**แบบประเมินความสอดคล้อง**

**ของประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

คำชี้แจง :

1. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย ประมวลแนวทางปฏิบัติ จำนวน ๓ ข้อ และกรอบมาตรฐาน จำนวน ๑๕ ข้อ
2. เนื่องจากมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ จะต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานให้สอดคล้องกับประกาศดังกล่าว ทั้งในส่วนของประมวลแนวทางปฏิบัติ จำนวน ๓ ข้อ และกรอบมาตรฐาน จำนวน ๑๕ ข้อ ซึ่งอาจมีเอกสารที่ต้องดำเนินการเป็นจำนวนมาก สำนักงานจึงกำหนดให้หน่วยงานเริ่มดำเนินการในส่วนของประมวลแนวทางปฏิบัติทั้ง ๓ ข้อก่อน โดยให้แล้วเสร็จภายในวันที่ ๑๕ กันยายน ๒๕๖๖ ทั้งนี้ สำนักงานจะได้พิจารณาแจ้งให้หน่วยงานได้ดำเนินการจัดทำในส่วนของกรอบมาตรฐานเป็นลำดับต่อไป
3. แบบประเมินนี้ มีวัตถุประสงค์เพื่อช่วยให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ นำไปใช้ในการประเมินว่าประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน มีความสอดคล้องกับประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน ๓ ข้อ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ หรือไม่
4. การประเมินความสอดคล้องนี้ หน่วยงานจำเป็นต้องอ้างถึงหลักฐานที่ชัดเจนว่าได้มีการดำเนินการอย่างไร พร้อมแนบหลักฐานดังกล่าวมายังสำนักงาน ทั้งนี้ หน่วยงานของท่านอาจพิจารณาปิด (Masking) ส่วนของข้อมูลที่มีความอ่อนไหว (Sensitive data) ได้ และการประเมินโดยหน่วยงานของท่านเป็นเพียงการประเมินขั้นต้นเท่านั้น ยังไม่ถือว่าได้มีการจัดทำแผนรับมือฯ สอดคล้องกับประกาศดังกล่าวข้างต้น จนกว่าสำนักงานจะได้ตรวจสอบแล้วเสร็จ และแจ้งเป็นหนังสือรับรองกลับไปยังหน่วยงานเป็นลายลักษณ์อักษร แล้วเท่านั้น

| **ข้อ** | **รายการ** | **สถานะ****ปัจจุบัน** | **หลักฐาน\*** |
| --- | --- | --- | --- |
| **มี** | **ไม่มี** |
|  | **แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** |  |  |  |
| ๑๗.๑ | ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้ | 🗹 |  | หน่วยตรวจสอบภายใน |
|  | (ก) กระบวนการจัดทําและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) |  | 🗹 |  |
|  | (ข) บริการที่สําคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก) |  | 🗹 |  |
|  | (ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกําหนด | 🗹 |  | 1.ประกาศ มทส. เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีสุรนารี พ.ศ. 25542.ระเบียบ มหาวิทยาลัยเทคโนโลยีสุรนารี ว่าด้วยการรักษาความปลอดภัย- ด้านเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีสุรนารี พ.ศ. 2564 |
| ๑๗.๒ | หน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสํานักงานภายในกําหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดําเนินการแล้วเสร็จตามที่กําหนดไว้ในมาตรา ๕๔ พร้อมทั้งส่งสําเนาให้หน่วยงานควบคุมหรือกํากับดูแลด้วย |  | 🗹 |  |
| ๑๗.๓ | ในกรณีที่การตรวจสอบดําเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑๗.๑ เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศส่งแผนการดําเนินการแก้ไขไปยังสํานักงานภายในกําหนด ๓๐ (สามสิบ) วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดําเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้ |  |  |  |
|  | (ก) ให้รายละเอียดการดําเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศจะดําเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ |  | 🗹 |  |
|  | (ข) กําหนดระยะเวลาสําหรับการดําเนินการตามที่ระบุไว้ในข้อ ๑๗.๓ (ก) |  | 🗹 |  |
| ๑๗.๔ | ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดําเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศดําเนินการและส่งแผนการดําเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสํานักงานภายในระยะเวลาที่ กกม. กําหนด พร้อมส่งทั้งสําเนาให้หน่วยงานควบคุมหรือกํากับดูแลด้วย |  | 🗹 |  |
| ๑๗.๕ | ๑๗.๕ เมื่อแผนการดําเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศจะดําเนินการตามแผนการดําเนินการแก้ไขดังกล่าว และดําเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกําหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม. |  | 🗹 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** |  |  |  |
|  | หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศต้องกําหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สําหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนํานโยบายดังกล่าวมาจัดทําระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้ |  |  |  |
| ๑๘.๑ | การประเมินความเสี่ยง (Risk Assessment) |  |  |  |
|  | (ก) การระบุความเสี่ยง (Risk Identification)ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก | 🗹 |  | ระบบความเสี่ยง มหาวิทยาลัยเทคโนโลยีสุรนารี http://ascend.sut.ac.th/rm2018/ |
|  | (ข) การวิเคราะห์ความเสี่ยง (Risk Analysis)ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม | 🗹 |  | ระบบความเสี่ยง มหาวิทยาลัยเทคโนโลยีสุรนารี http://ascend.sut.ac.th/rm2018/ |
|  | (ค) การประเมินค่าความเสี่ยง (Risk Evaluation)ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดําเนินธุรกิจ รวมถึงกําหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite) | 🗹 |  | ระบบความเสี่ยง มหาวิทยาลัยเทคโนโลยีสุรนารี http://ascend.sut.ac.th/rm2018/ |
| ๑๘.๒ | การจัดการความเสี่ยง (Risk Treatment) |  |  |  |
|  | ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคํานึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ | 🗹 |  | ระบบความเสี่ยง มหาวิทยาลัยเทคโนโลยีสุรนารี http://ascend.sut.ac.th/rm2018/ |
|  | นอกจากนี้ต้องกําหนดดัชนีชี้วัดความเสี่ยงที่สําคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดําเนินธุรกิจ ให้สอดคล้องกับความสําคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง | 🗹 |  | ระบบความเสี่ยง มหาวิทยาลัยเทคโนโลยีสุรนารี http://ascend.sut.ac.th/rm2018/ |
| ๑๘.๓ | การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) | 🗹 |  |  |
|  | ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กําหนดไว้ |  |  | ระบบความเสี่ยง มหาวิทยาลัยเทคโนโลยีสุรนารี http://ascend.sut.ac.th/rm2018/ |
| ๑๘.๔ | การรายงานความเสี่ยง (Risk Reporting) |  |  |  |
|  | ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจํา เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย | 🗹 |  | ระบบความเสี่ยง มหาวิทยาลัยเทคโนโลยีสุรนารี http://ascend.sut.ac.th/rm2018/ |
|  | ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสําคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสําคัญ เป็นต้น | 🗹 |  | ระบบความเสี่ยง มหาวิทยาลัยเทคโนโลยีสุรนารี http://ascend.sut.ac.th/rm2018/ |
|  | **แผนการรับมือภัยคุกคามทางไซเบอร์** |  |  |  |
| ๑๙.๑ | ต้องจัดทําแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กําหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้ | 🗹 |  | (ร่าง) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) |
|  | (ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กําหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ |  | 🗹 |  |
|  | (ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกําหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทําขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกําหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสําคัญทางสารสนเทศ |  | 🗹 |  |
|  | (ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT |  | 🗹 |  |
|  | (ง) ขั้นตอนจํากัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ |  | 🗹 |  |
|  | (จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process) | 🗹 |  | แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan) |
|  | (ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์ |  | 🗹 |  |
|  | (ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน |  | 🗹 |  |
|  | (ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสําหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดําเนินคดี และ |  | 🗹 |  |
|  | (ฌ) กระบวนการทบทวนหลังการดําเนินการ (After-Action Review Process) เพื่อระบุและแนะนําให้ปรับปรุงการดําเนินการเพื่อป้องกันการเกิดซ้ำ |  | 🗹 |  |
| ๑๙.๒ | ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสําคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศ |  | 🗹 |  |
| ๑๙.๓ | ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ |  | 🗹 |  |
| ๑๙.๔ | ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสําคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่ สําคัญของหน่วยงานของรัฐและ หน่วยงานโครงสร้างพื้นฐานสําคัญทางสารสนเทศ หรือข้อกําหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ |  | 🗹 |  |

ลงชื่อ\*\* ..........................................................

( )

\*หลักฐานที่หน่วยงานอ้างถึง จะต้องนำส่งมายังสำนักงานด้วยวิธีการแบบปลอดภัย โดยอาจนำส่งโดยผู้นำสาร หรือด้วยวิธีการทางอิเล็กทรอนิกส์ (PGP) ตามคู่มือที่ส่งมาด้วย ทั้งนี้ หน่วยงานของท่านอาจพิจารณาปิด (Masking) ส่วนของข้อมูลที่มีความอ่อนไหว (Sensitive data) ได้

\*\*ผู้ลงชื่อ หมายถึง ผู้ที่ทำหน้าที่ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (Chief Information Security Officer : CISO) หรือ ผู้บริหารด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือ ผู้บริหารที่ได้รับมอบอำนาจจากผู้บริหารสูงสุดของหน่วยงานให้รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์