

Subject

Re: ขอเรียนปรึกษาเรื่องการแก้ไขนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ สถาบันมาตรวิทยาแห่งชาติ ประจำปี 2570

From Jarat Somwang <jarat@nimt.or.th>

To Chatchai Phongwichial <chatchai@nimt.or.th>

Cc Manop Tinsirisuk <manop@nimt.or.th>

Date Thursday January 29, 2026 2:19:08 PM

เรียน คุณชัชชัย พนักงานกลุ่มงานเทคโนโลยีสารสนเทศ

ตามที่คุณชัชชัยได้ส่งจดหมายอิเล็กทรอนิกส์เพื่อขอเรียนปรึกษาหน่วยงานตรวจสอบภายใน เกี่ยวกับประเด็นการทบทวน/ปรับปรุง/แก้ไข นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปีงบประมาณ 2570 นั้น

หน่วยงานตรวจสอบภายในได้พิจารณาตามเอกสารประกอบที่คุณชัชชัยส่งมา จึงมีข้อเสนอแนะ ดังนี้

1. การปรับปรุงแก้ไขข้อความ ในหมวดที่ 1 การเข้าถึงและควบคุมการ ใช้งานสารสนเทศ (Access Control) ข้อ 2. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility) ในประเด็นข้อย่อยที่ 2.1.4 และ ข้อย่อยที่ 2.1.5 ซึ่งในนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปีงบประมาณ 2569 ทั้ง 2 ข้อดังกล่าวมีเนื้อหาที่ต่อเนื่องกัน หน่วยงานตรวจสอบภายในจึงมีความเห็นว่า ควรควรรวมทั้ง 2 ข้อดังกล่าวไว้ด้วยกัน ให้คงเหลือเพียงข้อเดียว เพื่อให้มีความกระชับ เข้าใจง่าย พนักงานสถาบันสามารถปฏิบัติงานได้อย่างถูกต้อง

2. การปรับปรุงแก้ไขข้อความ ในหมวดที่ 1 การเข้าถึงและควบคุมการ ใช้งานสารสนเทศ (Access Control) ข้อ 4 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) ข้อย่อยที่ 4.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Restrict Information system connection period)

- ข้อ 4.6.1 กำหนดให้มีการจำกัดช่วงระยะเวลาการเชื่อมต่อระบบสารสนเทศ เพื่อให้มีการใช้งานภายในระยะเวลาที่กำหนด โดยกำหนดให้ใช้งานได้ตั้งแต่เวลา ๖.๐๐ น. ถึง ๑๙.๐๐ น. ในวันทำการเท่านั้น

- ข้อ 4.6.2 กำหนดให้มีการจำกัดระยะเวลาในการเชื่อมต่อที่สั้นลงสำหรับระบบสารสนเทศที่มีความสำคัญเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต และเป็นไปตามข้อ ๒.๒ ข้อ ๒.๓ และข้อ ๒.๔

- ข้อ 4.6.3 ยกเว้นบางระบบเชื่อมต่อที่ต้องใช้การเชื่อมต่อตลอดเวลาที่จำเป็นในการ Script เพื่อทำการ Backup ข้อมูล และในบางระบบที่จำเป็นต้องเชื่อมต่อตลอดเวลาเช่น ระบบสอบเทียบ เพื่อสนองความต้องการของลูกค้าตลอด ๒๔ ชั่วโมง

- 4.6.3.1 ระบบภายใน สามารถเชื่อมต่อในเวลาราชการ

- 4.6.3.2 ระบบภายนอก เปิดตลอดเวลา (ระบบทำงาน ๒๔ ชั่วโมง) เช่น ระบบสำรองข้อมูล ระบบสอบเทียบบริการลูกค้า การ Monitor ระบบวันละ ๑ ครั้ง

คุณชัชชัย ขอปรึกษาหารือว่าควรดำเนินการตัดข้อความข้อ 4.6.1 , 4.6.2 และ 4.6.3 ออกจากนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปีงบประมาณ 2570 หรือไม่ เนื่องจากปัจจุบันสถาบันโดยกลุ่มงานเทคโนโลยีสารสนเทศไม่ได้จำกัดเวลาการเข้าถึงระบบสารสนเทศของสถาบันจากผู้ใช้งาน(พนักงานสถาบัน) เนื่องจากกระบวนการดำเนินงานของผู้ใช้งานบางฝ่ายจำเป็นต้องเข้าถึงระบบสารสนเทศของสถาบันตลอดเวลา นั้น

หน่วยงานตรวจสอบภายในได้พิจารณาข้อปรึกษาข้อที่ 2 และได้ศึกษา พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และนโยบายรักษาความปลอดภัยด้านสารสนเทศของหน่วยงานราชการอื่น ๆ แล้ว พบว่า มีการกำหนดให้มีการจำกัดช่วงระยะเวลาการเชื่อมต่อระบบสารสนเทศ ทุกหน่วยงาน(เคสที่ศึกษา) จึง

เห็นควรให้คงข้อความ ข้อ 4.6.1 , ข้อ 4.6.2 และ ข้อ 4.6.3 ไว้ เพื่อให้เป็นไปตามหลักสากล และให้เพิ่มข้อความ ข้อ 4.6.3 จากเดิม โดยให้ระบุหน่วยงานที่มีความจำเป็นต้องใช้งานระบบสารสนเทศนอกเวลาราชการ (โดยการสำรวจความจำเป็นในการใช้งานระบบสารสนเทศของทุกฝ่ายของสถาบัน)

จึงเรียนมาเพื่อโปรดพิจารณา'ตามข้อเสนอแนะของหน่วยงานตรวจสอบภายใน

ขอแสดงความนับถือ

จรัส สมหวัง

พณ.ตรวจสอบภายในชำนานฎการ

โทร 4209

From: Chatchai <chatchai@nimt.or.th>

To: Jarat <jarat@nimt.or.th>

Date: Thursday, 29 January 2026 10:17 AM +07

Subject: ขอเรียนปรึกษาเรื่องการแก้ไขนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ สถาบันมาตรวิทยาแห่งชาติ ประจำปี 2570

เรียนผู้ตรวจสอบภายใน

ผมขอเรียนปรึกษาเรื่องการแก้ไขนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ สถาบันมาตรวิทยาแห่งชาติ ประจำปี 2570 ตามที่ได้ตรวจสอบเมื่อปี ที่ผ่านมา ผมได้แก้ไขและตัดข้อความตามภาพที่ส่งมาแล้ว โปรดพิจารณาและให้คำแนะนำด้วยครับ

ขอบคุณครับ

ชัชชัย พงษ์วิเชียร

กทส.ฝน.