มั่นใจว่าช่องโหว่หรือข้อบกพร่องที่พบได้รับการจัดการอย่างเหมาะสม

๖.๔ ภาระหน้าที่ตามกฎหมาย (Legal Obligations)

๖.๔.๑ ตามมาตรา ๕๔ แห่ง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มหาวิทยาลัยต้องจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จ

๖.๔.๒ กรณีที่มหาวิทยาลัยอยู่ภายใต้การกำกับดูแลเฉพาะด้าน ต้องจัดส่งสำเนารายงานให้หน่วยงานกำกับดูแลทราบตามระยะเวลาและวิธีการที่กำหนดด้วย