ประกาศกรมสุขภาพจิต
เรื่อง รายชื่อผู้ผ่านการประเมินบุคคลเพื่อเลื่อนขึ้นแต่งตั้งให้ดำรงตำแหน่งประเภทวิชาการ ระดับชำนาญการ

ตามหนังสือสำนักงาน ก.พ. ที่ นร ๑๐๐๖/ว ๑๔ ลงวันที่ ๑๑ สิงหาคม ๒๕๖๔ ได้กำหนดหลักเกณฑ์และวิธีการประเมินบุคคลเพื่อเลื่อนขึ้นแต่งตั้งให้ดำรงตำแหน่งในตำแหน่งระดับควบ และมีผู้ครองตำแหน่งนั้นอยู่ โดยให้ผู้มีอำนาจสั่งบรรจุตามมาตรา ๕๗ หรือผู้ที่ได้รับมอบหมายเป็นผู้ประเมินบุคคลตามหลักเกณฑ์และวิธีการที่ อ.ก.พ. กรมสุขภาพจิต กำหนด นั้น

กรมสุขภาพจิต ได้คัดเลือกข้าราชการผู้ผ่านการประเมินบุคคลที่จะเข้ารับการประเมินผลงานเพื่อแต่งตั้งให้ดำรงตำแหน่งในระดับที่สูงขึ้น (ตำแหน่งระดับควบ) จำนวน ๒ ราย ดังรายละเอียดแนบท้ายประกาศนี้ โดยผู้ผ่านการประเมินบุคคลเพื่อเลื่อนขึ้นแต่งตั้งให้ดำรงตำแหน่งในระดับที่สูงขึ้น จะต้องจัดส่งผลงานประเมินตามจำนวนและเงื่อนไขที่คณะกรรมการประเมินผลงานกำหนด ภายใน ๖ เดือน นับแต่วันที่ประกาศรายชื่อผู้ผ่านการประเมินบุคคล หากพ้นระยะเวลาดังกล่าวแล้วผู้ผ่านการประเมินบุคคลยังไม่ส่งผลงาน จะต้องขอรับประเมินบุคคลใหม่ เว้นแต่กรณีผู้ผ่านการประเมินบุคคลจะเกษียณอายุราชการในปีงบประมาณใด ให้ส่งผลงานเข้ารับการประเมินล่วงหน้าไม่น้อยกว่า ๖ เดือน ในปีงบประมาณนั้น

ทั้งนี้ หากมีผู้ใดจะทักท้วงให้ทักท้วงได้ ภายใน ๓๐ วัน นับตั้งแต่วันประกาศรายชื่อผู้ผ่านการประเมินบุคคล การทักท้วงหากตรวจสอบแล้วมีหลักฐานว่า ข้อทักท้วงเป็นการกลั่นแกล้งหรือไม่สุจริตให้ดำเนินการสอบสวนผู้ทักท้วง เพื่อหาข้อเท็จจริงและดำเนินการตามที่เห็นสมควรต่อไป

ประกาศ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๖

(นายจุมภฏ พรมสิตา)
รองอธิบดีกรมสุขภาพจิต
ปฏิบัติราชการแทนอธิบดีกรมสุขภาพจิต

บัญชีรายละเอียดแนบท้ายประกาศกรมสุขภาพจิต ลงวันที่ ๒๔ พฤษภาคม ๒๕๖๖
เรื่อง รายชื่อผู้ผ่านการประเมินบุคคลเพื่อเลื่อนขึ้นแต่งตั้งให้ดำรงตำแหน่งประเภทวิชาการ ระดับชำนาญการ
ครั้งที่ ๔๘ /๒๕๖๖

ลำดับที่	ผู้ผ่านการประเมินบุคคล/หน่วยงาน	ตำแหน่งที่เข้ารับการประเมินผลงาน/หน่วยงาน	ชื่อผลงานที่เสนอขอประเมิน	ชื่อข้อเสนอแนวคิดเพื่อพัฒนางาน
๑.	นางสาวขวัญหทัย บุญทิพย์ เภสัชกรปฏิบัติการ ตำแหน่งเลขที่ ๓๘๕๓ กลุ่มงานเภสัชกรรม กลุ่มภารกิจบริการจิตเวชและสุขภาพจิต สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ กรมสุขภาพจิต	เภสัชกรชำนาญการ (ด้านเภสัชกรรมคลินิก) ตำแหน่งเลขที่ ๓๘๕๓ กลุ่มงานเภสัชกรรม กลุ่มภารกิจบริการจิตเวชและสุขภาพจิต สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ กรมสุขภาพจิต	การพัฒนาระบบการจัดส่งยาเดิมทางไปรษณีย์ เพื่อลดความแออัดในสถานการณ์การแพร่ระบาดของ COVID – ๑๙ ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ จังหวัดสุราษฎร์ธานี	การประเมินผลกระทบของนโยบายควบคุมค่าใช้จ่ายด้านยา ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้
๒.	นายมณฑล บัวแก้ว นักวิชาการคอมพิวเตอร์ปฏิบัติการ ตำแหน่งเลขที่ ๑๐๔ กลุ่มงานพัฒนาข้อมูลและสารสนเทศ กองยุทธศาสตร์และแผนงาน ปฏิบัติราชการที่สำนักเทคโนโลยีสารสนเทศ กรมสุขภาพจิต	นักวิชาการคอมพิวเตอร์ชำนาญการ ตำแหน่งเลขที่ ๑๐๔ กลุ่มงานพัฒนาข้อมูลและสารสนเทศ กองยุทธศาสตร์และแผนงาน ปฏิบัติราชการที่สำนักเทคโนโลยีสารสนเทศ กรมสุขภาพจิต	การพัฒนาระบบคอมพิวเตอร์ระบบเครือข่าย และระบบสารสนเทศ ณ ศูนย์ข้อมูล (Data Center) สู่มาตรฐาน ISO/IEC 27001:2013	ยกระดับการพัฒนาระบบคอมพิวเตอร์ระบบเครือข่าย และระบบสารสนเทศ ณ ศูนย์ข้อมูล (Data Center) สู่มาตรฐาน ISO/IEC 27001:2022

ส่วนที่ 3 แบบการเสนอผลงาน

(ผลงานที่เป็นผลการปฏิบัติงานหรือผลสำเร็จของงาน/ผลงานที่ผ่านมาไม่เกิน 5 หน้ากระดาษ A4)

ชื่อผู้สมัครเข้ารับการประเมินบุคคล นายมณฑล บัวแก้ว

◆ **ตำแหน่งที่ขอเข้ารับการประเมินบุคคล** นักวิชาการคอมพิวเตอร์ **ระดับ** ชำนาญการ

ด้าน (ถ้ามี).....ตำแหน่งเลขที่ 104 **กลุ่มงาน** พัฒนาข้อมูลและสารสนเทศ

กลุ่มภารกิจ .....หน่วยงาน กองยุทธศาสตร์และแผนงาน

กรมสุขภาพจิต

---

1) ชื่อผลงานเรื่อง การพัฒนาระบบคอมพิวเตอร์ ระบบเครือข่าย และ ระบบสารสนเทศ ณ ศูนย์ข้อมูล (Data Center) สู่มาตรฐาน ISO/IEC 27001:2013

2) ระยะเวลาที่ดำเนินการ 1 ตุลาคม 2563 – 30 กันยายน 2566

3) ความรู้ ความชำนาญงาน หรือความเชี่ยวชาญและประสบการณ์ที่ใช้ในการปฏิบัติงาน

- วงจร PDCA (Plan-Do-Check-Act หรือ วางแผน-ปฏิบัติ-ตรวจสอบ-ปรับปรุง)
- ISO/IEC 27001:2013 Awareness and Requirements
- ISO 9001:2015 Internal Auditor based on ISO 19011
- [illegible] Cyber
-

4) สรุปสาระสำคัญขั้นตอนการดำเนินการและเป้าหมายของงาน

การดำเนินการมีวัตถุประสงค์เพื่อพัฒนาคุณภาพระบบคอมพิวเตอร์ ระบบเครือข่าย และ ระบบสารสนเทศ ณ ศูนย์ข้อมูล (Data Center) ให้ผ่านเกณฑ์มาตรฐาน ISO/IEC 27001:2013 โดยใช้หลักจัดการความปลอดภัยของข้อมูล 3 ด้าน ได้แก่ CIA 1) ความลับ (C: Confidentiality) 2) ความถูกต้องสมบูรณ์ (I: Integrity) 3) ความพร้อมใช้ (A: Availability) ครอบคลุมทั้งคน กระบวนงาน และเทคโนโลยีที่เกี่ยวข้องทั้งระบบ โดยจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems: ISMS) ที่มีข้อกำหนดหลัก 14 ข้อ มีรายการควบคุมความเสี่ยง 35 รายการ (Annex A) และ มีรายการตรวจสอบเพื่อทวนสอบความสอดคล้องกับข้อกำหนด 114 ข้อ ใช้วิธีการบริหารจัดการตามวงจรการบริหารงานคุณภาพ (PDCA) โดยมีขั้นตอนดังนี้

1. แต่งตั้งคณะทำงานฯ
2. อบรมให้ความรู้และสร้างความตระหนักรู้เกี่ยวกับ ISO/IEC 27001:2013
3. จัดทำรายการทรัพย์สินสารสนเทศ ครอบคลุม กระบวนงาน เทคโนโลยี
4. ประเมินและวิเคราะห์ความเสี่ยงตามหลัก CIA เพื่อหาจุดอ่อน ช่องโหว่ และสาเหตุของการเกิดปัญหา
5. จัดทำแผนจัดการความเสี่ยง (Related Risk Treatment Plan)
6. ตรวจสอบรายการความเสี่ยงเพื่อทวนสอบความสอดคล้องกับข้อกำหนด 114 ข้อ
7. กำหนดมาตรการควบคุมความเสี่ยงที่จะนำมาใช้ในองค์กรจาก Annex A แล้วจัดทำเป็นเอกสาร

Statement of Applicability (SOA) สำหรับการจัดทำมาตรการควบคุมความเสี่ยง ISMS

8. จัดทำเอกสารมาตรฐาน นโยบาย โครงสร้าง หน้าที่คณะทำงาน คู่มือ ระบบ ISMS และ แนวปฏิบัติ พร้อมทั้งกำหนดตัวชี้วัดความสำเร็จ

9. ประกาศ นโยบาย คำสั่ง มอบหมายภารกิจการปฏิบัติตามมาตรการควบคุมความเสี่ยง ISMS

10. ติดตามการปฏิบัติ และ ซักซ้อมแผนความต่อเนื่อง Business Continuity Plan: BCP

11. อบรม Internal Audit Training (bases on ISO 19011)

12. ประเมิน Internal Audit เพื่อวัดผลและเตรียมความพร้อมสู่การขอรับรองมาตรฐานฯ

13. ประชุมทบทวนระบบ ISO27001 (ISMS Management Review)

14. ตรวจประเมินเบื้องต้น และซักซ้อมการขอรับรองมาตรฐาน (Pre audit)

15. ดำเนินการขอรับรองมาตรฐาน ISO/IEC 27001:2013

5) ผลสำเร็จของงาน(เชิงปริมาณ/คุณภาพ)

- มีมาตรฐานการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ณ ศูนย์ข้อมูล (data center) กรมสุขภาพจิต ตามมาตรฐานสากล ISO/IEC 27001:2013
- ได้รับรองมาตรฐานการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013

6) การนำไปใช้ประโยชน์/ผลกระทบ

- มีระบบการบริหารจัดการความเสี่ยง บริหารจัดการบุคลากร กระบวนการ สามารถช่วยให้การบริการด้านเทคโนโลยีดิจิทัลมีความต่อเนื่อง ปลอดภัย ตามมาตรฐานสากล
- มีการปรับปรุงระบบคอมพิวเตอร์ ระบบเครือข่าย และ ระบบสารสนเทศอย่างต่อเนื่อง เพื่อปกป้องสินทรัพย์สารสนเทศ และ อุดช่องโหว่จากภัยคุกคามทางไซเบอร์ตามกฎหมายกำหนด
- สร้างความมั่นใจได้ว่าข้อมูลที่เป็นความลับมีการควบคุมดูแลอย่างเหมาะสม ป้องกันข้อมูลรั่วไหล และคงความถูกต้องสมบูรณ์ของข้อมูลครบถ้วนตามกฎหมายกำหนด
- เพิ่มความเชื่อมั่นให้กับประชาชนผู้ใช้บริการกับกรมสุขภาพจิต เนื่องจากมีการบริหารจัดการข้อมูลสารสนเทศให้มั่นคงปลอดภัยตามมาตรฐานที่ทั่วโลกให้การยอมรับ
- สร้างภาพลักษณ์ความน่าเชื่อถือในการเป็นหน่วยงานหลักดูแลข้อมูลด้านสุขภาพจิตของประเทศ

7) ความยุ่งยากและซับซ้อนในการดำเนินการ

จากการประเมินความเสี่ยงตามหลัก CIA พบว่า ศูนย์ข้อมูล (Data Center) ไม่เป็นไปตามมาตรฐาน ที่ต้องได้รับการควบคุมความเสี่ยงโดยจัดทำแผนจัดการความเสี่ยง ดังนี้ 1) โครงสร้างเชิงกายภาพของศูนย์ข้อมูล (Data Center) ไม่เป็นไปตามมาตรฐาน เช่น ตำแหน่งเครื่องคอมพิวเตอร์แม่ข่ายติดตั้งอยู่ใต้เครื่องปรับอากาศ อาจทำให้น้ำหยดเกิดความเสียหาย อุณหภูมิและความชื้นในห้องศูนย์ข้อมูลไม่อยู่ในเกณฑ์ที่กำหนด กล้องวงจรปิดไม่มีระบบการเข้ารหัส และไม่มีการสำรองข้อมูล 2) ความเสี่ยงด้านความปลอดภัย (Security) พบว่า ไม่มีการกำหนดสิทธิในการเข้าถึงข้อมูลแต่ละระบบ พบช่องโหว่จากการพัฒนาโปรแกรมและเว็บไซต์ มีการถูกโจมตีหรือมีผู้บุกรุกภายนอกและภายในเข้ามาทำการเจาะระบบ หรือระบบถูกโจมตีด้วยไวรัสคอมพิวเตอร์ อุปกรณ์ Firewall ไม่ได้รับการปรับปรุงให้เป็นปัจจุบัน รายละเอียดของการสำรองข้อมูลยังไม่ชัดเจน 3) ความเสี่ยงด้านบุคคล พบว่ามีการรู้เท่าไม่ถึงการณ์ของผู้ใช้งานระบบเครือข่าย

8) ปัญหาและอุปสรรคในการดำเนินการ

- การประเมินความเสี่ยง (Risk Assessment) ที่ไม่ครบถ้วนและไม่ครอบคลุม ทำให้กระบวนการในการบริหารจัดการความเสี่ยงเกิดช่องโหว่ขึ้นซึ่งอาจก่อให้เกิดความเสียหายและกระทบต่อการดำเนินงานได้ การประเมินความเสี่ยงให้ถูกต้องอาจต้องอาศัยคำแนะนำและความช่วยเหลือจากผู้เชี่ยวชาญ
- จำนวนบุคลากรด้านเทคโนโลยีสารสนเทศไม่เพียงพอในการดำเนินการ

9) ข้อเสนอแนะ

- ควรมีการกำหนด นำสู่การปฏิบัติ บำรุงรักษา และปรับปรุงอย่างต่อเนื่องสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- เตรียมพร้อมเพื่อปรับสู่มาตรฐาน ISO/IEC 27001:2022 Information Security, Cyber Security and Privacy Protection
- ยกระดับการบริหารจัดการข้อมูลส่วนบุคคล ตามมาตรฐาน ISO/IEC 27701 (Privacy Information Management System: PIMS) ให้สามารถบริหารจัดการข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัย และนำไปประยุกต์ใช้เพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

10) การเผยแพร่(ถ้ามี)

☑ผลงานแล้วเสร็จและเผยแพร่แล้ว ระบุแหล่งเผยแพร่ https://ict.dmh.go.th/mainiso/main/

☐ผลงานแล้วเสร็จแต่ยังไม่ได้เผยแพร่

☐ผลงานยังไม่แล้วเสร็จ

11) การรับรองสัดส่วนของผลงาน ในส่วนที่ตนเองปฏิบัติและผู้มีส่วนร่วมในผลงาน

ผู้สมัครเข้ารับการประเมินบุคคลมีส่วนร่วมในผลงานที่ขอรับการประเมิน ร้อยละ 80 และมีผู้มีส่วนร่วมในผลงาน ดังนี้

รายชื่อผู้มีส่วนร่วมในผลงาน	สัดส่วนมีส่วนร่วมในผลงาน	ลายมือชื่อ
นางอมรรัตน์ ทวีกุล	20	

ส่วนที่ 4 แบบเสนอข้อเสนอแนวคิดในการปรับปรุงหรือพัฒนางาน

(ข้อเสนอแนวคิดในการปรับปรุงหรือพัฒนางานไม่เกิน 3 หน้ากระดาษ A4)

ชื่อผู้สมัครเข้ารับการประเมินบุคคล นายมณฑล บัวแก้ว

- **ตำแหน่งที่ขอเข้ารับการประเมินบุคคล** นักวิชาการคอมพิวเตอร์ **ระดับ** ชำนาญการ

ด้าน (ถ้ามี).....ตำแหน่งเลขที่ 104 **กลุ่มงาน** พัฒนาข้อมูลและสารสนเทศ

กลุ่มภารกิจ .....หน่วยงาน กองยุทธศาสตร์และแผนงาน

กรมสุขภาพจิต

---

1) ชื่อผลงานเรื่อง ยกระดับการพัฒนาระบบคอมพิวเตอร์ ระบบเครือข่าย และ ระบบสารสนเทศ ณ ศูนย์ข้อมูล (Data Center) สู่มาตรฐาน ISO/IEC 27001:2022

2) หลักการและเหตุผล

ปัจจุบันภัยคุกคามทางไซเบอร์ได้แพร่กระจายอย่างรวดเร็วไม่ต่างจากไวรัส สร้างผลกระทบร้ายแรงตั้งแต่ระดับองค์กรไปจนถึงระดับบุคคล โดยอาศัยช่องโหว่เพื่อโจรกรรมข้อมูลส่วนบุคคล หรือ Cyber Attack โดยอาชญากรไซเบอร์ (Hacker) ทำให้ข้อมูลสำคัญขององค์กรได้รับความเสียหาย การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ และการตั้งรับ เฝ้าระวัง เตรียมความพร้อมที่มีมาตรฐานตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์กำหนด สามารถปิดช่องทางความเสี่ยงและปกป้ององค์กรจากภัยคุกคามทางไซเบอร์ได้ ประกอบกับนโยบายการขับเคลื่อนระบบสุขภาพจิตด้วยระบบดิจิทัล เพื่อให้เกิดการบูรณาการเชื่อมโยงแลกเปลี่ยนข้อมูล และการให้บริการดิจิทัลได้อย่างต่อเนื่องปลอดภัย กรมสุขภาพจิตดำเนินการพัฒนาระบบคอมพิวเตอร์ ระบบเครือข่าย และ ระบบสารสนเทศ ณ ศูนย์ข้อมูล (Data Center) สู่มาตรฐาน ISO/IEC 27001:2013 ตั้งแต่ปีงบประมาณ พ.ศ. 2564 เป็นต้นมา ประกอบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และมีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 ซึ่งเป็นกฎหมายว่าด้วยการให้สิทธิกับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต เพื่อความต่อเนื่องในการดำเนินการตามมาตรฐานระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System: ISMS) และต้องการขยายขอบเขตของระบบเดิมให้ครอบคลุมการคุ้มครองข้อมูลส่วนบุคคล การเลือกใช้ ISO/IEC 27001:2022 จะเป็นตัวเลือกที่น่าสนใจ เพราะเป็นการขยายกระบวนการ และมาตรการของ ISO 27001 ที่มีอยู่เดิม สามารถจัดการกับความเสี่ยงด้านความปลอดภัยที่ซับซ้อนมากขึ้น มุ่งเน้นการป้องกัน ตรวจจับ และตอบสนองต่อการโจมตีทางไซเบอร์ (cyberattack) ควบคู่ไปกับการการปกป้องข้อมูล (ตามกรอบการทำงานของ NIST Cybersecurity)

3) บทวิเคราะห์/แนวความคิด/ข้อเสนอ และข้อจำกัดที่อาจเกิดขึ้นและแนวทางแก้ไข

มาตรฐาน ISO/IEC 27001:2013 เป็นมาตรฐานด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และมาตรการควบคุมในมาตรฐานฉบับนี้ถือว่าเป็นชุดมาตรการควบคุมที่ได้รับการยอมรับ และถูกนำไปปรับใช้อย่าง

แพร่หลาย ปกติแล้วมาตรฐานจะมีการปรับปรุงทุก ๆ 8-10 ปี ทาง ISO (International Organization for Standard) ได้ประกาศใช้มาตรฐานใหม่ เมื่อวันที่ 25 ตุลาคม 2565 จากเดิม ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements เป็น ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems Requirements การปรับเปลี่ยนครั้งนี้ เพื่อให้ตัวมาตรฐานมีความทันสมัย ลดทอนข้อกำหนดที่มีความซับซ้อน และให้ความสำคัญมากขึ้นกับ Cybersecurity และ Privacy Protection ตามชื่อมาตรฐานที่มีการปรับเปลี่ยน เพื่อช่วยให้องค์กรสามารถจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียและธุรกิจได้ดียิ่งขึ้น โดยมีระยะเวลาในการปรับเปลี่ยน (Transition Period) 3 ปี หรือ 36 เดือน นับจากวันสุดท้ายของเดือนที่มีการประกาศมาตรฐานฉบับใหม่ หรือ ภายใน 31 ตุลาคม 2568

กรมสุขภาพจิตดำเนินการพัฒนาระบบคอมพิวเตอร์ ระบบเครือข่าย และ ระบบสารสนเทศ ณ ศูนย์ข้อมูล (Data Center) สู่มาตรฐาน ISO/IEC 27001:2013 ในปีงบประมาณ พ.ศ. 2564 และได้รับการตรวจประเมินเพื่อต่ออายุการรับรอง (Recertification Audit) ครบ 3 ปี ในปีงบประมาณ พ.ศ.2566 ดังนั้นเพื่อความต่อเนื่องในการดำเนินการตามมาตรฐานระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ สามารถจัดการกับความเสี่ยงด้านความปลอดภัยที่ซับซ้อนมากขึ้น จึงควรดำเนินการพัฒนาระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ณ ศูนย์ข้อมูล (Data Center) สู่มาตรฐาน ISO/IEC 27001:2022 ในปีงบประมาณ 2567

การดำเนินการตามมาตรฐานระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ และการรักษาความต่อเนื่องเป็นสิ่งจำเป็นในการปฏิบัติงานในยุคปัจจุบัน แต่เนื่องด้วยข้อจำกัดของจำนวนบุคลากรของสำนักเทคโนโลยีสารสนเทศที่มีไม่เพียงพอและการเปลี่ยนแปลงผู้รับผิดชอบในแต่ละด้านอาจส่งผลกระทบต่อการดำเนินการ ดังนั้นการสร้างความรู้ ความเข้าใจ และความตระหนักให้แก่บุคลากรที่ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศถือเป็นเรื่องสำคัญ ผู้บริหารเป็นผู้มีความสำคัญในการสนับสนุน และกระตุ้นให้บุคลากรมีความเข้าใจในนโยบาย ตลอดจนนำไปปฏิบัติให้เกิดความชินในการปฏิบัติงาน และมีความตระหนักในด้านความมั่นคงปลอดภัยสารสนเทศมากขึ้น

4) ผลที่คาดว่าจะได้รับ

- มีความต่อเนื่องในการดำเนินการตามมาตรฐานระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ
- สามารถจัดการกับความเสี่ยงด้านความปลอดภัยที่ซับซ้อนมากขึ้น จากมาตรฐาน ISO/IEC 27001:2022 ที่มุ่งเน้นการป้องกัน ตรวจจับ และตอบสนองต่อการโจมตีทางไซเบอร์ (cyberattack) ควบคู่ไปกับการการปกป้องข้อมูล (ตามกรอบการทำงานของ NIST Cybersecurity)

5) ตัวชี้วัดความสำเร็จ

- มีมาตรฐานการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ณ ศูนย์ข้อมูล (Data Center) กรมสุขภาพจิต ตามมาตรฐานสากล ISO/IEC 27001:2022
- ได้รับรองมาตรฐานการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022