มหาวิทยาลัยมหิดล
คณะวิทยาศาสตร์
งานสารสนเทศและห้องสมุดสตางค์ มงคลสุข

พ.ร.บ. การรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. 2562

การรักษาความมั่นคงปลอดภัยไซเบอร์

คือ มาตรการเพื่อป้องกัน รับมือ และลดความเสี่ยง
จากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ
ที่กระทบต่อความมั่นคงของรัฐ เศรษฐกิจ การทหาร
และความสงบเรียบร้อยภายในประเทศ

ภัยคุกคามทางไซเบอร์

คือ การกระทำใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์
มุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์
ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
เป็นภัยอันตรายที่จะก่อให้เกิดความเสียหายต่อการทำงาน

ระดับของภัยคุกคามทางไซเบอร์

ระดับไม่ร้ายแรง ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานด้อยประสิทธิภาพลง

ระดับร้ายแรง ทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศเสียหาย
จนไม่สามารถทำงานหรือให้บริการได้

ระดับวิกฤติ ทำให้รัฐไม่สามารถควบคุมการทำงานจากส่วนกลาง
หรือทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน

หน่วยงานต้องทำอย่างไร

1. จัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์
2. ตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระ
   อย่างน้อยปีละหนึ่งครั้ง
3. กำหนดขั้นตอนการเฝ้าระวังภัยคุกคามทางไซเบอร์ และต้องร่วมซ้อมความพร้อมในการรับมือ
4. หากเกิดหรือคาดว่าจะเกิด ให้ดำเนินการตามแนวทางปฏิบัติ และแจ้งไปยังหน่วยงานควบคุม
5. แจ้งเตือนหน่วยงานที่อยู่ภายใต้การควบคุมและหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

หากเกิดภัยคุกคามในระดับวิกฤต

1. ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติ ในการดำเนินการตามกฎหมาย
   ว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง
2. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาจมอบหมายให้เลขาธิการสำนักงานฯ
   มีอำนาจดำเนินการได้โดยทันทีเท่าที่จำเป็น โดยไม่ต้องยื่นคำร้องต่อศาล

ที่มา : พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

lisc@mahidol.ac.th
https://stang.sc.mahidol.ac.th
StangMongkolsukLibrary
@StangLibrary