สถาบันมาตรวิทยาแห่งชาติ
National Institute of Metrology (Thailand)
NIMT

รายงานการตรวจสอบ
Audit Report
เรื่อง
ระบบงานเทคโนโลยีสารสนเทศ
กลุ่มงานเทคโนโลยีสารสนเทศ
ฝ่ายนโยบายและยุทธศาสตร์

หน่วยงานตรวจสอบภายใน
โทร 4240 4209

รายงานการตรวจสอบ

เรื่อง การตรวจสอบระบบงานเทคโนโลยีสารสนเทศ

หน่วยงาน/กิจกรรม กลุ่มงานเทคโนโลยีสารสนเทศ/ฝ่ายนโยบายและยุทธศาสตร์

วัตถุประสงค์การตรวจสอบ

1. เพื่อประเมินความเพียงพอของระบบรักษาความปลอดภัยทางไซเบอร์ ของกลุ่มงานเทคโนโลยีสารสนเทศ ให้เป็นไปอย่างมีประสิทธิภาพและเกิดประสิทธิผล
2. เพื่อให้แน่ใจว่ามีการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี 2569 สถาบันมาตรวิทยาแห่งชาติ อย่างครบถ้วน ถูกต้อง และเหมาะสม
3. เพื่อให้ความมั่นใจในความสมบูรณ์ ความถูกต้องตรงกันทุกประการ ความสมเหตุสมผล ของข้อมูลและการจำกัดการเข้าถึงข้อมูลและสินทรัพย์ทางสารสนเทศของสถาบัน(Application Control)

ขอบเขตการตรวจสอบ

การตรวจสอบในครั้งนี้ เป็นการตรวจสอบการปฏิบัติงานและประเมินความเพียงพอของการควบคุมภายในของระบบงานเทคโนโลยีสารสนเทศ ระบบรักษาความปลอดภัยทางไซเบอร์ มีการปฏิบัติงานตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี 2569 ของสถาบันมาตรวิทยาแห่งชาติ อย่างครบถ้วน เหมาะสม เพื่อสนับสนุนภารกิจของสถาบันให้บรรลุเป้าหมายที่วางไว้ได้อย่างเหมาะสม

ขอบเขตการตรวจสอบข้อมูลการปฏิบัติงานของกลุ่มงานเทคโนโลยีสารสนเทศสำหรับปีงบประมาณ พ.ศ. 2568 เริ่มตั้งแต่เดือน ตุลาคม 2567 ถึงสิ้นสุด เดือน สิงหาคม 2568 ดังนี้

1. ตรวจสอบการดำเนินการเพื่อพัฒนาระบบความปลอดภัยไซเบอร์ของสถาบัน ประจำปีงบประมาณ พ.ศ. 2568

2. ตรวจสอบเอกสารหลักฐานการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี 2569 ของสถาบันมาตรวิทยาแห่งชาติ

3.ตรวจสอบความสมบูรณ์ ความถูกต้องตรงกันทุกประการ ความสมเหตุสมผล ของข้อมูลของโปรแกรมระบบสอบเทียบของสถาบัน

ระเบียบที่เกี่ยวข้อง

1. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี 2569 ของสถาบันมาตรวิทยาแห่งชาติ
2. ประกาศสถาบันมาตรวิทยาแห่งชาติ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานในการรักษาความปลอดภัยไซเบอร์(Guideline and Cybersecurity Framework) ของสถาบันมาตรวิทยาแห่งชาติ พ.ศ. 2568
3. แผนการรับมือภัยคุกคามทางไซเบอร์(Cyber Incident Response Plan) สถาบันมาตรวิทยาแห่งชาติ พ.ศ. 2568
4. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์(Cybersecurity Audit Plan) สถาบันมาตรวิทยาแห่งชาติ พ.ศ. 2568

5. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) สถาบันมาตรวิทยาแห่งชาติ พ.ศ. 2568

ผู้รับผิดชอบโครงการตรวจสอบ

นายมาณพ ติณสิริสุข	ผู้ตรวจสอบภายใน	.....
นายจรัส สมหวัง	พนักงานตรวจสอบภายในชำนาญการ	.....

สารบัญ

บทสรุปผู้บริหาร

(Executive Summary)

จากการตรวจสอบการปฏิบัติงานและการควบคุมภายใน ของระบบงานเทคโนโลยีสารสนเทศ กลุ่มงานเทคโนโลยีสารสนเทศ ฝ่ายนโยบายและยุทธศาสตร์ ข้อมูลสิ้นสุด ณ. วันที่ 31 สิงหาคม 2568 มีประเด็นสำคัญสรุปดังนี้

1.) การดำเนินการเพื่อพัฒนาระบบความปลอดภัยไซเบอร์ของสถาบัน ประจำปีงบประมาณ พ.ศ. 2568

1.1 ตามรายงานการตรวจสอบระบบเทคโนโลยีสารสนเทศ ประจำปี 2567 สถาบันมี Firewall เพื่อใช้งานป้องกันการโจมตีทางไซเบอร์จำนวน 3 ประเภท ได้แก่

1.Sophos เพื่อป้องกันรักษาความปลอดภัย เครือข่าย LAN ของสถาบัน

2.Cisco เพื่อป้องกันรักษาความปลอดภัย เครือข่าย Wi-Fi ของสถาบัน

3.Sangfor เพื่อป้องกันรักษาความปลอดภัยของระบบ VPN หรือ การรีโมทระยะไกลของสถาบัน

จากการติดตามการแก้ไขปรับปรุงในปีงบประมาณ พ.ศ. 2568 จากรายงานการตรวจสอบประจำปี พ.ศ.2567 พบว่าสถาบันฯ มีระบบการป้องกัน Firewall บางส่วนไม่ครอบคลุม โดยเฉพาะ ในส่วนที่ป้องกันรักษาความปลอดภัย Web Application ซึ่งการป้องกันในกรณีดังกล่าว พบว่ากลุ่มงานเทคโนโลยีสารสนเทศได้ทำการประสานงานเพื่อขอความอนุเคราะห์จากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. เพื่อขอใช้ Firewall ในการใช้ป้องกัน Web Application และได้รับความอนุเคราะห์จาก สพร. ให้สถาบันฯ สามารถดำเนินการเพื่อได้ใช้ระบบป้องกัน Firewall ได้ แต่มีข้อจำกัดในด้านระยะเวลาที่กำหนดให้สถาบันฯ ใช้งานได้เพียง 1 ปี เท่านั้น จึงมีความจำเป็นที่ต้องจัดหา Firewall ที่ทำหน้าที่ในการป้องกัน Web Application ในอนาคตต่อไป

1.2 กลุ่มงานเทคโนโลยีสารสนเทศ ได้จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) ของสถาบันมาตรวิทยาแห่งชาติ พ.ศ. 2568 ตาม พ.ร.บ.การรักษาความมั่งคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 และประกาศใช้เมื่อวันที่ 16 เมษายน 2568 เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบัน มีประสิทธิภาพ มีความปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีดิจิทัลในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ

2.) การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศประจำปี 2569 ของสถาบันมาตรวิทยาแห่งชาติ

สถาบันได้ประกาศใช้ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศประจำปี 2569 เมื่อวันที่ 2 พฤษภาคม 2568 ซึ่งจากการตรวจสอบ พบว่า กลุ่มงานเทคโนโลยีสารสนเทศได้ปฏิบัติตามอย่างถูกต้อง เหมาะสม มีเพียงบางประเด็นที่ต้องดำเนินการปรับปรุงรายละเอียดของนโยบายและแนวปฏิบัติ ฯ เพื่อให้เกิดความทันสมัยและเป็นไปตามการปฏิบัติงานจริงของสถาบัน

3.) การตรวจสอบการควบคุมภายในเฉพาะระบบงาน (Application Control) โปรแกรมสอบเทียบของสถาบันมาตรวิทยาแห่งชาติ

การตรวจสอบการควบคุมภายในเฉพาะระบบงาน (Application Control) โปรแกรมสอบเทียบของสถาบันมาตรวิทยาแห่งชาติ ได้ดำเนินการโดยใช้คำสั่ง SQL Script Commands เพื่อตรวจสอบจำนวน 12 รายการ อาทิเช่น การตรวจสอบ Check digit validation การตรวจสอบ Range Check เป็นต้น **พบว่า** โปรแกรมระบบสอบเทียบของสถาบัน ให้ผลการตรวจสอบที่ถูกต้อง ไม่มีรายการ Error ทั้ง 12 รายการที่ตรวจสอบ จึงให้ความเชื่อมั่นได้ว่าโปรแกรมระบบสอบเทียบของสถาบัน มีความสมบูรณ์ ความถูกต้องตรงกันทุกประการ ความสมเหตุสมผล ของข้อมูล สร้างความเชื่อถือทั้งระบบต่อผู้ใช้งาน

เพื่อให้การเปลี่ยนผ่านของสถาบันก้าวไปสู่ยุคมาตรวิทยาดิจิทัลเป็นไปอย่างมีประสิทธิภาพ ดังนั้นระบบงานเทคโนโลยีสารสนเทศจึงมีความสำคัญอย่างยิ่ง เพื่อช่วยสนับสนุนฝ่ายงานด้านมาตรวิทยาและฝ่ายงานภายในสถาบัน จึงมีความจำเป็นต้องได้รับการสนับสนุนงบประมาณจากผู้บริหารของสถาบันอย่างเต็มที่ เพื่อสามารถส่งเสริมการเปลี่ยนผ่านของสถาบันสู่ยุคมาตรวิทยาดิจิทัลได้อย่างมีประสิทธิภาพสูงสุดได้

รายงานการตรวจสอบ

Audit Report

หน่วยงาน/ระบบงาน ระบบงานเทคโนโลยีสารสนเทศ **โครงการเลขที่ IA-68-004**

สิ่งที่ตรวจพบ (Audit Finding)	ข้อเสนอแนะของผู้ตรวจสอบ (Recommendation)	ความเห็นหน่วยรับตรวจ/กำหนดเสร็จ (Auditee's Opinion/Action Plan)
ความเสี่ยงระดับสูง		
1.) การดำเนินการเพื่อพัฒนาระบบความปลอดภัยไซเบอร์ของสถาบัน ประจำปีงบประมาณ พ.ศ. 2568 การดำเนินการเพื่อพัฒนาระบบความปลอดภัยไซเบอร์ของสถาบัน ประจำปีงบประมาณ 2568 มีดังนี้ 1.1 ตามรายงานการตรวจสอบระบบเทคโนโลยีสารสนเทศ ประจำปี 2567 สถาบันมี Firewall เพื่อใช้งานป้องกันการโจมตีทางไซเบอร์จำนวน 3 ประเภท ได้แก่ 1.Sophos เพื่อป้องกันรักษาความปลอดภัย เครือข่าย LAN ของสถาบัน 2.Cisco เพื่อป้องกันรักษาความปลอดภัย เครือข่าย Wi-Fi ของสถาบัน 3.Sangfor เพื่อป้องกันรักษาความปลอดภัยของระบบ VPN หรือ การรีโมทระยะไกลของสถาบัน ยังคงขาด Firewall ในส่วนที่ป้องกันรักษาความปลอดภัย Web Application นั้น จากการติดตามการแก้ไขปรับปรุงในปีงบประมาณ พ.ศ. 2568 พนักงานกลุ่มงานเทคโนโลยีสารสนเทศได้ประสานขอความอนุเคราะห์จากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เพื่อขอใช้ Firewall ที่ทำหน้าที่ป้องกัน Web Application ซึ่งได้รับความอนุเคราะห์ให้ใช้งาน Firewall ดังกล่าวได้ แต่มีข้อจำกัดด้วยว่า Firewall ดังกล่าวสามารถใช้งานได้เพียง 1 ปี จึงมีความจำเป็นที่ต้องจัดหา Firewall ที่ทำหน้าที่ป้องกัน Web Application อย่างถาวรมาใช้งาน 1.2 กลุ่มงานเทคโนโลยีสารสนเทศ ได้	**ประเด็นความเสี่ยง** - สถาบันมี Firewall ที่ทำหน้าที่ป้องกัน Web Application โดยระบบ Firewall ที่ใช้งานในปัจจุบันได้รับความอนุเคราะห์จากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ให้สถาบันฯ ใช้งานชั่วคราว โดยมีระยะเวลาการใช้งานได้เพียง 1 ปี เท่านั้น **ประเมินความเสี่ยง** = ระดับสูง **ผลกระทบ** หากพ้นกำหนดเวลา 1 ปี แล้ว อาจเกิดความไม่ปลอดภัยทางไซเบอร์ ที่ผู้ไม่ประสงค์ดีจะโจมตีระบบ Web Application ของสถาบันได้ **ข้อเสนอแนะ** 1.กลุ่มงานเทคโนโลยีสารสนเทศควรพิจารณาจัดทำโครงการเพื่อเสนอการจัดซื้อ Firewall ต่อผู้บริหารเพื่อพิจารณาความเหมาะสม เพื่อใช้ในการป้องกัน Firewall ที่อาจมีผลกระทบต่อระบบโปรแกรมงาน Web Application มาใช้งาน 2. ในกรณีที่สถาบันไม่ได้รับการจัดสรรงบประมาณในการจัดซื้อ Firewall ดังกล่าว ระดับผู้บริหารของสถาบันฯ ควรประสานงานหรือทำการเจรจา กับสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. ในระดับผู้บริหารของทั้ง 2	กลุ่มงานเทคโนโลยีสารสนเทศได้ทำการประสานงานเพื่อขอความอนุเคราะห์จากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. เพื่อขอใช้ Firewall ในการใช้ป้องกัน Web Application และได้รับความอนุเคราะห์จาก สพร. ให้สถาบันฯ สามารถดำเนินการเพื่อได้ใช้ระบบป้องกัน Firewall ได้ แต่มีข้อจำกัดในด้านระยะเวลาที่กำหนดให้สถาบันฯ ใช้งานได้เพียง 1 ปี เท่านั้น จึงมีความจำเป็นที่ต้องจัดหา Firewall ที่ทำหน้าที่ในการป้องกัน Web Application ในอนาคตต่อไป - รับทราบข้อเสนอแนะของผู้ตรวจสอบภายใน และได้ดำเนินการจัดทำคำของบประมาณเพื่อจัดซื้อ Firewall ที่ใช้ป้องกันรักษาความปลอดภัย Web Application ในปีงบประมาณ พ.ศ. 2570 ในส่วนข้อเสนอแนะที่ 2 หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศจะนำเรื่องเข้าปรึกษาหารือกับ CIO ของสถาบันต่อไป

สิ่งที่ตรวจพบ (Audit Finding)	ข้อเสนอแนะของผู้ตรวจสอบ (Recommendation)	ความเห็นหน่วยรับตรวจ/ กำหนดเสร็จ (Auditee's Opinion/Action Plan)
จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) ของสถาบันมาตรวิทยาแห่งชาติ พ.ศ. 2568 ตาม พ.ร.บ.การรักษาความมั่งคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 และประกาศใช้เมื่อวันที่ 16 เมษายน 2568 เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบัน มีประสิทธิภาพ มีความปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีดิจิทัลในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ	องค์กร เพื่อสถาบันฯ ขอความอนุเคราะห์ใช้ Firewall จาก สพร. ในการป้องกัน Firewall ที่อาจกระทบต่อโปรแกรม Web Application มาใช้งานต่อไป	
2.) <u>การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี 2568 ของสถาบันมาตรวิทยาแห่งชาติ</u> <u>2.1) แนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ</u> สถาบันโดยกลุ่มงานเทคโนโลยีสารสนเทศได้ดำเนินการจัดทำและประกาศใช้ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี 2569 เมื่อวันที่ 2 พฤษภาคม 2568 ในระบบ Intranet ของสถาบัน พบว่า การปฏิบัติงานของสถาบันดำเนินการตามนโยบายและแนวปฏิบัติที่ได้ประกาศใช้ และเป็นไปตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์แห่งชาติ อย่างถูกต้อง เหมาะสม	**<u>ไม่พบประเด็นความเสี่ยง</u>**	
<u>2.2) แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่กระทบ พ.ร.บ. คอมพิวเตอร์</u> สถาบันโดยกลุ่มงานเทคโนโลยีสารสนเทศได้ให้ความสำคัญต่อการปฏิบัติตาม พ.ร.บ. คอมพิวเตอร์ทุกฉบับ ซึ่งได้ระบุข้อปฏิบัติตาม พ.ร.บ.คอมพิวเตอร์ไว้ในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2569 และได้ดำเนินงานตามขั้นตอนปฏิบัติที่ระบุไว้ในนโยบายและแนวปฏิบัติดังกล่าว อย่างเคร่งครัด อาทิ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ 90 วัน และการ	**<u>ไม่พบประเด็นความเสี่ยง</u>**	

สิ่งที่ตรวจพบ (Audit Finding)	ข้อเสนอแนะของผู้ตรวจสอบ (Recommendation)	ความเห็นหน่วยรับตรวจ/ กำหนดเสร็จ (Auditee's Opinion/Action Plan)
สื่อสารเนื้อหาสาระ แนวปฏิบัติ ข้อพึงระวัง ในการใช้งานคอมพิวเตอร์และระบบสารสนเทศของสถาบัน ในรูปแบบ Infographic ที่หน้าจอคอมพิวเตอร์ของพนักงานสถาบันทุกคน (ผู้ใช้งาน)		
2.3) การควบคุมการเข้าถึงและควบคุมการใช้งาน สถาบันโดยกลุ่มงานเทคโนโลยีสารสนเทศได้ดำเนินการเกี่ยวกับการควบคุมการเข้าถึงและการควบคุมการใช้งานของผู้ใช้งาน เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ **ยกเว้น การกำหนดเวลาในการเข้าถึงสารสนเทศของสถาบัน ซึ่งในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี 2569 กำหนดไว้ที่เวลา 06.00 น.ถึง 19.00 น. แต่การปฏิบัติจริงไม่สามารถกำหนดเวลาเข้าถึงสารสนเทศได้เนื่องจากความจำเป็นในการใช้งานของพนักงานของสถาบัน**	**ประเด็นความเสี่ยง** การปฏิบัติงานของพนักงานของสถาบันไม่เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความปลอดภัยด้านสารสนเทศประจำปี 2569 ในบางประเด็น **ประเมินความเสี่ยง** = ระดับปานกลาง **ผลกระทบ** ทำให้พนักงานของสถาบันดำเนินการไม่เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่สถาบันประกาศใช้ **ข้อเสนอแนะ** เนื่องจากความจำเป็นในการใช้งานสารสนเทศนอกเวลาทำการของพนักงานสถาบัน เห็นควรให้ในการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในปีถัดไป ให้แก้ไขให้ตรงตามการปฏิบัติงานจริง เพื่อให้การปฏิบัติงานของสถาบันเป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างถูกต้อง เหมาะสม	ในการทบทวนและปรับปรุงเพื่อจัดทำนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี 2570 กลุ่มงานจะดำเนินการปรับปรุงตามข้อเสนอแนะของผู้ตรวจสอบภายใน
2.4) การใช้งานตามภารกิจ สถาบันโดยกลุ่มงานเทคโนโลยีสารสนเทศได้ดำเนินการควบคุมการเข้าถึงระบบสารสนเทศโดยการใช้รหัสผ่านเป็นการให้สิทธิแก่ผู้ใช้งานตามภารกิจ(พนักงานของสถาบันทุกคน) ซึ่งการควบคุมการเข้าถึงระบบสารสนเทศได้บรรจุไว้ในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2569 สถาบันมาตรวิทยาแห่งชาติ	**ไม่พบประเด็นความเสี่ยง**	
2.5) การบริหารจัดการการเข้าถึงของผู้ใช้งาน	**ไม่พบประเด็นความเสี่ยง**	ในการทบทวนและปรับปรุงเพื่อ

สิ่งที่ตรวจพบ (Audit Finding)	ข้อเสนอแนะของผู้ตรวจสอบ (Recommendation)	ความเห็นหน่วยรับตรวจ/ กำหนดเสร็จ (Auditee's Opinion/Action Plan)
สถาบันโดยกลุ่มงานเทคโนโลยีสารสนเทศได้ดำเนินการเกี่ยวกับการบริหารจัดการการเข้าถึงผู้ใช้งานได้อย่างเหมาะสม มีการดำเนินการให้ความรู้ผ่านการอบรมพนักงานและผ่านระบบ Infographic หน้าจอคอมพิวเตอร์ของผู้ใช้งาน และได้ดำเนินการให้มีการทบทวนสิทธิของผู้ใช้งานทุกปี ปีละ 1 ครั้ง ตามรายงานการทบทวนบัญชีผู้ใช้งานระบบสารสนเทศ ประจำปี 2568	**ข้อเสนอแนะ** เพื่อให้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีความกระชับเข้าใจง่าย เห็นควรให้ในการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในปีถัดไป ปรับแก้ไขข้อความของ หมวดที่ 1 ข้อ 2 หน้าที่ความรับผิดชอบของผู้ใช้งาน โดยปรับข้อความของข้อ 2.1.4 และ 2.1.5 ซึ่งมีเนื้อหาเดียวกันให้รวมเป็นข้อเดียว	จัดทำนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี 2570 กลุ่มงานจะดำเนินการปรับปรุงตามข้อเสนอแนะของผู้ตรวจสอบภายใน
2.6) การเข้าถึงระบบเครือข่าย การควบคุมการเข้าถึงระบบเครือข่ายของสถาบัน โดยกลุ่มงานเทคโนโลยีสารสนเทศได้ดำเนินการตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปี 2568 อย่างเคร่งครัดและเหมาะสม อาทิ เช่น การยืนยันตัวบุคคลก่อนการเข้าใช้งาน การควบคุม Port สำหรับการตรวจสอบ และ Port สำหรับการปรับแต่งระบบ	**ไม่พบประเด็นความเสี่ยง**	
2.7) การเข้าถึงระบบปฏิบัติการ สถาบันโดยกลุ่มงานเทคโนโลยีสารสนเทศได้ดำเนินการเกี่ยวกับการควบคุมการเข้าถึงระบบปฏิบัติการและการควบคุมการใช้งานของผู้ใช้งาน เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ **ยกเว้น การกำหนดเวลาในการเข้าถึงสารสนเทศของสถาบัน ซึ่งในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกำหนดไว้ที่เวลา 06.00 น.ถึง 19.00 น. แต่การปฏิบัติจริงไม่สามารถกำหนดเวลาเข้าถึงสารสนเทศได้เนื่องจากความจำเป็นในการใช้งานของพนักงานของสถาบัน**	**ประเด็นความเสี่ยง** การปฏิบัติงานของพนักงานของสถาบันไม่เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความปลอดภัยด้านสารสนเทศประจำปี 2569 ในบางประเด็น **ประเมินความเสี่ยง** = ระดับปานกลาง **ผลกระทบ** ทำให้พนักงานของสถาบันดำเนินการไม่เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่สถาบันประกาศใช้ **ข้อเสนอแนะ** เนื่องจากความจำเป็นในการใช้งานสารสนเทศนอกเวลาทำการของ	กลุ่มงานเทคโนโลยีสารสนเทศจะปรับแก้ไขเนื้อหาของนโยบายและแนวปฏิบัติการรักษาความปลอดภัยด้านสารสนเทศ ประจำปี 2570 ใน หมวดที่ 1 ข้อ 4.6.1 ประเด็นการเข้าถึงระบบปฏิบัติการ โดยใช้คำว่า "ผู้ดูแลระบบ" แทน "ผู้ใช้งาน" และจะไม่กำหนดเวลาในการเข้าถึงระบบปฏิบัติการของผู้ดูแลระบบ

สิ่งที่ตรวจพบ (Audit Finding)	ข้อเสนอแนะของผู้ตรวจสอบ (Recommendation)	ความเห็นหน่วยรับตรวจ/ กำหนดเสร็จ (Auditee's Opinion/Action Plan)
	พนักงานสถาบัน เห็นควรให้ในการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในปีถัดไป ให้แก้ไขให้ตรงตามการปฏิบัติงานจริง เพื่อให้การปฏิบัติงานของสถาบันเป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างถูกต้อง เหมาะสม	
2.8) การเข้าถึงโปรแกรมประยุกต์ หรือ Application และสารสนเทศ การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือ Application และสารสนเทศ ของสถาบัน โดยกลุ่มงานเทคโนโลยีสารสนเทศ ได้ดำเนินการตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปี 2569 อย่างเคร่งครัดและเหมาะสม โดยการใช้รหัสผ่านเฉพาะบุคคล ตามอำนาจหน้าที่ของพนักงานนั้น ๆ ซึ่งปัจจุบันกำหนดให้พนักงานต้องทำการเปลี่ยนรหัสผ่านทุก ๆ 90 วัน	**ไม่พบประเด็นความเสี่ยง**	
2.9) การจัดระบบสำรองและแผนเตรียมความพร้อม กรณี ฉุกเฉิน สถาบันโดยกลุ่มงานเทคโนโลยีสารสนเทศ ได้ดำเนินการเกี่ยวกับการการจัดระบบสำรองและแผนเตรียมความพร้อม กรณี ฉุกเฉิน และมีการทบทวนและปรับปรุงทุกปี อย่างน้อย 1 ครั้งต่อปี มีการกำหนดตัวบุคคลไว้เพื่อรองรับการดำเนินการหากเกิด กรณี ฉุกเฉินขึ้นมา สามารถดำเนินการได้อย่างทันท่วงที และได้ดำเนินการซ้อมรับมือหากเกิดกรณีฉุกเฉินขึ้น	**ไม่พบประเด็นความเสี่ยง**	
2.10) การสอบทาน การจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ 1.หน่วยงานตรวจสอบภายในได้บรรจุโครงการตรวจสอบระบบเทคโนโลยีสารสนเทศของสถาบันเข้าไว้ในแผนปฏิบัติงานตรวจสอบประจำปี ทุกปี และได้จัดทำบันทึก รายงานผลการตรวจสอบระบบเทคโนโลยีสารสนเทศเพื่อนำเสนอข้อตรวจพบ ข้อเสนอแนะ ต่อผู้บริหารทุกครั้ง	**ไม่พบประเด็นความเสี่ยง**	

สิ่งที่ตรวจพบ (Audit Finding)	ข้อเสนอแนะของผู้ตรวจสอบ (Recommendation)	ความเห็นหน่วยรับตรวจ/ กำหนดเสร็จ (Auditee's Opinion/Action Plan)
2.ผู้ตรวจสอบภายนอกที่สถาบันจัดจ้างเพื่อดำเนินการตรวจสอบระบบงานต่าง ๆ ของสถาบันได้ดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568 และนำเสนอผลการตรวจสอบต่อผู้บริหารสถาบันทุกครั้ง **และพบว่า สถาบันโดยกลุ่มงานเทคโนโลยีสารสนเทศได้ดำเนินการแก้ไขตามข้อเสนอแนะของผู้ตรวจสอบภายนอก(บ.สอบบัญชีธรรมนิติ จำกัด เรียบร้อยแล้ว โดยได้มีการกำหนดวิธีการจัดการหรือทำลายสื่อบันทึกข้อมูล (Media Handling) ที่หมดอายุการใช้งานหรือไม่ประสงค์จะใช้งานแล้วอย่างมีลายลักษณ์อักษร ไว้ในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปี 2569 ในหมวดที่ 3 ข้อ 7 เรียบร้อยแล้ว**		
<u>3.ตรวจสอบการควบคุมภายในเฉพาะระบบงาน (Application Control) โปรแกรมสอบเทียบของสถาบันมาตรวิทยาแห่งชาติ</u> การตรวจสอบการควบคุมภายในเฉพาะระบบงาน (Application Control) โปรแกรมสอบเทียบของสถาบันมาตรวิทยาแห่งชาติ ได้ดำเนินการโดยใช้คำสั่ง SQL Script Commands เพื่อตรวจสอบ จำนวน 12 รายการ ได้แก่ 1.Check digit validation ทดสอบข้อมูลวันที่ได้แก่ วันที่รับเครื่องมือ วันที่ส่งมอบให้เครื่องมือวัดให้ห้องปฏิบัติการ วันที่ส่งมอบเครื่องคืนให้ลูกค้า ของระบบสอบเทียบ	**<u>ไม่พบประเด็นความเสี่ยง</u>**	
2.Range Check ทดสอบข้อมูลของลูกค้าได้แก่ ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล์ ในระบบสอบเทียบ		
3. Limit Check ทดสอบการอนุมัติปิดงาน (ปิดใบ Work Order) สถานะของ Job ในระบบสอบเทียบ		

สิ่งที่ตรวจพบ (Audit Finding)	ข้อเสนอแนะของผู้ตรวจสอบ (Recommendation)	ความเห็นหน่วยรับตรวจ/ กำหนดเสร็จ (Auditee's Opinion/Action Plan)
4. Sequence Check ทดสอบเลขที่ใบ Work Order ไม่ซ้ำกัน ในระบบสอบเทียบ		
5. Type check ทดสอบ Data Type ของข้อมูลในระบบสอบเทียบ เช่น ตัวอักษร ตัวเลข		
6. Self-checking digit check ทดสอบความยาวของตัวอักษรในระบบสอบเทียบ		
7.การอนุมัติรายการ ทดสอบการอนุมัติผลการสอบเทียบเครื่องมือโดยใช้รหัสผ่านโปรแกรมของหัวหน้าฝ่าย/หัวหน้ากลุ่มงาน		
8.การบันทึกรายการ ทดสอบ การบันทึกรายการใบขอสอบเทียบ (CIF)		
9.การรวบรวมข้อมูลรายการทดสอบการรวบรวมข้อมูล เช่น ชื่อลูกค้า สัญชาติ ที่อยู่ ชื่อเครื่องมือวัดที่นำมาสอบเทียบ		
10.การควบคุมยอดรวม ทดสอบ ยอด Summary ของใบ Work Order ภายใน 1 วันทำการ ในระบบสอบเทียบ		
11.ควบคุมการเข้าถึง ทดสอบการทำงานของผู้ใช้งานโดยการทดสอบ Pass word เข้าโปรแกรมระบบสอบเทียบ		
12.การควบคุมข้อมูลส่งออก ทดสอบการส่งข้อมูลให้ลูกค้ารับทราบของโปรแกรมระบบสอบเทียบ		
<u>ข้อตรวจพบ</u> การตรวจสอบการควบคุมภายในเฉพาะระบบงาน (Application Control) โปรแกรมสอบเทียบของสถาบันมาตรวิทยาแห่งชาติ ได้ดำเนินการโดยใช้คำสั่ง SQL Script Commands เพื่อตรวจสอบ จำนวน 12 รายการ ได้แก่ 1.Check digit validation 2.Range Check 3. Limit Check 4. Sequence Check 5.		

สิ่งที่ตรวจพบ (Audit Finding)	ข้อเสนอแนะของผู้ตรวจสอบ (Recommendation)	ความเห็นหน่วยรับตรวจ/ กำหนดเสร็จ (Auditee's Opinion/Action Plan)
Type check 6. Self-checking digit check 7.การอนุมัติรายการ 8.การบันทึกรายการ 9.การรวบรวมข้อมูลรายการ 10.การควบคุมยอดรวม 11.ควบคุมการเข้าถึง 12.การควบคุมข้อมูลส่งออก พบว่า โปรแกรมระบบสอบเทียบของสถาบัน ให้ผลการตรวจสอบที่ถูกต้อง ไม่มีรายการ Error ทั้ง 12 รายการที่ตรวจสอบ จึงให้ความเชื่อมั่นได้ว่าโปรแกรมระบบสอบเทียบของสถาบัน มีความสมบูรณ์ ความถูกต้องตรงกันทุกประการ ความสมเหตุสมผล ของข้อมูล สร้างความเชื่อถือทั้งระบบต่อผู้ใช้งาน		