ประกาศมหาวิทยาลัยนเรศวร
เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
มหาวิทยาลัยนเรศวร

.....

เพื่อให้การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ เหมาะสมกับสภาพการณ์ปัจจุบัน มหาวิทยาลัยนเรศวร จึงกำหนดแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบ หรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของมหาวิทยาลัยนเรศวร เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็วและมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา ๒๐ มาตรา ๒๑ และมาตรา ๓๗ แห่งพระราชบัญญัติมหาวิทยาลัยนเรศวร พ.ศ. ๒๕๓๓ ประกอบกับมติคณะกรรมการบริหารมหาวิทยาลัยนเรศวร ในการประชุมครั้งที่ ๑๙/๒๕๖๖ เมื่อวันที่ ๑๗ ตุลาคม ๒๕๖๖ ให้กำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า ประกาศมหาวิทยาลัยนเรศวร เรื่อง “แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร ให้เป็นไปตามบัญชีแนบท้ายประกาศนี้

ข้อ ๔ ให้อธิการบดีเป็นผู้รักษาการตามประกาศนี้ กรณีที่มีปัญหาจากการปฏิบัติตามประกาศนี้ หรือที่ประกาศนี้มิได้กำหนดไว้ ให้อธิการบดีเป็นผู้วินิจฉัยและคำวินิจฉัยนั้นให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๒๗ ตุลาคม พ.ศ. ๒๕๖๖

(รองศาสตราจารย์ ดร.ศรินทร์ทิพย์ แทนธานี)
รักษาราชการแทนอธิการบดีมหาวิทยาลัยนเรศวร

บัญชีแนบท้ายประกาศมหาวิทยาลัยนเรศวร
เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
มหาวิทยาลัยนเรศวร
ฉบับลงวันที่ ๒๗ ตุลาคม พ.ศ. ๒๕๖๖

.....

๑. หลักการและเหตุผล

ตามที่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของมหาวิทยาลัยนเรศวร เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็วและมีประสิทธิภาพ

๒. วัตถุประสงค์

มหาวิทยาลัยนเรศวร ได้กำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีวัตถุประสงค์ ดังต่อไปนี้

๑) เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยนเรศวร มีแนวทางปฏิบัติและกรอบมาตรฐานที่มีประสิทธิภาพ และปฏิบัติได้อย่างถูกต้องตามกฎหมายต่าง ๆ ที่ได้กำหนดไว้

๒) เพื่อเผยแพร่แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้บุคลากรทุกระดับในมหาวิทยาลัยได้รับทราบและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์

๓) เพื่อกำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบเครือข่าย ผู้ดูแลระบบสารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย จะต้องปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดอย่างเคร่งครัด

๓. องค์ประกอบของแนวทางปฏิบัติและกรอบมาตรฐาน

แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มหาวิทยาลัยนเรศวร จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ เพื่อใช้เป็นแนวทางสำหรับ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบเครือข่าย ผู้ดูแลระบบสารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ให้ตระหนักถึงความมั่นคงปลอดภัยไซเบอร์และปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยที่กำหนดอย่างเคร่งครัด โดยแบ่งแนวปฏิบัติออกเป็นส่วน ๆ ดังต่อไปนี้

ส่วนที่ ๑ นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ส่วนที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ส่วนที่ ๓ แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑) การระบุความเสี่ยงที่อาจเกิดขึ้น (Identify)

๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

ส่วนที่ ๔ แผนรับมือภัยคุกคามทางไซเบอร์

ส่วนที่ ๕ นโยบายการสร้างความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. นิยามคำศัพท์

"มหาวิทยาลัย" หมายความว่า มหาวิทยาลัยนเรศวร

"ส่วนงาน" หมายความว่า สำนักงานอธิการบดี บัณฑิตวิทยาลัย คณะ วิทยาลัย สถาบัน สำนัก ศูนย์ และหน่วยงานที่เรียกชื่ออย่างอื่นมีฐานะเทียบเท่าคณะที่เป็นส่วนราชการและที่สภามหาวิทยาลัยประกาศจัดตั้ง

"ระบบเครือข่าย" หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย NU-NET

"ระบบสารสนเทศ" หมายความว่า ระบบงานของหน่วยงานที่ได้นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ และข้อมูลสารสนเทศ มาช่วยในการสร้างสารสนเทศที่หน่วยงาน สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการ การพัฒนาและควบคุม การติดต่อสื่อสาร เป็นต้น

"ผู้ใช้งาน" หมายความว่า บุคลากร นิสิต และนักเรียน ในสังกัดมหาวิทยาลัย หรือ บุคคลภายนอกที่ได้รับอนุญาตให้เข้าใช้งานระบบสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ NU-NET

"ผู้ดูแลระบบเครือข่าย" หมายความว่า บุคลากรในสังกัดมหาวิทยาลัยที่มีหน้าที่ดูแลระบบเครือข่ายคอมพิวเตอร์ NU-NET

"ผู้ดูแลระบบสารสนเทศ" หมายความว่า บุคลากรในสังกัดมหาวิทยาลัยที่มีหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่าย และฐานข้อมูลของระบบสารสนเทศในด้านต่าง ๆ

"ผู้ดูแลระบบ" หมายความว่า บุคลากรในสังกัดมหาวิทยาลัยที่มีหน้าที่ดูแลระบบเครือข่ายคอมพิวเตอร์ NU-NET หรือมีหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่าย หรือมีหน้าที่ดูแลฐานข้อมูลของระบบสารสนเทศในด้านต่าง ๆ

"ผู้บริหาร" หมายความว่า ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เหมือน CISO ของส่วนงาน

"ผู้ให้บริการภายนอก" หมายความว่า บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของมหาวิทยาลัย

ส่วนที่ ๑
นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย

๒. เพื่อเป็นการป้องกันและลดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้นกับระบบสารสนเทศของมหาวิทยาลัย

ผู้ปฏิบัติ

๑. ผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย

๒. ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

แนวทางปฏิบัติ

๑. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

๑.๑ ควรมีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยจัดโครงสร้างองค์กรพร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)

๑.๒ ส่วนงานมีการกำหนด ผู้รับผิดชอบในการทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยบุคคลดังกล่าวต้องเป็นผู้มีความรู้ หรือมีประสบการณ์ด้านเทคโนโลยีสารสนเทศ หรือเคยผ่านการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์

๑.๓ ควรมีคณะทำงานที่มีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) รวมทั้งควรมีบทบาทหน้าที่และความรับผิดชอบให้ส่วนงาน ดำเนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๑.๔ มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เหมือน CISO ของส่วนงาน

๒. การจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๒.๑ ต้องมีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์

๒.๒ ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสารสนเทศ ที่มีหน้าที่ดูแลระบบสำคัญของส่วนงาน/หน่วยงาน ต้องมีการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๓ มีการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทั้งหมด อย่างมีประสิทธิผล

๒.๔ มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๓. การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๓.๑ ต้องมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ตามเกณฑ์การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยที่กำหนด

๓.๒ ต้องมีการปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังจากการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒
การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของมหาวิทยาลัย สามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบเครือข่ายและผู้ดูแลระบบสารสนเทศในการปฏิบัติงานให้กับมหาวิทยาลัยเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์

ผู้ปฏิบัติ

๑. ผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย

๒. ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

แนวทางปฏิบัติ

๑. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๑ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

(๑) ให้ส่วนงาน/หน่วยงาน ตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

(๒) ให้ส่วนงาน/หน่วยงาน ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่ดำเนินการโดยผู้ตรวจสอบจากภายใน (Internal Auditor) หรือโดยผู้ตรวจสอบจากภายนอก (External Auditor) เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยไซเบอร์

(๓) มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๒ กำหนดให้มีการประเมินความเสี่ยง (Risk Management) ดังนี้

(๑) มีการระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่างๆ

(๒) มีความเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(๓) มีการประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๑.๓ กำหนดให้มีการจัดการความเสี่ยง (Risk Treatment) ดังนี้

(๑) มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

(๒) มีการกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินงาน ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน

๑.๔ การรายงานความเสี่ยง (Risk Reporting) ดังนี้

(๑) มีการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ

(๒) มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๒. กำหนดให้มีการรายงานผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และแจ้งคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยเพื่อรับทราบ

ส่วนที่ ๓
แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วัตถุประสงค์

๑. เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

๒. เพื่อให้มีแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของมหาวิทยาลัย

๓. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์

ผู้ปฏิบัติ

๑. ผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย

๒. ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๒. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔

๓. กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ NIST Cybersecurity

แนวทางปฏิบัติ

๑. การระบุความเสี่ยงที่อาจเกิดขึ้น (Identify)

๑.๑ การจัดการทรัพย์สิน (Asset Management)

(๑) มีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญและดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน

(๒) มีการระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

(๓) มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญตามรายการที่ระบุไว้ในทะเบียนทรัพย์สิน

(๔) มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลงใดๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๒ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(๑) มีการประเมินช่องโหว่ของบริการที่สำคัญ อ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน โดยครอบคลุมบริการที่สำคัญซึ่งเป็นระบบเทคโนโลยีสารสนเทศ (Information Technology system) และระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

(๒) ขอบเขตของการประเมินช่องโหว่ของบริการที่สำคัญครอบคลุมการประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม

(๓) มีการประเมินช่องโหว่ของบริการที่สำคัญก่อนที่จะทำการทดสอบระบบใหม่ใดๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ

(๔) ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

(๕) มีการตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) ได้รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ

(๖) ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง ตามความจำเป็น

(๗) มีการตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระ

(๘) มีการตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

(๙) มีกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

๑.๒ การจัดการผู้ให้บริการภายนอก (Third-Party Management)

(๑) ผู้ให้บริการภายนอกต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ แม้ว่าจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญ

(๒) มีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก

(๓) ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา

(๔) ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

(๑) มีการจำกัดการเข้าถึงบริการที่สำคัญเฉพาะบุคลากร กิจกรรม อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตเท่านั้น

(๒) มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

(๓) มีการเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ

(๔) มีการตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ และการเข้าถึงทางลอจิกคอล (Logical) มีการกำกับดูแลโดยหน่วยงาน และดำเนินการในสถานที่ หากเป็นไปได้

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(๑) มีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)

(๒) มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังนี้

- บุคลากร และกิจกรรมที่ได้รับอนุญาต และ
- อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

(๓) มีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ

(๔) มีการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีกระบวนการจัดการเปลี่ยนแปลง (Change Management Process)

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

(๑) มีการตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ

(๒) มีการปฏิบัติตามแนวทางปฏิบัติ ดังนี้

- ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น
- ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง
- ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น
- ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญหน่วยงานของมหาวิทยาลัย เว้นแต่จะได้รับอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(๑) มีการควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา กับบริการที่สำคัญ

(๒) มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

(๑) มีแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้

(๒) มีการทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

(๑) แบ่งปันข้อมูล ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสารสนเทศ เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าว

๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

(๑) มีการสร้างกลไกและกระบวนเพื่อตรวจจับ จัดประเภท วิเคราะห์ และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ

(๒) มีการทบทวนกลไกและกระบวนการภายใน อย่างน้อยปีละ ๑ ครั้ง ดังนี้

- ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของมหาวิทยาลัย

- การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และการระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของมหาวิทยาลัยหรือไม่

๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)

๔.๑ มีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

(๑) มีการจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) มีแผนการสื่อสารในภาวะวิกฤต ซึ่งกำหนดรายละเอียด ดังนี้

- จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานช่วงวิกฤต
- ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ข้อมูลที่เหมาะสม
- ระบุผู้เชี่ยวชาญด้านเทคนิค เพื่อแก้ไขปัญหาในภาวะวิกฤต

- ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

- ระบุสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง

(๓) มีการตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ

(๔) มีการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง

๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

(๑) มีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งส่วนของมหาวิทยาลัยหรือส่วนงาน

(๒) มีการตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

(๓) มีการปฏิบัติตามคำขอใด ๆ ของมหาวิทยาลัย เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของส่วนงาน เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์

ส่วนที่ ๔
แผนรับมือภัยคุกคามทางไซเบอร์

วัตถุประสงค์

๑. เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย

๒. เพื่อให้มีการดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของมหาวิทยาลัย และส่วนงาน รวมถึงพฤติกรรมแวดล้อม สำหรับการรับมือภัยคุกคามทางไซเบอร์

๓. เพื่อเป็นการป้องกันและลดความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้ปฏิบัติ

๑. ผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย

๒. ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

แนวทางปฏิบัติ

๑. การเตรียมการป้องกันการเกิดภัยคุกคามทางไซเบอร์

๑.๑ จัดเตรียมเครื่องมือและสิ่งอำนวยความสะดวกในการสื่อสารของบุคลากรที่ทำหน้าที่รับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์

๑.๒ กำหนดรายชื่อและช่องทางในการติดต่อผู้ที่เกี่ยวข้อง และประสานงานในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์

๑.๓ กำหนดช่องทางการรายงานเหตุการณ์ โดยให้ผู้ที่ได้รับผลกระทบหรือพบเห็นเหตุการณ์แจ้งมายังกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๔ กำหนดสถานที่จัดเก็บข้อมูลหลักฐานที่สำคัญ ในสถานที่ที่มีความมั่นคงปลอดภัยไซเบอร์ (Secure Storage Facility)

๑.๕ มีเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์

๑.๖ รายงานสถานการณ์ดำเนินการของเหตุการณ์โดยเร็ว

๒. การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

๒.๑ กำหนดวิธีการที่จะใช้ในการตรวจจับ (Incident)

(๑) ควรจะมีการติดตั้งอุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับตามความเหมาะสมกับระบบที่ต้องการป้องกัน

(๒) สอดส่องดูแล ตรวจจับความผิดปกติอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบสารสนเทศ และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายที่ผิดปกติให้รายงานต่อผู้อำนวยการหรือผู้ที่ได้รับมอบหมายจากกองบริการเทคโนโลยีสารสนเทศและการสื่อสารทราบโดยทันที

(๓) มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสมและสามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(๔) มีกลไกแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน

(๕) มีกระบวนการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident, Respond, Capability, Testing)

๒.๒ การติดต่อประสานงานและแจ้งข้อมูล

ทีมงานรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ต้องแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามทางไซเบอร์กับผู้ที่เกี่ยวข้อง เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่กำหนดไว้ ดังนี้

ลำดับ	ผู้ที่เกี่ยวข้อง	หน้าที่
๑	ผู้ที่ได้ผลกระทบจากภัยคุกคามทางไซเบอร์	แจ้งเหตุหรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบหรือสงสัยว่ามีภัยคุกคามที่เกิดขึ้น
๒	ผู้รับแจ้งเหตุ	รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์
๓	ทีมงานรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์	๑. รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ๒. ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ทุกส่วนงาน ๓. มีส่วนร่วมกับหน่วยงานภายนอกมหาวิทยาลัย เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์ รวมถึงแจ้งไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ เพื่อป้องกันและตอบสนองภัยคุกคามได้เร็วขึ้น
๔	ทีมงานเฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามทางไซเบอร์	๑. เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับ ๒. ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ทุกส่วนงานทราบ ๓. มีส่วนร่วมกับหน่วยงานภายนอกมหาวิทยาลัย เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์ รวมถึงแจ้งไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ เพื่อป้องกันและตอบสนองภัยคุกคามได้เร็วขึ้น
๕	ผู้บริหาร	กำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหาและสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับ ควบคุมเจ้าหน้าที่ที่เกี่ยวข้องกับการป้องกันความมั่นคงปลอดภัยไซเบอร์

หมายเหตุ ทีมรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ และทีมงานเฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามทางไซเบอร์ ควรเป็นบุคลากรที่มีความรู้ ความสามารถ มีประสบการณ์ ผ่านการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ที่มีการรับรอง Certification และความเชี่ยวชาญเฉพาะด้าน

๓. การระงับภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบที่ได้รับผลกระทบ

๓.๑ การควบคุมความเสียหายในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์ คือ การตัดสินใจเลือกใช้วิธีการที่เหมาะสมตามสถานการณ์ของภัยคุกคามที่กำลังเผชิญ ดังนี้

(๑) ปิดระบบ (Shutdown)

(๒) ตัดการเชื่อมต่อระบบเครือข่ายทั้งหมด ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับกระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์ (Endpoint Detection & Response Agent)

(๓) หยุดการทำงานของฟังชันที่เกี่ยวข้อง (Disabling Certain Functions)

๓.๒ การจัดเก็บและดูแลรักษาหลักทางทางดิจิทัล

(๑) มีแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่างๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ

(๒) การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ให้เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล

(๓) หลักฐานมีบันทึกการเข้าถึงและการกระทำใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม

๓.๓ การกำจัดสาเหตุภัยคุกคามทางไซเบอร์

(๑) การปิดช่องโหว่ของระบบ

(๒) การยกเลิกเพิกถอนการอนุญาต User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ

(๓) การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน

(๔) การลบโปรแกรมประเภท Backdoor ออกจากระบบสารสนเทศ

(๕) การใช้ข้อมูล Indicator of Compromise (Ioc) ในการสแกนหา Malware หรือร่องรอยอื่นๆ ในระบบที่ยังหลงเหลือ เพื่อดำเนินการกำจัดให้ออกจากระบบสารสนเทศทั้งหมด

๓.๔ การกู้คืนระบบให้กลับมาทำงานปกติ หลังจากดำเนินการควบคุมความเสียหายและกำจัดสาเหตุของภัยคุกคามเสร็จสิ้นแล้ว

(๑) จะต้องดำเนินตามนโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ เพื่อให้การกู้คืนข้อมูลของระบบมีความสมบูรณ์และสามารถกลับมาทำงานได้ตามปกติ

(๒) การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย

(๓) การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

๔. การดำเนินการภายหลังการแก้ไขปัญหาภัยคุกคามทางไซเบอร์

๔.๑ ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบของมหาวิทยาลัย

มหาวิทยาลัยนเรศวร

๔.๒ จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน เพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจัดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต

๔.๓ การดำเนินการเก็บรักษาข้อมูลและพยานหลักฐานที่เกี่ยวข้อง

เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และแก้ไขเพิ่มเติม หรือกฎหมายอื่นๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภท อาจจำเป็นต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี โดยหลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญ มีดังนี้

(๑) Assessment : การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของภัยคุกคามทางไซเบอร์ ที่กำลังรับมือและตอบสนอง

(๒) Acquisition : ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนาด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้

- ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker
- ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟฟ้าคอยเลี้ยง
- ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด
- ต้องทำการจดบันทึกหลักฐาน (Chain of Custody)

(๓) Authentication : ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับด้วยวิธี Cryptographic Hash เช่น MD๕, SHA๑, SHA๒๕๖

(๔) Analysis & Report : วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิดภัยคุกคามทางไซเบอร์

(๕) Archive : จัดเก็บหลักฐานไว้ในที่ที่เหมาะสม ปลอดภัย และบันทึกหลักฐาน (Chain of Custody) ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย

<u>หมายเหตุ</u> Chain of Custody หรือ ห่วงโซ่การคุ้มครองพยานหลักฐาน คือ เอกสารแสดงลำดับการเกิดเหตุการณ์ หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ยืนยันในชั้นศาล หลักฐานเหล่านี้จึงจะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือจัดทำขึ้นมา

ส่วนที่ ๕
นโยบายการสร้างความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วัตถุประสงค์

๑. เพื่อเผยแพร่แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรทุกระดับในมหาวิทยาลัยได้รับทราบและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์

ผู้ปฏิบัติ

๑. ผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย

๒. ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

แนวทางปฏิบัติ

๑. จัดให้มีการฝึกอบรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ของมหาวิทยาลัย อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงระบบการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติให้ลักษณะเกร็ดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายโดยมีการปรับปรุงความรู้อยู่เสมอ

๓. ส่วนงาน ควรส่งเสริมให้ผู้ดูแลระบบ เข้ารับการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์