ประกาศสำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของสำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว เพื่อให้การดำเนินการด้านสารสนเทศของสำนักบริการคอมพิวเตอร์ (สบค.) มหาวิทยาลัยเกษตรศาสตร์ มีความมั่นคงปลอดภัยเพื่อรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความสมบูรณ์พร้อมใช้ (Availability) ของข้อมูลและระบบสารสนเทศ และเชื่อถือได้ สอดคล้องกับกฎหมายที่เกี่ยวข้อง มาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๒๒

อาศัยอำนาจตามความในมาตรา ๑๙ และ ๒๒ แห่งพระราชบัญญัติมหาวิทยาลัยเกษตรศาสตร์ พ.ศ. ๒๕๔๑ อธิการบดีมหาวิทยาลัยเกษตรศาสตร์จึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไว้ดังนี้

๑. ให้ยกเลิก ประกาศสำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับลงวันที่ ๒๔ กันยายน ๒๕๖๘

๒. ในประกาศนี้

"สบค." หมายถึง สำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์

"ผู้บริหาร" หมายถึง ผู้บริหารสำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์

"ผู้ดูแลระบบ" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ ระบบฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์

"ผู้ใช้" หมายถึง บุคคลหรือหน่วยงานใด ๆ ที่ได้รับสิทธิในการเข้าถึง ใช้งาน หรือดำเนินการใด ๆ บนระบบเทคโนโลยีสารสนเทศของ สบค. ไม่ว่าจะเป็นการเข้าถึงโดยตรงหรือผ่านระบบเครือข่าย ซึ่งรวมถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานราชการ ลูกจ้างชั่วคราว บุคลากรภายนอกที่ได้รับมอบหมาย นักศึกษาที่ได้รับอนุญาตให้ใช้งานระบบ รวมถึงผู้ให้บริการภายนอกที่ได้รับสิทธิชั่วคราว

"หน่วยงานภายนอก" หมายถึง หน่วยงานซึ่ง สบค. อนุญาตให้มีสิทธิ ในการเข้าถึงหรือใช้ข้อมูลหรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของ สบค. โดยจะได้รับสิทธิตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผยความลับของ สบค. โดยมิได้รับอนุญาต

"ความมั่นคงปลอดภัยสารสนเทศ" (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ

"ความลับ" (Confidentiality) หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

"ความถูกต้องครบถ้วน" (Integrity) หมายถึง การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่มีสิทธิไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

"สภาพพร้อมใช้งาน" (Availability) หมายถึง การรับรองได้ว่าข้อมูลหรือระบบสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

๓. วัตถุประสงค์

๓.๑ คงไว้ซึ่งการให้บริการเครือข่ายคอมพิวเตอร์มหาวิทยาลัยได้อย่างมีประสิทธิภาพและเสถียรภาพ

๓.๒ ปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้

๓.๓ ปกป้องและรักษาซึ่งเอกภาพของข้อมูลและทรัพยากรสารสนเทศของมหาวิทยาลัยเกษตรศาสตร์

๓.๔ ให้ผู้มีส่วนเกี่ยวข้องเข้าใจถึงหลักปฏิบัติการใช้เครือข่ายตามหลักจริยธรรมและหลักกฎหมาย

๔. สบค. ต้องจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้มีสาระสำคัญเพื่อใช้ในการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ ดังนี้

หมวดที่ ๑
การกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
(Information and Cybersecurity Governance)

---

๑. การกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Information and Cybersecurity Governance)

๑.๑. นโยบายความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และมาตรการที่เกี่ยวข้อง ต้องมีการกำหนดและอนุมัติโดยผู้บริหาร มีการเผยแพร่ รวมทั้งสร้างการรับรู้ให้แก่บุคลากรและบุคคลภายนอกที่เกี่ยวข้อง ตลอดจนทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยให้ครอบคลุมการรักษาความลับ (Confidentiality), ความถูกต้อง (Integrity), และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๒๒ และเป็นไปตามกฎหมายและกฎระเบียบของที่เกี่ยวข้อง

๑.๒. โครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศ ต้องจัดให้มีการถ่วงดุลตามหลักการควบคุม กำกับและตรวจสอบ (Three Lines of Defense) พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมอบหมายบทบาท หน้าที่และความรับผิดชอบให้แก่ผู้บริหาร ผู้ดูแลระบบ และผู้ใช้

๑.๓. สบค. ต้องดำเนินการพิจารณา กฎหมาย กฎระเบียบ สัญญาและข้อบังคับที่เกี่ยวข้องในการปฏิบัติงานด้านความมั่นคงปลอดภัย ความเป็นส่วนตัวสิทธิในสินทรัพย์ทางปัญญา ต้องได้รับการทบทวน และกำหนดให้มีการควบคุมดูแลให้ปฏิบัติตามที่กำหนดไว้

๑.๔. สบค. ต้องดำเนินการ จัดทำแผนการตรวจสอบและประเมินความสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ และกฎหมายที่เกี่ยวข้อง

๑.๕. สบค. ต้องดำเนินการ จัดทำรายงานผลการตรวจสอบ พร้อมทั้งวิเคราะห์ปัญหาและนำข้อเสนอแนะไปปรับปรุงระบบการบริหารจัดการความมั่นคงปลอดภัยให้มีประสิทธิภาพยิ่งขึ้น

๑.๖. ภาระความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

๑) ผู้บริหารของทุกส่วนงานต้องกำกับดูแลให้ผู้ใช้ได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ และปฏิบัติตามนโยบายและแนวปฏิบัติของ สบค.

๒) ผู้ใช้ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของ สบค. และต้องรายงานต่อ สบค. หากพบปัญหาหรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ

๓) ผู้ดูแลระบบที่เกี่ยวกับสารสนเทศของ สบค. ต้องตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ โดยมาตรการด้านความมั่นคงปลอดภัยของระบบต้องผ่านการพิจารณาและได้รับคำแนะนำจากผู้บริหารและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศของ สบค. ต้องมีความรับผิดชอบในเรื่องความมั่นคงปลอดภัยของสารสนเทศ

๔) หน่วยงานภายนอกที่ สบค. อนุญาตให้มีสิทธิในการเข้าถึงข้อมูลสารสนเทศ หรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของมหาวิทยาลัยต้องรับผิดชอบและปฏิบัติตามนโยบายและแนวปฏิบัติของ สบค. อย่างเคร่งครัด โดยการใช้งานตามสิทธิที่ได้รับอนุญาต และต้องรับผิดชอบในการกระทำที่เกิดขึ้นและไม่เปิดเผยความลับของ สบค. โดยมิได้รับอนุญาต

หมวดที่ ๒
การระบุสินทรัพย์สารสนเทศและการบริหารจัดการความเสี่ยง
(Information Asset Identification and Risk Management)

---

๑. การระบุสินทรัพย์สารสนเทศและการบริหารจัดการความเสี่ยง (Information Asset Identification Risk Management)

๑.๑. ทะเบียนสินทรัพย์สารสนเทศและการจัดชั้นความลับสารสนเทศ (Information Asset Inventory and Information Classification)

๑) ทะเบียนสินทรัพย์สารสนเทศทั้งเทคโนโลยีสารสนเทศ (Information Technology: IT) โดยเฉพาะระบบที่สำคัญ (Critical System) พร้อมทั้งผู้รับผิดชอบ ต้องได้รับการจัดทำและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

๒) การใช้งานสินทรัพย์สารสนเทศ (Acceptable Use Policy: AUP) ต้องมีการกำหนดเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสินทรัพย์เหล่านั้น

๓) แนวทางการจัดระดับชั้นความลับของสารสนเทศ การบ่งชี้สารสนเทศ และการดูแลสารสนเทศตามระดับชั้นความลับ ต้องมีการกำหนดให้สอดคล้องตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศของ สบค.

๑.๒. การประเมินความเสี่ยงและกลยุทธ์ในการบริหารจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๑) สบค. ต้องดำเนินการจัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง พร้อมทั้งกำหนดมาตรการควบคุมและต้องควบคุมและบริหารจัดการความเสี่ยงที่เกิดขึ้น โดยการประเมินความเสี่ยงจะต้องครอบคลุมทรัพย์สินของ สบค. และหน่วยงานภายนอกที่ให้บริการหรือสนับสนุนการดำเนินงานระบบเทคโนโลยีสารสนเทศของ สบค.

๒) สบค. ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยง ต้องควบคุมและติดตามการบริหารจัดการความเสี่ยงให้เป็นไปตามแผนการจัดการความเสี่ยงที่กำหนดไว้ และให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้ของ สบค.

๑.๓. การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

๑) สบค. ต้องดำเนินการกำหนดเกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศในการคัดเลือกผู้ให้บริการภายนอก รวมถึงกระบวนการและขั้นตอนปฏิบัติในการบริหารจัดการผู้ให้บริการภายนอกซึ่งจัดหาผลิตภัณฑ์หรือให้บริการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศแก่ สบค. ต้องมีการกำหนดและนำไปปฏิบัติ ให้ครอบคลุมตลอดทั้งห่วงโซ่ของผลิตภัณฑ์และบริการ และการถ่ายโอนข้อมูลสารสนเทศ

๒) สบค. ต้องดำเนินการกำหนดข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information Security) รวมถึงข้อตกลงของระดับการให้บริการ (Service Level Agreement: SLA) ต้องได้รับการระบุในสัญญากับผู้ให้บริการภายนอก

๑.๔. การกำกับดูแลการใช้งานระบบคลาวด์ (Cloud Computing Governance)

๑) การนำเทคโนโลยีคลาวด์มาใช้งานต้องมีการควบคุม กำกับดูแล และการประเมินความเสี่ยงในการนำระบบคลาวด์มาใช้ในการให้บริการและการดำเนินการภายใน สบค. โดยควบคุมผลกระทบจากการใช้คลาวด์ในการใช้บริการและให้บริการและผลกระทบต่อผู้มีส่วนได้เสียทั้งหมด โดยต้องควบคุมความเสี่ยงต่างๆ ให้อยู่ในระดับที่ยอมรับได้ และมีความชัดเจนตรวจสอบได้

๒) สบค. ต้องดำเนินการจัดการและควบคุมความมั่นคงปลอดภัยของบริการคลาวด์ การจัดเก็บข้อมูลบนระบบคลาวด์ต้องดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัย เช่น การเข้ารหัสข้อมูล การจำกัดสิทธิ์การเข้าถึง และการตรวจสอบผู้ให้บริการคลาวด์อย่างสม่ำเสมอ

หมวดที่ ๓

การป้องกันสารสนเทศ

(Information Protection)

---

๑. การป้องกันสารสนเทศ (Information Protection)

๑.๑. การควบคุมการเข้าถึง (Access Control)

๑) สบค. ต้องดำเนินการกำหนดสิทธิการเข้าถึงข้อมูลและสินทรัพย์ที่เกี่ยวข้อง ต้องจัดให้มีการควบคุมและจำกัดสิทธิ เพื่อเข้าถึงและใช้งานสินทรัพย์แต่ละประเภท โดยใช้หลักการให้สิทธิเท่าที่จำเป็น (Need-to-Know Basis) และหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (Principle of Least Privilege) และต้องทบทวน ปรับปรุง ตามระยะเวลาที่กำหนด และถอดถอน เมื่อไม่มีความจำเป็นในการใช้งาน

๒) สบค. ต้องกำหนดมาตรการควบคุมการเข้าถึงก่อนอนุญาตให้เข้าถึงข้อมูลและสินทรัพย์ที่เกี่ยวข้อง ต้องมีการพิสูจน์ตัวตนโดยใช้มาตรการที่มั่นคงปลอดภัยและต้องมีการสื่อสารแนวปฏิบัติการใช้รหัสผ่านที่ดีไปยังผู้ใช้ที่เกี่ยวข้อง เช่น การใช้ระบบยืนยันตัวตนหลายขั้นตอน (MFA) การใช้รหัสผ่านที่มีความมั่นคงปลอดภัย และการจำกัดสิทธิ์การเข้าถึงตามบทบาท (RBAC) เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓) สบค. ต้องดำเนินการใช้มาตรการเข้ารหัสข้อมูลสำคัญ ในระหว่างการจัดเก็บและการส่งผ่านโดยใช้มาตรฐานการเข้ารหัสที่เหมาะสม เพื่อป้องกันการถูกดักจับหรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑.๒. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

๑.๒.๑. การสร้างความมั่นคงปลอดภัยก่อนการว่าจ้าง (Prior to Employment)

๑) ก่อนการว่าจ้าง บุคลากร สบค. ต้องดำเนินการตรวจสอบภูมิหลังอย่างละเอียดและความเหมาะสมของบุคลากรก่อนเข้าปฏิบัติงาน เช่น การตรวจสอบประวัติการทำงาน (Background Check), ประวัติอาชญากรรม, สุขภาพ เป็นต้น โดยพิจารณาควบคู่กับกฎหมาย ระเบียบข้อบังคับ จริยธรรม และความเสี่ยงที่เกี่ยวข้อง เมื่อประสงค์จะว่าจ้าง

๒) สบค. ต้องดำเนินการระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศลงในข้อตกลงการจ้างงาน และต้องควบคุมให้ลงนามในข้อตกลงการรักษาความลับการปฏิบัติงานที่เกี่ยวข้องกับข้อมูลและความลับของ สบค.

๑.๒.๒. การสร้างความมั่นคงปลอดภัยในระหว่างการว่าจ้าง (During Employment)

๑) สบค. ต้องกำหนดแผนการฝึกอบรมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับบุคลากรภายในและบุคคลภายนอกที่เกี่ยวข้อง ต้องได้รับการสร้างความตระหนักการให้ความรู้ การฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอเป็นประจำอย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยทาง

ไซเบอร์

๒) สบค. ต้องกำหนดกระบวนการทางวินัยเพื่อลงโทษผู้ใช้งานที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของ สบค. ต้องมีการกำหนดและสื่อสารไปยังบุคลากรและบุคคลภายนอกที่เกี่ยวข้อง

๓) สบค. ต้องกำหนดมาตรการการปฏิบัติงานจากระยะไกลให้กับบุคลากรและบุคคลภายนอกที่เกี่ยวข้องที่จำเป็นต้องปฏิบัติงานและต้องได้รับการอนุญาตจากผู้บังคับบัญชาและต้องปฏิบัติตามระเบียบหรือข้อบังคับในการปฏิบัติงานจากระยะไกลอย่างเคร่งครัด

๔) เมื่อพบจุดอ่อน หรือช่องโหว่ หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ บุคลากรและบุคคลภายนอกที่เกี่ยวข้องต้องรายงานสิ่งที่เกิดขึ้นให้แก่หน่วยงานที่รับผิดชอบทราบโดยทันที โดยผ่านช่องทางที่ สบค. กำหนดไว้

๑.๒.๓. การสร้างความมั่นคงปลอดภัยเมื่อสิ้นสุดหรือเปลี่ยนแปลงการว่าจ้าง (Termination or Change of Employment)

๑) สบค. ต้องกำหนดมาตรการสำหรับบุคลากรที่พ้นสภาพการทำงานเมื่อลาออกหรือพ้นสภาพการทำงาน

๒) สบค. ต้องดำเนินการเพิกถอนสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูลสำคัญทันที เช่น การระงับบัญชีผู้ใช้งาน และยืนยันการคืนอุปกรณ์ที่ได้รับไป เป็นต้น

๓) สบค. ต้องกำหนดกระบวนการและช่องทางให้กับบุคลากรและบุคคลภายนอกที่เกี่ยวข้องต้องคืนสินทรัพย์ของ สบค. ทั้งหมดที่ตนเองถือครองเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงานสิทธิในการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องถูกถอดถอนเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงานทันทีหรือภายในระยะเวลาที่กำหนดไว้

๑.๒.๔. การแบ่งปันข้อมูล (Information Sharing)

๑) สบค. ต้องจัดทำข้อมูลสำหรับการติดต่อกับหน่วยงานผู้ควบคุม/กำกับดูแล และกลุ่มพิเศษที่มีความสนใจในเรื่องเดียวกัน ต้องมีการจัดทำและปรับปรุงให้เป็นปัจจุบัน เพื่อใช้ในการติดต่อประสานงานในเรื่องที่สำคัญและจำเป็น

๒) สบค. ต้องดำเนินการรวบรวม ติดตามข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์จากแหล่งที่น่าเชื่อถือ เจ้าของผลิตภัณฑ์หรือผู้ให้บริการภายนอก สำหรับจัดทำข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย เพื่อกำหนดแนวทางแผนการในการป้องกันและรับมือภัยคุกคามทางไซเบอร์

๑.๒.๕. ความมั่นคงปลอดภัยกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

๑) พื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

- สบค. ต้องดำเนินการกำหนดพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย หรือพื้นที่

สำนักงาน ห้องทำงาน และห้องจัดเก็บอุปกรณ์ต่างๆ ต้องมีการกำหนดขอบเขตหรือบริเวณที่ชัดเจน โดยบริเวณดังกล่าว ต้องมีการป้องกันทางกายภาพและด้านสภาพแวดล้อม ต้องมีการควบคุมการเข้า-ออก รวมถึงมีการเฝ้าระวังและติดตามการเข้าถึงพื้นที่

- สบค. ต้องจัดทำมาตรการรักษาความมั่นคงปลอดภัยสำหรับพื้นที่ปฏิบัติงานและมาตรการรักษาความมั่นคงปลอดภัยต้องครอบคลุมพื้นที่สำคัญ เช่น ศูนย์คอมพิวเตอร์ ห้องเซิร์ฟเวอร์ ห้องควบคุมระบบ และพื้นที่จัดเก็บข้อมูลสำคัญ และกำหนดให้การควบคุมการเข้าถึงต้องถูกจำกัดเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เช่น การใช้บัตรผ่าน, ลายนิ้วมือ หรือระบบสแกนใบหน้า พร้อมบันทึกการเข้า-ออก เพื่อตรวจสอบย้อนหลัง
- สบค. ต้องดำเนินการติดตั้งระบบเฝ้าระวัง เช่น กล้องวงจรปิด (CCTV) ระบบเตือนภัยอัตโนมัติ หรือสัญญาณเตือนภัยต่างๆ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต หรือมาตรการอื่นๆ ที่มีความเหมาะสมสำหรับป้องกันข้อมูลและระบบสารสนเทศโดยครอบคลุมพื้นที่สำคัญทั้งหมดของหน่วยงาน และระบบที่ดำเนินการติดตั้งต้องบันทึกข้อมูลอย่างน้อย ๙๐ วัน
- เอกสารหรือสื่อบันทึกข้อมูลแบบพกพา (Removable Storage Media) หรือสื่อบันทึกข้อมูลภายนอก (External Storage Media) ต้องได้รับการจัดเก็บในสถานที่ที่ปลอดภัยและได้รับการควบคุมดูแล

๒) ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

- อุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการจัดวางและป้องกันโดยคำนึงถึงความมั่นคงปลอดภัย ผู้ใช้งานต้องออกจากระบบหรือทำการล็อคหน้าจอ เมื่อออกห่างจากเครื่องคอมพิวเตอร์ หรือปิดเครื่องหากไม่มีความจำเป็นต้องใช้งาน ซึ่งครอบคลุมถึงอุปกรณ์ที่มีการใช้งานนอก สบค. ระบบสาธารณูปโภคที่สนับสนุนการทำงานของอุปกรณ์ดังกล่าว สายสัญญาณไฟฟ้าและข้อมูล โดยต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้บริการด้านเทคโนโลยีสารสนเทศใช้งานได้อย่างต่อเนื่อง
- ก่อนที่จะจำหน่ายอุปกรณ์ที่มีสื่อบันทึกข้อมูลสารสนเทศ หรือนำอุปกรณ์นั้นกลับมาใช้ใหม่ ต้องได้รับการตรวจสอบว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ถูกลบทิ้ง ย้าย หรือทำลายตามระดับชั้นความลับด้วยวิธีการที่ทำให้มั่นใจได้ว่าจะไม่สามารถกู้คืนข้อมูลเหล่านั้นกลับมาใช้ได้อีก
- สบค. ต้องกำหนดมาตรการทำลายอุปกรณ์และสื่อจัดเก็บข้อมูลที่ไม่ได้ใช้งาน โดยจัดทำกระบวนการทำลายข้อมูลที่ปลอดภัย เช่น การลบข้อมูลแบบถาวร (Data Wiping) การบดทำลายอุปกรณ์ หรือการเผาทำลาย ตามหลักมาตรฐานด้านความ

มั่นคงปลอดภัย เพื่อป้องกันไม่ให้ข้อมูลรั่วไหลออกไป

๑.๒.๖. การรักษาความมั่นคงปลอดภัยสารสนเทศและข้อมูลส่วนบุคคล (Information and Personal Data Protection))

๑) การรักษาความมั่นคงปลอดภัยของสารสนเทศ (Information Protection)

- สารสนเทศของ สบค. ต้องได้รับการควบคุมดูแลโดยสอดคล้องและเป็นไปตามระดับชั้นความลับของสารสนเทศที่ สบค. กำหนด รวมถึงต้องมีการกำหนดมาตรการการสำรองสารสนเทศและการทดสอบการกู้คืน มาตรการในการป้องกันการรั่วไหลของสารสนเทศ และมาตรการในการลบหรือทำลายสารสนเทศเมื่อไม่มีความจำเป็นในการเก็บรักษาหรือใช้งาน

๒) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Security in Personal Data Protection)

- มาตรการที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ได้แก่ มาตรการสำรองและทดสอบการกู้คืน มาตรการการป้องกันการรั่วไหลของข้อมูลส่วนบุคคล และมาตรการการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ต้องได้รับการกำหนดและนำไปปฏิบัติ โดยครอบคลุมถึงการป้องกันส่วนประกอบต่างๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล โดยคำนึงถึงหลักการป้องกันเชิงลึก (Defense in Depth) และการคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบและโดยค่าเริ่มต้น (Data Protection by Design and by Default)
- บันทึกกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ต้องมีการจัดเก็บและป้องกัน เพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคลได้

๓) ความมั่นคงปลอดภัยในการปฏิบัติงาน (Operation Security)

- ขั้นตอนในการปฏิบัติงานด้านสารสนเทศ ต้องมีการกำหนด ทบทวน และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- มาตรการด้านความมั่นคงปลอดภัยในการปฏิบัติงาน ต้องมีการกำหนดให้ครอบคลุมด้านการบริหารการเปลี่ยนแปลง การบริหารจัดการความต้องการทรัพยากรสารสนเทศ การป้องกันโปรแกรมไม่พึงประสงค์ การสำรองข้อมูลและทดสอบข้อมูลที่สำคัญ การเฝ้าระวังความผิดปกติ การจัดเก็บบันทึกเหตุการณ์ (Logging) การตั้งค่านาฬิกาของระบบสารสนเทศให้ตรงกัน การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ การเข้ารหัสลับข้อมูล และการป้องกันอุปกรณ์ปลายทางของผู้ใช้งาน
- สบค. ต้องกำหนดแนวทางควบคุมการเข้าถึงและการป้องกันการดัดแปลง Log Files การบันทึกกิจกรรมการใช้งานระบบต้องมีการจัดเก็บและป้องกันการเข้าถึงโดยไม่ได้

รับอนุญาต สบค. ต้องกำหนดสิทธิ์ในการดูแลรักษาและตรวจสอบ Log Files อย่างเหมาะสม เพื่อให้มั่นใจได้ว่ามีความน่าเชื่อถือ และสามารถใช้เป็นหลักฐานเมื่อมีเหตุการณ์ผิดปกติ

๔) ความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

- เครือข่ายและอุปกรณ์เครือข่าย ต้องได้รับการควบคุมและป้องกันด้านความมั่นคงปลอดภัย มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย และระดับของการให้บริการลงในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายของ สบค. รวมถึงต้องมีการเฝ้าระวัง และต้องมีการแบ่งแยกเครือข่ายย่อยเพื่อจำกัดการเข้าถึง โดยพิจารณาจากระดับความสำคัญของข้อมูลที่อยู่บนเครือข่าย และผลกระทบทางด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น

๑.๒.๗. การจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)

๑) ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

- สบค. ต้องมีการพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems) ในการจัดหาหรือพัฒนาระบบสารสนเทศ ทั้งที่เป็นระบบใหม่หรือระบบที่มีอยู่เดิม
- สบค. ต้องกำหนดมาตรการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยในทุกขั้นตอนของการพัฒนาซอฟต์แวร์ต้องดำเนินการตาม Secure Development Lifecycle (SDLC) เช่น การตรวจสอบโค้ด (Code Review) การทดสอบช่องโหว่ และการแก้ไขจุดอ่อนของระบบก่อนใช้งานจริง

๒) การพัฒนาและทดสอบระบบสารสนเทศ (Information Systems Development and Testing)

- การพัฒนาระบบสารสนเทศ ต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ต้องมีกระบวนการทดสอบด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงต้องแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน หากเป็นระบบที่พัฒนาโดยบุคคลภายนอก ต้องมีการกำกับดูแล เฝ้าระวัง ติดตาม และทบทวนกิจกรรม เพื่อตรวจสอบให้แน่ใจว่ามีการปฏิบัติตามที่ได้ระบุในสัญญาจ้าง
- สบค. ต้องดำเนินการติดตั้งระบบป้องกันมัลแวร์และดำเนินการตั้งค่าให้ระบบดำเนินการตรวจสอบเป็นประจำ รวมถึงระบบป้องกันช่องโหว่ (Patch Management) และต้องอัปเดตอย่างสม่ำเสมอ เพื่อป้องกันการโจมตีจากมัลแวร์และภัยคุกคามอื่นๆ

หมวดที่ ๔
การเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์
(Cyber Threat Monitoring and Detection)

---

๑. การเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Monitoring and Detection)

ระบบเทคโนโลยีสารสนเทศและระบบเทคโนโลยีปฏิบัติการที่สำคัญ ต้องได้รับการเฝ้าระวังเพื่อตรวจหาช่องโหว่ทางเทคนิค (Technical Vulnerabilities) และพฤติกรรมที่ผิดปกติ รวมถึงต้องมีการประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Event) ที่อาจเป็นเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident) และมีการตอบสนองตามที่กำหนดไว้

หมวดที่ ๕
การตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ
(Information Security Incident Response)

---

๑. การตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Response)

๑.๑. ขั้นตอนในการบริหารจัดการ บทบาท และหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Event) และเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident) ต้องได้รับการกำหนดและสื่อสารไปยังบุคลากรที่เกี่ยวข้อง ต้องมีการทดสอบตามขั้นตอนเพื่อให้ใช้ได้จริงในทางปฏิบัติ และบทเรียนที่ได้รับจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นต้องถูกนำมาวิเคราะห์และทบทวนการดำเนินการ เพื่อปรับปรุงมาตรการความมั่นคงปลอดภัยสารสนเทศให้มีประสิทธิภาพ

๑.๒. เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องและจำเป็นต้องดำเนินการทางกฎหมาย หลักฐานของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศดังกล่าวต้องถูกรวบรวมและจัดเก็บให้เป็นไปตามที่กฎหมายกำหนด

๑.๓. สบค. ต้องจัดทำแผนการจัดการเหตุการณ์ที่ครอบคลุมขั้นตอนการตรวจจับ การแจ้งเตือน การประเมินผลกระทบ และการกู้คืนระบบ โดยแผนดังกล่าวต้องระบุบทบาทของทีมงานที่เกี่ยวข้องอย่างชัดเจน และต้องจัดทำระบบแจ้งเตือนที่สามารถส่งข้อมูลไปยังทีมรับมือเหตุการณ์ได้อย่างรวดเร็ว

๑.๔. สบค. ต้องมีช่องทางในการรายงานเหตุการณ์ เช่น ระบบ Helpdesk หรือ Email ที่สามารถแจ้งเหตุการณ์ได้ตลอด ๒๔ ชั่วโมง ทีมที่เกี่ยวข้องต้องวิเคราะห์เหตุการณ์และจัดทำรายงานสรุปผลเพื่อนำมาปรับปรุงมาตรการป้องกันและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำอีก

หมวดที่ ๖
การกู้คืนและความต่อเนื่องทางธุรกิจ
(Recovery for Business Continuity)

---

๑. การกู้คืนและความต่อเนื่องทางธุรกิจ (Recovery for Business Continuity)

๑.๑. สบค. ต้องดำเนินการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) บทบาท และหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการบริหารจัดการความต่อเนื่องทางธุรกิจ ต้องได้รับการกำหนดโดยคำนึงถึงความมั่นคงปลอดภัย และสื่อสารไปยังบุคลากรที่เกี่ยวข้อง พร้อมทั้งปรับปรุงและทบทวนแผนให้มีความสอดคล้องกับการดำเนินงานเป็นประจำอย่างน้อยปีละ ๑ ครั้ง

๑.๒. ต้องมีการทดสอบตามแผนเพื่อให้ใช้ได้จริงในทางปฏิบัติอย่างน้อยปีละ ๑ ครั้ง รวมถึงดำเนินการทบทวนและปรับปรุงแผนให้เป็นปัจจุบัน

หมวดที่ ๗
ขอบเขตมีผลบังคับใช้
(Boundary)

นโยบายนี้มีผลบังคับใช้กับทุกตำแหน่งพื้นที่ที่สามารถเข้าถึง ระบบสารสนเทศและเครือข่ายของ สบค. ซึ่งรวมถึงการเข้าถึงจากระยะไกลหรือการเชื่อมโยงจากหน่วยงานภายนอก การอนุญาตและมอบหมายสิทธิในการเข้าถึงระบบของ สบค. ไม่ว่าจะเป็นระบบสารสนเทศด้านวิชาการ และระบบสารสนเทศด้านการบริหาร สบค.ต้องมั่นใจว่าได้มีการดำเนินการตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และได้มีการสร้างความเข้าใจในเรื่องภาวะความเสี่ยงที่อาจจะเกิดขึ้นและการควบคุมความเสี่ยงที่เหมาะสม

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๖ สิงหาคม พ.ศ. ๒๕๖๘ เป็นต้นไป

(ผศ.ดร.อภิรักษ์ จันทร์สร้าง)
ผู้อำนวยการสำนักบริการคอมพิวเตอร์