ประกาศกรมวิทยาศาสตร์บริการ

เรื่อง นโยบายด้านความปลอดภัยทางไซเบอร์ของกรมวิทยาศาสตร์บริการ

.....

เพื่อให้การบริหารจัดการระบบเทคโนโลยีสารสนเทศและการบูรณาการข้อมูลภาครัฐของกรมวิทยาศาสตร์บริการเป็นไปด้วยความมั่นคงปลอดภัย มีธรรมาภิบาล สามารถป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความน่าเชื่อถือของข้อมูลและการให้บริการสาธารณะ ตลอดจนมีมาตรการป้องกันมิให้ข้อมูลและระบบโครงสร้างพื้นฐานถูกโจมตีหรือเข้าถึงโดยมิชอบ โดยที่พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้หน่วยงานของรัฐมีการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการบูรณาการข้อมูลภาครัฐอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล นั้น

ดังนั้น อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๘ และมาตรา ๑๒ แห่งพระราชบัญญัติระเบียบบริหารราชการกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม พ.ศ. ๒๕๖๒ ประกอบมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และมาตรา ๔ มาตรา ๑๒ ประกอบมาตรา ๘ แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ประกอบมาตรา ๔๔ และ มาตรา ๔๕ ประกอบมาตรา ๑๓ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จึงออกประกาศนโยบายด้านความปลอดภัยทางไซเบอร์ของกรมวิทยาศาสตร์บริการ เพื่อยึดถือเป็นแนวทางปฏิบัติภายในของกรมวิทยาศาสตร์บริการต่อไป รายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

จึงประกาศเพื่อทราบและถือปฏิบัติอย่างเคร่งครัดโดยทั่วกัน

ประกาศ ณ วันที่ ๒๐ พฤษภาคม พ.ศ. ๒๕๖๙

(นางพจมาน ท่าจีน)

รองอธิบดี รักษาราชการแทน

อธิบดีกรมวิทยาศาสตร์บริการ

**รายละเอียดแนบท้ายประกาศกรมวิทยาศาสตร์บริการ**
**เรื่อง นโยบายด้านความปลอดภัยทางไซเบอร์ของกรมวิทยาศาสตร์บริการ**
**ประกาศ ณ วันที่ ๒๐ พฤษภาคม พ.ศ. ๒๕๖๙**

**๑. วัตถุประสงค์**

๑) เพื่อให้กรมวิทยาศาสตร์บริการ (วศ.) มีนโยบายด้านความปลอดภัยทางไซเบอร์ที่เป็นกรอบและแนวทางมาตรฐานในการป้องกัน รับมือ และแก้ไขเหตุการณ์ภัยคุกคามทางไซเบอร์ สอดคล้องกับกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ มาตรฐาน NIST Cybersecurity Framework มาตรฐานสากล ISO/IEC 27001 รวมถึงรองรับการปฏิบัติงานของสำนักบริหารและรับรองห้องปฏิบัติการตามมาตรฐาน ISO/IEC 17011 และ ISO/IEC17024 และการดำเนินการของห้องปฏิบัติการตามมาตรฐาน ISO/IEC 17025

๒) เพื่อปกป้องระบบสารสนเทศ ระบบบริหารจัดการห้องปฏิบัติการ ข้อมูลผลการทดสอบ และข้อมูลที่เกี่ยวข้องให้มีความถูกต้อง ครบถ้วน เป็นความลับและพร้อมใช้งานอยู่เสมอ

๓) เพื่อสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามด้านความปลอดภัยทางไซเบอร์และเป็นแนวทางในการปฏิบัติงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ให้แก่ผู้บริหาร เจ้าหน้าที่ ผู้ปฏิบัติงาน และผู้ที่เกี่ยวข้องกับการรับบริการของกรมวิทยาศาสตร์บริการ

**๒. ขอบเขตและการบังคับใช้**

นโยบายด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Policy) ฉบับนี้ จัดทำโดยคณะกรรมการบริหารการเปลี่ยนแปลงสู่องค์กรดิจิทัลของกรมวิทยาศาสตร์บริการ มีขอบเขตการบังคับใช้ครอบคลุมทุกหน่วยงานภายใต้กรมวิทยาศาสตร์บริการ รวมถึงบุคลากรทุกประเภท ผู้ให้บริการภายนอก และผู้มีส่วนเกี่ยวข้องในการดำเนินงานด้านระบบสารสนเทศและเครือข่ายของกรมวิทยาศาสตร์บริการ นโยบายนี้มุ่งเน้นการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ภารกิจหลัก ทั้งด้านการวิจัย การบริหารจัดการมาตรฐาน และการให้บริการทางวิทยาศาสตร์ สามารถดำเนินงานได้อย่างต่อเนื่องแม้ในภาวะฉุกเฉิน ผู้ที่ฝ่าฝืนนโยบายนี้ถือว่าเป็นการกระทำความผิด และจะต้องได้รับการดำเนินการตามระเบียบหรือข้อบังคับของ วศ. รวมถึงกฎหมายที่เกี่ยวข้อง

**๓. ข้อยกเว้น**

นโยบายนี้อาจมีการขยายผลหรือมีการยกเว้น โดยปฏิบัติตามขั้นตอนการยกเว้นนโยบายของรัฐด้านอื่น ๆ หรือนโยบายของกรมวิทยาศาสตร์บริการร่วมด้วย ตามที่คณะกรรมการบริหารการเปลี่ยนแปลงสู่องค์กรดิจิทัลพิจารณาเห็นชอบ โดยต้องมีการบันทึกการดำเนินการไว้เป็นลายลักษณ์อักษร

การขอขยายผลหรือขอยกเว้นไม่ปฏิบัติตามนโยบายนี้ ให้ปฏิบัติตามหลักเกณฑ์ของรัฐ หรือนโยบายของกรมวิทยาศาสตร์บริการ โดยต้องได้รับความเห็นชอบจากคณะกรรมการบริหารการเปลี่ยนแปลงสู่องค์กรดิจิทัล และจัดทำบันทึกหลักฐานการดำเนินการไว้เป็นลายลักษณ์อักษร

**๔. บทบาทและความรับผิดชอบ**

๑) อธิบดีกรมวิทยาศาสตร์บริการหรือผู้ที่ได้รับมอบหมาย ต้องควบคุมและกำกับดูแลให้บุคลากรทุกประเภท ผู้ให้บริการภายนอก และผู้มีส่วนเกี่ยวข้องในการดำเนินงานด้านระบบสารสนเทศและเครือข่ายของกรมวิทยาศาสตร์บริการ ดำเนินการตามนโยบายด้านความปลอดภัยทางไซเบอร์อย่างเคร่งครัด

๒) ผู้บังคับบัญชา/ผู้ที่ได้รับมอบหมาย ต้องตรวจสอบให้แน่ใจว่าบุคลากรทุกประเภท ผู้ให้บริการภายนอก และผู้มีส่วนเกี่ยวข้องในการดำเนินงานด้านระบบสารสนเทศและเครือข่ายของกรมวิทยาศาสตร์บริการที่ได้รับมอบหมายให้เข้าถึงระบบสารสนเทศหรือเครื่องมือวิเคราะห์ของกรมวิทยาศาสตร์บริการ ได้รับการอบรมและปฏิบัติตามมาตรการด้านความปลอดภัยอย่างเหมาะสม

๓) บุคลากรทุกประเภท ผู้ให้บริการภายนอก และผู้มีส่วนเกี่ยวข้องในการดำเนินงานด้านระบบสารสนเทศและเครือข่ายของกรมวิทยาศาสตร์บริการที่เชื่อมต่อหรือใช้งานระบบเครือข่าย ซอฟต์แวร์ และข้อมูลของกรมวิทยาศาสตร์บริการ ต้องปฏิบัติตามนโยบาย มาตรการ และแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่กรมวิทยาศาสตร์บริการกำหนด

๔) คณะกรรมการบริหารการเปลี่ยนแปลงสู่องค์กรดิจิทัลของกรมวิทยาศาสตร์บริการ และหน่วยงานที่ดูแลด้านเทคโนโลยีดิจิทัล มีหน้าที่กำหนด เฝ้าระวัง ประเมินความเสี่ยง และตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยทางไซเบอร์

**๕. นโยบายด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Policy)**

๑) การกำกับดูแลและการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้ข้อมูลและระบบสารสนเทศมีความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) อย่างเหมาะสม

๒) การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management) เพื่อให้มีการประเมินความเสี่ยงทางไซเบอร์ของระบบสารสนเทศและระบบโครงสร้างพื้นฐานของกรมวิทยาศาสตร์บริการ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อระบบสารสนเทศและระบบโครงสร้างพื้นฐานของกรมวิทยาศาสตร์บริการ โดยเฉพาะระบบที่มีการเชื่อมโยงกับฐานข้อมูลทางวิทยาศาสตร์และเครื่องมือในห้องปฏิบัติการ เพื่อกำหนดมาตรการควบคุมและป้องกันภัยคุกคามที่เหมาะสมกับระดับความเสี่ยง

๓) การบริหารจัดการทรัพย์สิน (Asset Management) เพื่อให้มีการจัดทำทะเบียนทรัพย์สินให้ครบถ้วน และเป็นปัจจุบัน รวมถึงดูแลทรัพย์สินให้มีความพร้อมใช้งานและสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง โดยครอบคลุมขอบเขตเครือข่ายและระบบที่มีความเชื่อมโยงอย่างมีนัยสำคัญ และตรวจสอบความถูกต้องของทะเบียนอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลง

๔) การควบคุมการเข้าถึง (Access Control) เพื่อให้มีการควบคุมการเข้าถึงระบบเครือข่าย ระบบบริหารจัดการข้อมูลห้องปฏิบัติการ และระบบกระบวนการทำงานอัตโนมัติ (Automated Workflows) โดยใช้หลักการให้สิทธิเท่าที่จำเป็น (Least Privilege) เพื่อป้องกันการเข้าถึงข้อมูลหรือการปรับเปลี่ยนมาตรฐานและผลการทดสอบโดยไม่ได้รับอนุญาต นอกจากนี้ ต้องจัดเก็บและตรวจสอบบันทึกเหตุการณ์การเข้าถึง (Logs of All Access) เพื่อเฝ้าระวังความผิดปกติเป็นประจำ และต้องตรวจสอบการเข้าถึงอินเทอร์เฟซทางกายภาพ

๕) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) เพื่อให้มีการดำเนินการประเมินช่องโหว่ของระบบ โดยครอบคลุมทั้งระดับโฮสต์ (Host Security Assessment) เครือข่าย (Network Security Assessment) และสถาปัตยกรรมความมั่นคงปลอดภัย (Architecture Security Review) ทั้งนี้ต้องดำเนินการประเมินก่อนเริ่มใช้งานระบบใหม่หรือเมื่อมีการเปลี่ยนแปลงระบบที่มีนัยสำคัญ

๖) การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management) เพื่อให้มีการกำหนดข้อกำหนดด้านความปลอดภัยไซเบอร์ในสัญญาจ้างหรือข้อตกลงระดับการให้บริการ (SLA) และควรจัดให้มีกระบวนการตรวจสอบการทำงานของผู้ให้บริการภายนอกให้สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้ทันสมัยและสอดคล้องกับกฎหมายหรือข้อบังคับใหม่ที่อาจเกิดขึ้น เพื่อลดความเสี่ยงจากการเข้าถึงและดำเนินงานของผู้ให้บริการภายนอกอย่างมีประสิทธิภาพ

๗) การทำให้ระบบมีความแข็งแกร่ง (System Hardening) เพื่อให้มีมาตรฐานการกำหนดค่าความปลอดภัยขั้นต่ำ (Security Baseline) สำหรับทุกระบบสารสนเทศ โดยต้องตรวจสอบความถูกต้องก่อนใช้งานหรือเมื่อมีการเปลี่ยนแปลง และทบทวนมาตรฐานอย่างน้อยปีละ ๑ ครั้ง พร้อมทั้งจัดทำกระบวนการจัดการการเปลี่ยนแปลง (Change Management) เพื่อควบคุมและป้องกันไม่ให้การแก้ไขระบบส่งผลกระทบต่อความมั่นคงปลอดภัยของบริการสำคัญในภาพรวม

๘) การปกป้องข้อมูลและระบบสารสนเทศทางวิทยาศาสตร์ (Scientific Data and System Protection) เพื่อให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลดิจิทัล ข้อมูลอ้างอิง และข้อมูลผลการทดสอบทางวิทยาศาสตร์ เพื่อรักษาสภาพความถูกต้อง ความลับ และความพร้อมใช้งาน รวมถึงการเข้ารหัสข้อมูลที่สำคัญและการสำรองข้อมูล (Data Backup) อย่างเป็นระบบ เพื่อป้องกันการสูญหายหรือถูกโจมตีจากผู้ไม่หวังดี

๙) การรักษาความมั่นคงปลอดภัยสำหรับการเชื่อมต่อระบบและ API (Security for Integration and APIs) เพื่อให้มีการบูรณาการข้อมูลและการเชื่อมต่อระหว่างแพลตฟอร์ม ฐานข้อมูล หรือระบบอัตโนมัติต่าง ๆ ภายในองค์กร ต้องใช้ช่องทางและโปรโตคอลที่มีความปลอดภัย มีการตรวจสอบช่องโหว่ เพื่อลดความเสี่ยงจากการถูกโจมตีผ่านช่องทางการเชื่อมต่อระบบ

๑๐) การเชื่อมต่อระยะไกล (Remote Connection) ต้องได้รับอนุญาตตามความจำเป็น โดยใช้การพิสูจน์ตัวตนที่เข้มงวดและเข้ารหัสข้อมูลด้วยโปรโตคอลมาตรฐานความปลอดภัยสูง รวมถึงจำกัดสิทธิ์การเข้าถึงเฉพาะฟังก์ชันที่จำเป็นต่อการปฏิบัติงาน (Least Privilege) เพื่อรักษาไว้ซึ่งความลับของข้อมูล และป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและเหมาะสม

๑๑) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) เพื่อให้มีระบบการเฝ้าระวังความมั่นคงปลอดภัยเครือข่ายอย่างต่อเนื่อง พร้อมจัดประเภทความรุนแรงของภัยคุกคาม และต้องมีการทบทวน และฝึกซ้อม แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) อย่างน้อยปีละ ๑ ครั้งเพื่อให้สามารถตรวจจับ วิเคราะห์ ระงับเหตุ และฟื้นฟูระบบการให้บริการทางวิทยาศาสตร์และการบริหารงานให้กลับมาสู่สภาวะปกติได้อย่างมีประสิทธิภาพ

๑๒) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) เพื่อให้มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อรับมือเหตุการณ์ภัยคุกคามไซเบอร์ โดยระบุทีมสื่อสาร โฆษกหลัก และช่องทางเผยแพร่ข้อมูล รวมถึงต้องดำเนินการฝึกซ้อมแผนสื่อสารอย่างน้อยปีละ ๑ ครั้ง เพื่อทดสอบความพร้อมและประสิทธิภาพในการสื่อสารข้อมูลได้อย่างทันท่วงทีในช่วงวิกฤต

๑๓) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) เพื่อให้มีการกำหนดให้บุคลากรที่เกี่ยวข้องตามแผนรับมือภัยคุกคามและแผนสื่อสารภาวะวิกฤต ต้องเข้าร่วมการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ทั้งในระดับภาคส่วนและระดับชาติ เพื่อสร้างความเข้าใจในการเผชิญเหตุและทดสอบกระบวนการปฏิบัติงานให้เป็นไปตามแผนที่กำหนด

๑๔) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) เพื่อให้มีการจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) เพื่อให้ธุรกิจสามารถดำเนินการต่อไปได้อย่างต่อเนื่อง และสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติ ภายในระยะเวลาที่ยอมรับ รวมถึงกำหนดให้มีการฝึกซ้อมแผน BCP อย่างน้อยปีละ ๑ ครั้ง

๑๕) การสร้างความตระหนักรู้และการฝึกอบรม (Cybersecurity Awareness Training) เพื่อให้มีการส่งเสริมและจัดการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรทุกระดับ รวมถึงผู้รับเหมาและผู้ให้บริการภายนอก เพื่อให้รู้เท่าทันรูปแบบของภัยคุกคาม รวมถึงแนวทางปฏิบัติในการใช้เทคโนโลยีดิจิทัลในการประกอบวิชาชีพอย่างปลอดภัย โดยกำหนดให้มีการทบทวนและปรับปรุงแผนงานการสร้างความตระหนักรู้อย่างน้อย ปีละ ๑ ครั้ง