**แผนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของสำนักงานสถิติแห่งชาติ ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รับผิดชอบหลัก**

| ชื่อแผน | ผู้รับผิดชอบ | ฉบับที่ใช้ | ความถี่การปรับปรุง(ปี) | ระเบียบ/ข้อบังคับ/ปัจจุบัน | ผู้ได้รับผลกระทบ |
| --- | --- | --- | --- | --- | --- |
| 1. แผนปฏิบัติการดิจิทัล สสช. ระยะ 5 ปี (พ.ศ. 2566-2570) | ศท. กวจ. ร่าง/  คกก.ไอที พิจารณา | 2566-2570 | 5 | เป็นแผนปฏิบัติการด้านเทคโนโลยีดิจิทัล ของสำนักงานสถิติแห่งชาติ | ทุก ศูนย์/กอง/สำนัก/สำนักงานสถิติจังหวัด |
| 2. ประกาศสำนักงานสถิติแห่งชาติ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานสถิติแห่งชาติ พ.ศ. 2562 และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562  ตามมาตรา 7 ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 | กวจ. ร่าง /  คทง.  (ฝ่ายเลขาฯ : กพค.) พิจารณา | 2562 | 2 | ประกาศสำนักงานสถิติแห่งชาติ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานสถิติแห่งชาติ พ.ศ. 2562 (ข้อ 3 ให้มีหมวดของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จำนวน 11 หมวด และให้มีการปรับปรุงให้สอดคล้องกับภารกิจและเป็นปัจจุบันอยู่เสมอใน ทุก 2 ปี) และ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562 (หมวดที่ 1 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ แนวปฏิบัติ ข้อ 3. ข้อย่อย 1) (1) ให้จัดทำ ทบทวน ปรับปรุง นโยบาย แนวตามข้อกำหนดในนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศ 11 หมวด และสถาปัตยกรรมระบบความมั่นคงปลอดภัยอย่างสม่ำเสมอทุก 2 ปี เพื่อให้สอดคล้องกับความต้องการของกระบวนการสถิติ สภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงและข้อบังคับ) | ทุก ศูนย์/กอง/สำนัก/สำนักงานสถิติจังหวัด |
| 3. แผนไอทีในสถานการณ์ความไม่แน่นอนจากภัยพิบัติ (IT Contingency Plan) พ.ศ. 2553-2555 | กพค. | 2553-2555 | 1 | แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562 (หมวดที่ 9 การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง แนวปฏิบัติ ข้อ 1. ข้อย่อย 10) ให้มีการทดสอบและปรับปรุงแผนต่อเนื่องปีละ 1 ครั้ง เพื่อให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่ | ศท.  (ห้ามเปิดเผยต่อบุคคลภายนอก) |
| 4. แผนการสำรองและกู้คืนข้อมูล (Backup and Recovery Plan) เวอร์ชั่น 2 เมษายน 2560 | กพค. | 2560 | 1 | แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562 (หมวดที่ 9 การบริหารจัดการด้านการบริการเพื่อให้มีความต่อเนื่อง แนวปฏิบัติ ข้อย่อย 3.2) ให้ทดสอบการกู้คืนข้อมูลที่สำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูลรวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้ ตลอดจนขั้นตอนและวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน | ทุก ศูนย์/กอง/สำนัก/สำนักงานสถิติจังหวัด |
| 5. คู่มือการตรวจสอบระบบสนับสนุนศูนย์ดาต้าเซ็นเตอร์ สำนักงานสถิติแห่งชาติ เวอร์ชั่น 2.0 กรกฎาคม 2560 | กพค. | 2560 |  | แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562 (หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม แนวปฏิบัติ ข้อย่อย 1.1), 2), 3), 4), 5), 6) ให้ตรวจสอบและเฝ้าระวังศูนย์คอมพิวเตอร์ หรือ ห้องคอมพิวเตอร์ | ศท. |
| 6. รายงานตรวจสอบไวรัส (Virus detected โดยโปรแกรม Sophos Central Intercept X Advanced ) ประจำเดือน....... แสดงบน(http://webintranet.nso.go.th/?q=สำนัก/ศท./ศท.กพค. | กพค. | 2565 | รายเดือน | แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562 (หมวดที่ 6 การบริหารจัดการด้านสื่อสารและการดำเนินงานของระบบงานคอมพิวเตอร์ แนวปฏิบัติ ข้อ 4. ข้อย่อย 3) (4) รายงานการติดไวรัสคอมพิวเตอร์ของเครื่องคอมพิวเตอร์ลูกข่ายพร้อมทั้งรายละเอียดของไวรัสคอมพิวเตอร์ที่แพร่กระจายในองค์กร | ทุก ศูนย์/กอง/สำนัก/สำนักงานสถิติจังหวัด |
| 7. ระเบียบสำนักงานสถิติแห่งชาติว่าด้วยการใช้งานทรัพย์สินสารสนเทศ พ.ศ. 2555  คุณ ศศิธร แจ้งว่า กพค. ไม่ได้ดำเนินการ เป็นคณะทำงานทบทวนนโยบายความมั่นคงฯ | กพค. | 2555 |  | ระเบียบสำนักงานสถิติแห่งชาติว่าด้วยการใช้งานทรัพย์สินสารสนเทศ พ.ศ. 2555 | ทุก ศูนย์/กอง/สำนัก/สำนักงานสถิติจังหวัด |
| 8. ประกาศสำนักงานสถิติแห่งชาติ เรื่องนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2564 | กวจ. ร่าง/  คทง.  (ฝ่ายเลขาฯ : กวจ.) | 2564 | 2 | ประกาศสำนักงานสถิติแห่งชาติ เรื่องนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2564 | ทุก ศูนย์/กอง/สำนัก/สำนักงานสถิติจังหวัด |
| 9.ประกาศสำนักงานสถิติแห่งชาติ เรื่องนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)  สำนักงานสถิติแห่งชาติ พ.ศ. 2565 | กวจ. ร่าง/  คทง.  (ฝ่ายเลขาฯ : กวจ.) พิจารณา | 2565 | เมื่อมีการเปลี่ยนแปลง | ประกาศสำนักงานสถิติแห่งชาติ เรื่องนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) สำนักงานสถิติแห่งชาติ พ.ศ. 2565 |  |
| 10. การบริหารความเสี่ยงด้านสารสนเทศ สำนักงานสถิติแห่งชาติ พ.ศ. 2560 | กพค. | 2561 |  | แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562 (หมวดที่ 1 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ แนวปฏิบัติ ข้อ 3. ข้อย่อย 3) (1) ให้ประเมินความเสี่ยงและจัดการกับความเสี่ยงอาจเกิดกับทรัพย์สินสารสนเทศที่สำคัญเป็นประจำอย่างสม่ำเสมอ โดยมีขั้นตอน การระบุปัจจัยที่มีผลทำให้เกิดความเสี่ยง และระบุความเสี่ยงที่มีโอกาสเกิดขึ้น (Risk Analysis) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการบริหารจัดการความเสี่ยง (Risk Management) | ทุก ศูนย์/กอง/สำนัก/สำนักงานสถิติจังหวัด |
| 11. เอกสารกำหนดสิทธิ์ (บัญชีรายชื่อผู้ใช้งานระบบสารสนเทศและจดหมายอิเล็กทรอนิกส์ พ.ศ. 2560 | กพค. | 2565 | 1 | แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562 (หมวดที่ 4 การสร้างความมั่นคงปลอดภัยด้านบุคลากร แนวปฏิบัติ ข้อ 6 ให้มีการทบทวนสิทธิของผู้ใช้ระบบสารสนเทศเป็นประจำทุกปี) | ทุก ศูนย์/กอง/สำนัก/สำนักงานสถิติจังหวัด |
| 12. แผนภาพระบบเครือข่าย สำนักงานสถิติแห่งชาติ | กพค. | 2565 | 2 | แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562 (หมวดที่ 1 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ แนวปฏิบัติ ข้อ 3. ข้อย่อย 1) (1) ให้จัดทำ ทบทวน ปรับปรุง นโยบาย แนวตามข้อกำหนดในนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศ 11 หมวด และสถาปัตยกรรมระบบความมั่นคงปลอดภัยอย่างสม่ำเสมอทุก 2 ปี เพื่อให้สอดคล้องกับความต้องการของกระบวนการสถิติ สภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงและข้อบังคับ) | ศท. |
| 13. แนวทางการทำลายข้อมูลและสื่ออิเล็กทรอนิกส์ รุ่น 1.0 (Data Sanitization) | กพค. | 2562 | เมื่อมีการเปลี่ยนแปลง |  |  |
| 14. แผนปฏิบัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ | กพค.ร่าง / คทง. |  |  |  |  |
| 15. (สพร.) ระดับความพร้อมในตัวชี้วัดย่อยด้าน Cyber Security และข้อเสนอแนะดังนี้  - ด้าน Cyber Security Standard & Procedure ได้คะแนนอยู่ในระดับ 1  ข้อเสนอแนะด้าน Cyber Security Standard & Procedure  หน่วยงานควรดำเนินการตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ทั้ง 5 กรอบมาตรฐาน ดังนี้  1. มีการระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)  2. มีมาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)  3. มีมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)  4. มีมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)  5. มีมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) | ศท. กพค.  คทง. |  |  |  |  |

หมายเหตุ

1. (มี.ค. 64) กพค. ศท. (คุณ ศศิธร มากธันญา) ให้ข้อมูลว่า การปรับปรุงแผนต่างๆ จะทำการปรับปรุงเมื่อมีการทบทวนเรื่องความมั่นคง ฯ เท่านั้น

โดย กลุ่มวิจัยและพัฒนา ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ปรับปรุง วันที่ 12 มีนาคม 2564

2. กวจ. ศท. ส่งการประเมินตนเองของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ สพธอ. พิจารณาเบื้องต้น ทางอีเมล และ สพธอ. ได้แจ้งกลับมาทางอีเมล เมื่อ 29 พ.ย. 65 ขณะนี้ กวจ. ศท. อยู่ระหว่างดำเนินการ