

ส่วนราชการ สป.ยธ. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทร. ๐ ๒๑๔๑ ๕๔๗๒

ที่ ยธ ๐๒๐๐๖/๓๘๖๕

วันที่ ๗ เมษายน ๒๕๖๖

เรื่อง ขอส่งประกาศกระทรวงยุติธรรม เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม พ.ศ. ๒๕๖๖

เรียน อธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ ได้กำหนดให้หน่วยงานของรัฐ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ดังนั้น เพื่อให้กระทรวงยุติธรรมมีมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ที่สอดคล้องกับพระราชบัญญัตินี้ สำนักงานปลัดกระทรวงยุติธรรม จึงได้ดำเนินการจัดทำประกาศกระทรวงยุติธรรม เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม พ.ศ. ๒๕๖๖

ในการนี้ สำนักงานปลัดกระทรวงยุติธรรม จึงขอจัดส่งประกาศกระทรวงยุติธรรม เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม พ.ศ. ๒๕๖๖ รายละเอียดปรากฏตามเอกสารแนบ มายังท่านเพื่อทราบและแจ้งบุคลากรในกำกับดูแลได้รับทราบและถือปฏิบัติต่อไป ทั้งนี้ สำนักงานปลัดกระทรวงยุติธรรม ได้ดำเนินการประชาสัมพันธ์ผ่านเว็บไซต์ของสำนักงานปลัดกระทรวงยุติธรรม (<https://www.moj.go.th/view/82902>) อีกช่องทางหนึ่งด้วย

จึงเรียนมาเพื่อทราบ และถือปฏิบัติต่อไป



(นางอรรณญา ทองน้ำตะโก)

รองปลัดกระทรวงยุติธรรม

ปฏิบัติราชการแทนปลัดกระทรวงยุติธรรม



ประกาศกระทรวงยุติธรรม  
เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม  
พ.ศ. ๒๕๖๖

-----

เพื่อให้การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรมเป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว และเพื่อให้มาตรฐานความปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรมเกิดความชัดเจน เป็นไปในทิศทางเดียวกัน และสอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๒๑ (๑) แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๔๓๔ และที่แก้ไขเพิ่มเติม ประกอบมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ปลัดกระทรวงยุติธรรมจึงออกประกาศมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม ดังต่อไปนี้

ข้อ ๑ ให้ส่วนราชการในสังกัดกระทรวงยุติธรรมปฏิบัติตามมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรมตามบัญชีแนบท้ายประกาศนี้

ข้อ ๒ กรณีที่มีการแก้ไขเพิ่มเติมมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่แตกต่างไปจากที่กำหนดไว้ในประกาศนี้ ให้ส่วนราชการในสังกัดกระทรวงยุติธรรมถือปฏิบัติตามที่ได้มีการแก้ไขหรือเพิ่มเติมนั้น

ข้อ ๓ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน

ให้ส่วนราชการในสังกัดกระทรวงยุติธรรมที่ถูกกำหนดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ปฏิบัติตามหลักเกณฑ์ว่าด้วยแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ประกาศ ณ วันที่ ๒๘ เดือน มีนาคม พ.ศ. ๒๕๖๖

**นางพงษ์สวาท**

(นางพงษ์สวาท กายอรุณสุทธิ์)

ปลัดกระทรวงยุติธรรม

บัญชีแนบท้ายประกาศกระทรวงยุติธรรม  
เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์  
ของกระทรวงยุติธรรม พ.ศ. ๒๕๖๖

## สารบัญ

|                                                                                                                                                                                          |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| ๑. บทนำ                                                                                                                                                                                  | ๑  |
| ๒. วัตถุประสงค์                                                                                                                                                                          | ๑  |
| ๓. ขอบเขตการใช้                                                                                                                                                                          | ๑  |
| ๔. คำนิยาม                                                                                                                                                                               | ๑  |
| ๕. การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม<br>สำหรับส่วนราชการในสังกัดกระทรวงยุติธรรม มี ๒ ส่วน                                                 | ๒  |
| ส่วนที่ ๑ ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์                                                                                                                            | ๒  |
| ๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์                                                                                                                                     | ๒  |
| ๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์                                                                                                                              | ๒  |
| ๓. แผนการรับมือภัยคุกคามทางไซเบอร์                                                                                                                                                       | ๓  |
| ๔. การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์                                                                                                                               | ๔  |
| ส่วนที่ ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์                                                                                                                                | ๕  |
| หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์<br>ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์<br>ทรัพย์สิน และชีวิตร่างกายของบุคคล (Identify) | ๕  |
| ๑.๑ การจัดการทรัพย์สิน (Asset Management)                                                                                                                                                | ๕  |
| ๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง<br>(Risk Assessment and Risk Management Strategy)                                                                                | ๕  |
| ๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ<br>(Vulnerability Assessment and Penetration Testing)                                                                                          | ๖  |
| ๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)                                                                                                                                 | ๗  |
| หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)                                                                                                                             | ๘  |
| ๒.๑ การควบคุมการเข้าถึง (Access Control)                                                                                                                                                 | ๘  |
| ๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)                                                                                                                                       | ๘  |
| ๒.๓ การเชื่อมต่อระยะไกล (Remote Control)                                                                                                                                                 | ๙  |
| ๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)                                                                                                                                    | ๙  |
| ๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์<br>(Cybersecurity Awareness)                                                                                                      | ๑๐ |
| ๒.๖ การแบ่งปันข้อมูล (Information Sharing)                                                                                                                                               | ๑๐ |
| หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)                                                                                                                       | ๑๐ |
| หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)                                                                                                                | ๑๑ |
| ๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์<br>(Cybersecurity Incident Response Plan)                                                                                                            | ๑๑ |
| ๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)                                                                                                                                 | ๑๑ |
| หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคาม<br>ทางไซเบอร์ (Cybersecurity Resilience and Recovery)                                                                    | ๑๑ |



บัญชีแนบท้ายประกาศกระทรวงยุติธรรม  
เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม  
พ.ศ. ๒๕๖๖

\*\*\*\*\*

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ ได้กำหนดให้หน่วยงานของรัฐ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว กระทรวงยุติธรรมในฐานะหน่วยงานของรัฐได้ให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานในสังกัดกระทรวงยุติธรรม จึงดำเนินการจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม โดยกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ หรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานในสังกัดกระทรวงยุติธรรมปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ของกระทรวงยุติธรรมจึงมีการแต่งตั้งคณะอนุกรรมการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม เป็นผู้รับผิดชอบในการ กำกับ ติดตาม และประเมินผลการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานในสังกัดกระทรวงยุติธรรม ตลอดจนประสานความร่วมมือระหว่างหน่วยงานเพื่อเร่งรัดการดำเนินงานตลอดจนแก้ไขอุปสรรคที่เกิดขึ้น

๒. วัตถุประสงค์

เพื่อการจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม และยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงยุติธรรมในภาพรวมให้ชัดเจนและเป็นไปในทิศทางเดียวกัน

๓. ขอบเขตการใช้

ใช้กับส่วนราชการในสังกัดกระทรวงยุติธรรม

๔. คำนิยาม

|                                          |         |                                                                        |
|------------------------------------------|---------|------------------------------------------------------------------------|
| หน่วยงาน                                 | หมายถึง | ส่วนราชการในสังกัดกระทรวงยุติธรรม                                      |
| หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ | หมายถึง | หน่วยงานของรัฐที่ถูกประกาศเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ |
| คณะกรรมการ                               | หมายถึง | คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ของกระทรวงยุติธรรม              |
| คณะอนุกรรมการ                            | หมายถึง | คณะอนุกรรมการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม         |
| Recovery Time Objective (RTO)            | หมายถึง | ระยะเวลาในการกู้คืนระบบ                                                |
| Recovery Point Objective (RPO)           | หมายถึง | ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย                                   |

|                                               |         |                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum Tolerance Period of Disruption (MTPD) | หมายถึง | ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด |
| Business Continuity Plan                      | หมายถึง | แผนบริหารความต่อเนื่องทางธุรกิจ                                                                                                                                                                                                                                                          |

๕. การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรมสำหรับส่วนราชการในสังกัดกระทรวงยุติธรรม มี ๒ ส่วน ดังนี้

## ส่วนที่ ๑

### ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

#### แนวปฏิบัติ

#### ๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๑ หน่วยงานต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบอย่างน้อย ดังนี้

๑) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน

๑.๒ หน่วยงานต้องจัดส่งรายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอกมายังคณะอนุกรรมการ ภายในสามสิบ (๓๐) วันนับถัดจากวันที่ได้รับรายงานการตรวจสอบ

#### ๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทําระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

##### ๒.๑ การประเมินความเสี่ยง (Risk Assessment)

##### ๑) การระบุความเสี่ยง (Risk Identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก



## ๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

เข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

## ๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

ประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจรวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

### ๒.๒ การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

### ๒.๓ ติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

### ๒.๔ การรายงานความเสี่ยง (Risk Reporting)

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการ ตามรอบการประชุมของคณะกรรมการ

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

## ๓. แผนการรับมือภัยคุกคามทางไซเบอร์

หน่วยงานต้องดำเนินการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

### ๓.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

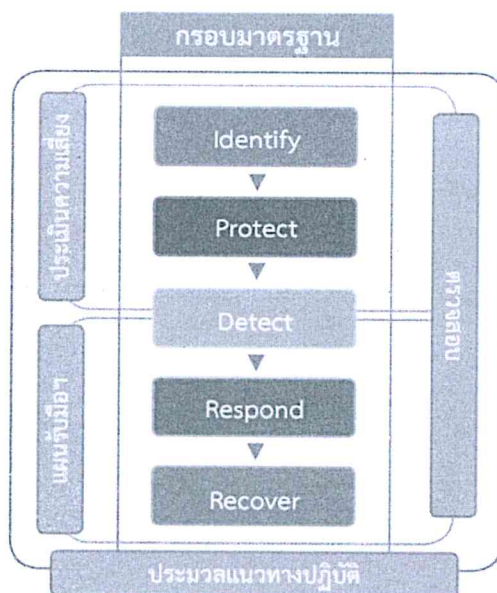
### ๓.๒ ตรวจสอบแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิภาพไปยังบุคลากรที่เกี่ยวข้อง

### ๓.๓ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

### ๓.๔ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงาน หรือข้อกำหนด ในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

### ๓.๕ ฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง





รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

#### ๔. การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์มายังคณะอนุกรรมการอย่างน้อยดังนี้

- ๔.๑ แผนนโยบายหรือแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ๔.๒ เหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) ที่ตรวจพบ และผลดำเนินการในการตรวจสอบเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) (ถ้ามี)
- ๔.๓ การดำเนินการเพื่อทำให้ระบบความมั่นคงปลอดภัยมีความแข็งแกร่ง (Hardening)
- ๔.๔ การดำเนินการทางกฎหมายที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident)
- ๔.๕ การพัฒนาด้านบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์
- ๔.๖ การรายงานปัญหาและอุปสรรคที่เกิดขึ้นในด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

## ส่วนที่ ๒

### กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

#### ๑.๑ การจัดการทรัพย์สิน (Asset Management)

การจัดเก็บรายละเอียดข้อมูลของอุปกรณ์ด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทั้งหมดของระบบเพื่อใช้ในการวางแผนและการบริหารด้านความมั่นคงปลอดภัยทางไซเบอร์

๑.๑.๑ หน่วยงานต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และ ซอฟต์แวร์ (Software) และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินแต่ละประเภทต้องมีข้อมูลอย่างน้อย ดังนี้

- ๑) ชื่อ/คำอธิบายของทรัพย์สิน
- ๒) ประเภทของอุปกรณ์/ยี่ห้อ
- ๓) ฟังก์ชันที่สำคัญของทรัพย์สิน
- ๔) ชื่อระบบปฏิบัติการ (Operation System) และเวอร์ชัน
- ๕) การระบุลำดับความสำคัญของทรัพย์สิน
- ๖) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สิน
- ๗) ตำแหน่งทางกายภาพของทรัพย์สิน
- ๘) การขึ้นต่อกันของทรัพย์สิน

๑.๑.๒ หน่วยงานต้องมีทะเบียนทรัพย์สินข้อมูล (Data Inventory) ที่ระบุข้อมูลที่เก็บไว้ภายในระบบสารสนเทศโดยจะต้องมีการกำหนดชั้นความลับของข้อมูล (Data Classification) เพื่อให้สามารถกำหนดสิทธิในการเข้าถึงข้อมูลได้อย่างปลอดภัย

๑.๑.๓ หน่วยงานต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๔ หน่วยงานต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๑.๕ หน่วยงานต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สินในข้อ ๑.๑ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๑.๑.๖ หน่วยงานต้องดำเนินการจัดทำแผนผังเครือข่าย (Network Diagram) ของหน่วยงานและปรับปรุงให้เป็นปัจจุบัน

#### ๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นการเตรียมความพร้อมในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน พร้อมทั้งหาแนวทางในการรับมือเพื่อลดความเสียหายที่จะเกิดกับหน่วยงาน

๑.๒.๑ หน่วยงานต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยต้องมีข้อมูลอย่างน้อย ดังนี้



- ๑) กำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยง
- ๒) ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk)
- ๓) ประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง
- ๔) กำหนดวิธีการหรือเครื่องมือในการบริหาร และจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

๑.๒.๒ หน่วยงานต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสาร โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

- ๑) วันที่ระบุความเสี่ยง (Date the Risk is Identified)
- ๒) คำอธิบายของความเสี่ยง (Description of the Risk)
- ๓) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- ๔) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- ๕) การจัดการความเสี่ยง (Risk Treatment)
- ๖) เจ้าของความเสี่ยง (Risk Owner)
- ๗) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)
- ๘) ความเสี่ยงที่เหลือ (Residual Risk)

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

เป็นการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ทางด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ครอบคลุมทั้งฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ว่ามีช่องโหว่ใดบ้างที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เพื่อให้หน่วยงานทราบถึงจุดอ่อนด้านความมั่นคงปลอดภัย และแก้ไขก่อนที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศของหน่วยงาน

๑.๓.๑ หน่วยงานต้องดำเนินการประเมินช่องโหว่ของอุปกรณ์ของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และการควบคุมโดยครอบคลุมบริการที่สำคัญของหน่วยงาน ซึ่งเป็น

- ๑) ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)
- ๒) ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

๑.๓.๒ หน่วยงานต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

- ๑) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
- ๒) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)
- ๓) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๑.๓.๓ หน่วยงานต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อหรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญของหน่วยงาน การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

- ๑.๓.๔ หน่วยงานควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของหน่วยงานโดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยงและพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย
- ๑.๓.๕ หน่วยงานต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของหน่วยงาน โดยเฉพาะอย่างยิ่งทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)
- ๑.๓.๖ หน่วยงานควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น
- ๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)
- การจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยประกอบด้วยการกำหนดบทบาทหน้าที่และความรับผิดชอบของผู้ให้บริการภายนอก
- ๑.๔.๑ หน่วยงานต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใดๆ ก็ตามในส่วนของบริการที่สำคัญของหน่วยงาน
- ๑.๔.๒ หน่วยงานต้องมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการ ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้
- ๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของหน่วยงานตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
  - ๒) ภาระหน้าที่ของผู้ให้บริการภายนอก ในการปกป้องบริการที่สำคัญของหน่วยงานจากภัยคุกคามทางไซเบอร์
  - ๓) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์
  - ๔) สิทธิของหน่วยงานในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก
- ๑.๔.๓ หน่วยงานควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์
- ๑.๔.๔ หน่วยงานควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่



## หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

### ๒.๑ การควบคุมการเข้าถึง (Access Control)

การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกในการเข้าถึงบริการที่สำคัญของหน่วยงาน

๒.๑.๑ หน่วยงานต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย อย่างน้อยดังนี้

- ๑) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)
- ๒) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
- ๓) การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย
- ๔) การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน
- ๕) การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

๒.๑.๒ หน่วยงานต้องกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจของหน่วยงาน ให้สอดคล้องกับหน้าที่ความรับผิดชอบของเจ้าหน้าที่

๒.๑.๓ หน่วยงานต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

๒.๑.๔ หน่วยงานต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเตอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงาน (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางสารสนเทศเท่านั้น

๒.๑.๕ หน่วยงานต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงาน

๒.๑.๖ ในการเข้าถึงระบบสารสนเทศของหน่วยงานต้องมีการเข้ารหัส Transaction ที่มีความปลอดภัย เช่น Secure Socket Layer (SSL) หรือ Transport Layer Security (TLS) เป็นต้น โดยต้องใช้ใบรับรอง (Certificate) ที่มีความปลอดภัย

### ๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ หน่วยงานต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงาน

๒.๒.๒ หน่วยงานต้องจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัย อย่างน้อยดังต่อไปนี้

- ๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
- ๒) การแบ่งแยกหน้าที่ (Separation of Duties)
- ๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
- ๔) การลบบัญชีที่ไม่ได้ใช้
- ๕) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)
- ๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์ (Malware)

๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบ อย่างทันการณ์ และเหมาะสม

๒.๒.๓ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใดๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน

๒.๒.๔ หน่วยงานต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงานอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๒.๕ หน่วยงานต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

## ๒.๓ การเชื่อมต่อระยะไกล (Remote Control)

๒.๓.๑ หน่วยงานต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของหน่วยงานมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงานต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

๑) เปิดใช้งานการเชื่อมต่อไคลเอนต์ระยะไกล เมื่อจำเป็นและได้รับการอนุญาตเท่านั้น

๒) ควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Internet Protocol Security (IPSEC)

๓) ต้องทำการเชื่อมต่อระยะไกลผ่านช่องทางระบบเครือข่ายเสมือน Virtual Private Network (VPN)

๔) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง เช่น การยืนยันตัวตนแบบสองปัจจัย (Two Factor Authentication) , กำหนดระยะเวลาในการเปลี่ยนรหัสผ่านตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน หรืออย่างสม่ำเสมอ

๕) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

๖) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการทำงานของบริการที่สำคัญของหน่วยงานเว้นแต่จะได้รับอนุญาต

๗) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

## ๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญของหน่วยงาน โดยใช้มาตรการอย่างน้อย ดังนี้

๑) ในกรณีที่ฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น



- ๒) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น
- ๓) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน
- ๒.๔.๒ หน่วยงานต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานบนสื่อบันทึกข้อมูลแบบถอดได้
- ๒.๔.๓ หน่วยงานต้องมีการกำหนดวิธีการที่ปลอดภัยในการทำลายสื่อบันทึกข้อมูลแบบถอดได้เพื่อป้องกันการรั่วไหลของข้อมูล
- ๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
  - ๒.๕.๑ หน่วยงานต้องเผยแพร่ ประชาสัมพันธ์ เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน ในลักษณะกระตุ้นความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย
  - ๒.๕.๒ หน่วยงานต้องจัดทำ ปรับปรุงคู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบัน และมีการเผยแพร่ผ่านช่องทางที่เหมาะสมของหน่วยงาน
  - ๒.๕.๓ หน่วยงานต้องจัดฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ
  - ๒.๕.๔ หน่วยงานต้องสร้างความตระหนัก (awareness program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย ให้แก่บุคลากรทุกระดับ
  - ๒.๕.๕ หน่วยงานควรจัดให้มีการฝึกอบรมและพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุมและเพียงพอต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกับเจ้าหน้าที่ดูแลระบบสารสนเทศ
- ๒.๖ การแบ่งปันข้อมูล (Information Sharing)

หน่วยงานต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ โดยต้องรายงานต่อคณะกรรมการด้านความมั่นคงปลอดภัยไซเบอร์กระทรวงยุติธรรม
- หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Treat Detection and Monitoring) การตรวจสอบการกระทำหรือการดำเนินการใดๆ โดยมีขอบ โดยใช้เครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมที่ไม่พึงประสงค์ ซึ่งมีจุดมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้ โดยหน่วยงานต้องมีกระบวนการในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

  - ๓.๑ มีกระบวนการในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความมั่นคงปลอดภัยทางไซเบอร์
  - ๓.๒ มีกระบวนการในการจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ
  - ๓.๓ มีกระบวนการในการระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน



๓.๔ ต้องดำเนินการตรวจสอบกลไกและกระบวนการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่างๆ ยังคงมีประสิทธิภาพ

#### หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ซึ่งมีแผนเกี่ยวข้องกับการตรวจพบภัยคุกคามทางไซเบอร์ จำนวน ๒ แผน ดังนี้

##### ๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

หน่วยงานต้องมีการจัดทำเอกสาร สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อย ปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

##### ๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๒.๑ หน่วยงานต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๒ หน่วยงานต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤต

๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๒) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง

๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๔) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

๕) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๔.๒.๓ หน่วยงานต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ หน่วยงานต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันทั่วถึงและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

#### หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้ อาจต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น

- ๕.๑ หน่วยงานต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงาน สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริงเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานเช่น ความสอดคล้องกันของขอบเขตค่านิยามและการกำหนดระยะเวลาที่สำคัญ Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น โดยมีรายละเอียดอย่างน้อยดังนี้
- ๕.๑.๑ จัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ โดยต้องพิจารณาจากปัจจัยที่สำคัญ เช่น ผลกระทบของการหยุดชะงัก ระยะเวลาที่ยอมรับได้ของการหยุดชะงักลำดับความสำคัญในการกู้คืนระบบ
  - ๕.๑.๒ จัดทำแผนกู้คืนภาวะวิกฤต สำหรับกระบวนการดำเนินงานของหน่วยงานที่ใช้ทรัพยากรสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด” เพื่อให้มั่นใจว่าสามารถดำเนินงานได้อย่างต่อเนื่องมีการควบคุมดูแลการแก้ไขและกู้คืนระบบเมื่อเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ
- ๕.๒ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม (Business Continuity Plan: BCP) อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อประเมินประสิทธิภาพของ (Business Continuity Plan: BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- ๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident) หน่วยงานต้องจัดทำรายงานภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าของการดำเนินการให้คณะกรรมการทราบทุกระยะ

ประกาศกระทรวงยุติธรรม  
เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม  
พ.ศ. ๒๕๖๖

เอกสารอ้างอิง

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ.๒๕๖๔
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
- (ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๙)
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๐)
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง กรอบการบริหารความเสี่ยงด้านไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๗)



| แก้ไขครั้งที่ | วันที่             | รายละเอียดการแก้ไข                                                                                                   |
|---------------|--------------------|----------------------------------------------------------------------------------------------------------------------|
| ๑             | ตุลาคม ๒๕๖๕        | ร่างเอกสารฉบับแรก                                                                                                    |
| ๒             | ๒๖ ตุลาคม ๒๕๖๕     | เพิ่มเติมเอกสารอ้างอิง / ปรับแก้ข้อความในประกาศฯ / ปรับแก้บัญชีแนบท้ายประกาศฯ                                        |
| ๓             | ๘ ธันวาคม ๒๕๖๕     | ปรับแก้ไขลำดับข้อ / ปรับแก้ข้อความในส่วนที่ ๑ / เพิ่มเติมสารบัญ                                                      |
| ๔             | ๒๒ ธันวาคม ๒๕๖๕    | ปรับแก้ข้อความในส่วนที่ ๑ / ปรับแก้ข้อความในส่วนที่ ๒ ในหัวข้อที่ ๒ หัวข้อย่อย ๒.๖                                   |
| ๕             | ๒๕ มกราคม ๒๕๖๖     | เพิ่ม, ปรับแก้, ลบข้อความในส่วนประกาศฯ                                                                               |
| ๖             | ๒๒ กุมภาพันธ์ ๒๕๖๖ | ปรับแก้ข้อความในบทนำ / เพิ่มคำนิยาม / ปรับแก้ข้อความในส่วนที่ ๑ / ปรับแก้ข้อความในส่วนที่ ๒                          |
| ๗             | ๗ มีนาคม ๒๕๖๖      | ปรับแก้ข้อความในบทนำ / เพิ่มคำนิยาม / ปรับแก้ข้อความในส่วนที่ ๑ / ปรับแก้ข้อความในส่วนที่ ๒                          |
| ๘             | ๑๐ มีนาคม ๒๕๖๖     | ปรับแก้ข้อความในส่วนที่ ๒ ในหัวข้อที่ ๑ หัวข้อย่อย ๑.๔, ในหัวข้อที่ ๒ หัวข้อย่อย ๒.๕ และในหัวข้อที่ ๕ หัวข้อย่อย ๕.๓ |