**แบบ ปม.**

**ชื่อหน่วยงาน กรมอู่ทหารเรือ**

**แบบประเมินการควบคุมภายใน**

สำหรับงวดตั้งแต่ วันที่ ๑ เดือน ต.ค. พ.ศ. ๕๘ ถึงวันที่ ๓๐ เดือน ก.ย. พ.ศ. ๕๙

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| วัตถุประสงค์ของการควบคุม  (กระบวนการปฏิบัติงานโครงการ/กิจกรรม/ด้านของงานที่ประเมิน)  (๑) | ความเสี่ยงที่ยังมีอยู่และสาเหตุ  (๒) | วัตถุประสงค์ของการควบคุม (ด้าน)  (๓) | ระดับความเสี่ยง(พิจารณาโอกาสและผลกระทบ)  (๔) | การควบคุม  ที่มีอยู่  (๕) | การประเมินผล  การควบคุม  (๖) | จุดอ่อนและสาเหตุ  (๗) | การปรับปรุงการควบคุม  (๘) |
| **ด้านระบบเทคโนโลยีสารสนเทศ ในการบริหารจัดการ**  **๑. โครงสรางทางดานความมั่นคงปลอดภัยสําหรับองคกร**  มีจุดประสงคเพื่อบริหารและจัดการความมั่นคงปลอดภัยสําหรับสารสนเทศขององคกร  **๒. ความมั่นคงปลอดภัยที่เกี่ยวของกับบุคลากร (Human resources security)**  **๒.๑ การสิ้นสุดหรือการเปลี่ยน การจางงาน (Termination or change of employment)**  มีจุดประสงคเพื่อใหพนักงาน ผูที่องคกรทําสัญญาวาจาง และ หนวยงานภายนอกไดทราบถึงหนา ที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจางงานหรือมีการเปลี่ยนการจางงาน | - ยังไม่ได้ดำเนินการปฏิบัติในการลงนาม มิให้เปิดเผยความลับองค์กร  - ยังขาดกฎเกณฑ์และระเบียบปฏิบัติในการถอนสิทธิการเข้าถึงสารสนเทศ สำหรับผู้พ้นหน้าที่ | O,C  O,C | ปานกลาง  ปานกลาง | - การลงนามมิใหเปิดเผยความลับขององคกร  - การถอดถอนสิทธิในการเข้าถึงสารสนเทศในองค์กร | - ยังไม่มีการประเมิน  - มีการตรวจสอบบุคลากรประจำปี เพื่อปรับปรุงสิทธิในการเข้าถึง | - ยังไม่มีการนำระเบียบต่าง ๆ มาดำเนินการอย่างเป็นรูปธรรม  - ยังไม่ได้ปฏิบัติตามระเบียบอย่างเป็นรูปธรรม | - ประชุมผู้ที่เกี่ยวข้องเพื่อกำหนดรายละเอียดและหลักปฏิบัติในการลงนามมิให้เปิดเผยความลับ  - ประชุมผู้ที่เกี่ยวข้องเพื่อกำหนดรายละเอียดระเบียบปฏิบัติในการถอนสิทธิการเข้าถึงสารสนเทศ สำหรับผู้พ้นหน้าที่ |

- ๒ -

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| วัตถุประสงค์ของการควบคุม  (กระบวนการปฏิบัติงานโครงการ/กิจกรรม/ด้านของงานที่ประเมิน)  (๑) | ความเสี่ยงที่ยังมีอยู่และสาเหตุ  (๒) | วัตถุประสงค์ของการควบคุม (ด้าน)  (๓) | ระดับความเสี่ยง(พิจารณาโอกาสและผลกระทบ)  (๔) | การควบคุม  ที่มีอยู่  (๕) | การประเมินผล  การควบคุม  (๖) | จุดอ่อนและสาเหตุ  (๗) | การปรับปรุงการควบคุม  (๘) |
| **๓. การบริหารจัดการเครื่อง แม่ข่ายและการดำเนินงานของเครือข่ายสารสนเทศ (Server and Network operation management)**  **๓.๑ การจัดการสื่อที่ใชในการบันทึกขอมูล (Media handling**)  มีจุดประสงคเพื่อปองกันการเปดเผย การเปลี่ยนแปลงแกไข การลบหรือการทําลายทรัพยสินสารสนเทศโดยไมไดรับอนุญาตและการติดขัดหรือหยุดชะงักต่อการปฏิบัติงาน  **๓.๒ การเฝาระวังทางดาน**  **ความมั่นคงปลอดภัย (Monitoring)**  มีจุดประสงคเพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไมไดรับอนุญาต | - ยังไม่มีมาตรการสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบอย่างเป็นรูปธรรม  - การตรวจสอบการใช้งานระบบยังไม่ครบถ้วนทุกระบบ  - ยังไม่มีมาตรการในการป้องกันข้อมูลบันทึกเหตุการณ์  - การบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ยังไม่ครบถ้วนทุกระบบ  - ยังไม่มีการบันทึกเหตุการณ์ข้อผิดพลาด | O  O, F  O, F  O, F  O, F | ต่ำ  ปานกลาง  ปานกลาง  ปานกลาง  ปานกลาง | - การสรางความมั่นคงปลอดภัยสําหรับเอกสารระบบ  - การตรวจสอบการใช้งานระบบ  - การป้องกันข้อมูลบันทึกเหตุการณ์  - บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ  - การบันทึกเหตุการณ์ ข้อผิดพลาด | - มีตู้จัดเก็บเอกสารระบบโดยเฉพาะ  - มี แต่ยังไม่ครบทุกระบบ  - ยังไม่มีการควบคุม  - มี แต่ยังไม่ครบทุกระบบ  - ยังไม่มีการควบคุม | - ยังไม่มีการปฏิบัติตามระเบียบอย่างจริงจัง  - ขาดแคลนกำลังพลในการดำเนินงาน  - ขาดแคลนกำลังพลในการดำเนินงาน  - ขาดแคลนกำลังพลในการดำเนินงาน  - ขาดแคลนกำลังพลในการดำเนินงาน | - ประชุมผู้ที่เกี่ยวข้องเพื่อกำหนดมาตรการสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ  - แจ้งผู้พัฒนาระบบให้ดำเนินการ  - กำหนดมาตรการในการป้องกันข้อมูลบันทึกเหตุการณ์ และแจ้งแก่ผู้พัฒนาระบบ  - แจ้งผู้รับผิดชอบให้ดำเนินการให้ครบถ้วน  - เสนอแนะให้ผู้พัฒนาระบบมีระบบการบันทึกเหตุการณ์ข้อผิดพลาด |

- ๓ -

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| วัตถุประสงค์ของการควบคุม  (กระบวนการปฏิบัติงานโครงการ/กิจกรรม/ด้านของงานที่ประเมิน)  (๑) | ความเสี่ยงที่ยังมีอยู่และสาเหตุ  (๒) | วัตถุประสงค์ของการควบคุม (ด้าน)  (๓) | ระดับความเสี่ยง(พิจารณาโอกาสและผลกระทบ)  (๔) | การควบคุม  ที่มีอยู่  (๕) | การประเมินผล  การควบคุม  (๖) | จุดอ่อนและสาเหตุ  (๗) | การปรับปรุงการควบคุม  (๘) |
| **๔. การควบคุมการเข้าถึงระบบสารสนเทศและฐานข้อมูล (Access control Information system and database)**  **๔.๑ การควบคุมการเขาถึงระบบปฏิบัติการ (Operating system access control)**  มีจุดประสงคเพื่อปองกันการเขา ถึงระบบปฏิบัติการโดยไมไดรับอนุญาต  **๔.๒ การสรางความมั่นคงปลอดภัยสําหรับกระบวนการในการพัฒนาระบบและ กระบวนการสนับสนุน** **(Security in development and support processes)**  มีจุดประสงคเพื่อรักษาความมั่นคงปลอดภัยสําหรับซอฟตแวรและสารสนเทศของระบบ | - ยังมีการกำหนดสิทธิ์บุคคลไม่ครบถ้วนครอบคลุมทุกระบบ ปฏิบัติการ  - ยังไม่ได้กำหนดขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลง หรือแก้ไขระบบ | O  O | ต่ำ  ต่ำ | - ขั้นตอนปฏิบัติในการเขาถึงระบบอยางมั่นคงปลอดภัย    - ขั้นตอนปฏิบัติสําหรับควบคุมการเปลี่ยนแปลงหรือ แกไขระบบ | - มีการกำหนดสิทธิ์บุคคล ในการเข้าถึงระบบ  - ยังไม่มีการควบคุม | - ขาดแคลนกำลังพลในการดำเนินงาน  - ยังไม่มีการดำเนินการตามระเบียบ | - สำรวจและกำหนดสิทธิ์ในการเข้าถึงระบบ ปฏิบัติการให้ครบถ้วน  - ประชุมผู้เกี่ยวข้องเพื่อกำหนดขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยน แปลงหรือแก้ไขระบบ |

- ๔ -

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| วัตถุประสงค์ของการควบคุม  (กระบวนการปฏิบัติงานโครงการ/กิจกรรม/ด้านของงานที่ประเมิน)  (๑) | ความเสี่ยงที่ยังมีอยู่และสาเหตุ  (๒) | วัตถุประสงค์ของการควบคุม (ด้าน)  (๓) | ระดับความเสี่ยง(พิจารณาโอกาสและผลกระทบ)  (๔) | การควบคุม  ที่มีอยู่  (๕) | การประเมินผล  การควบคุม  (๖) | จุดอ่อนและสาเหตุ  (๗) | การปรับปรุงการควบคุม  (๘) |
| **๕. การบริหารจัดการเหตุการณที่เกี่ยวของกับความมั่นคงปลอดภัยขององคกร (Information security incident management)**  **๕.๑ การรายงานเหตุการณและจุดออนที่เกี่ยวของกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)**  มีจุดประสงคเพื่อใหเหตุการณและจุดออนที่เกี่ยวของกับความมั่นคงปลอดภัยตอระบบสารสนเทศ ขององคกรไดรับการดําเนินการที่ถูกตองในชวงระยะเวลาที่เหมาะสม  **๕.๒ การบริหารจัดการและการปรับปรุงแกไขตอเหตุการณที่เกี่ยวของกับความมั่นคงปลอดภัย (Management of information**  **security incidents and improvements)**  มีจุดประสงคเพื่อใหมีวิธีการที่สอดคลองและไดผลในการบริหารจัดการ เหตุการณที่เกี่ยวของกับความมั่นคงปลอดภัยสําหรับสารสนเทศขององคกร | - ยังไม่มีการกำหนดกรอบและรายละเอียดในการรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร  - เจ้าหน้าที่ขาดความรู้ความเข้าใจในการเก็บรวบรวมหลักฐานความมั่นคงปลอดภัยองค์กร | O, F, C  O | ปานกลาง  ต่ำ | - การรายงานจุดออนที่เกี่ยวของกับความมั่นคงปลอดภัยขององคกร    - การเก็บรวบรวมหลักฐาน | - ยังไม่มีการควบคุม  - ยังไม่มีการควบคุม | - ยังไม่มีการปฏิบัติตามระเบียบอย่างจริงจัง  - มีหลักสูตรน้อยมาก | - ประชุมผู้ที่เกี่ยวข้องเพื่อกำหนดกรอบและรายละเอียดในการรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยองค์กร  - ส่งเจ้าหน้าที่ไปอบรมเพิ่มความรู้ในการเก็บหลักฐานด้านความปลอดภัยองค์กร |

- ๕ -

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| วัตถุประสงค์ของการควบคุม  (กระบวนการปฏิบัติงานโครงการ/กิจกรรม/ด้านของงานที่ประเมิน)  (๑) | ความเสี่ยงที่ยังมีอยู่และสาเหตุ  (๒) | วัตถุประสงค์ของการควบคุม (ด้าน)  (๓) | ระดับความเสี่ยง(พิจารณาโอกาสและผลกระทบ)  (๔) | การควบคุม  ที่มีอยู่  (๕) | การประเมินผล  การควบคุม  (๖) | จุดอ่อนและสาเหตุ  (๗) | การปรับปรุงการควบคุม  (๘) |
| **๖. การบริหารความตอเนื่องในการดําเนินงานขององคกร**  **(Activity continuity management)**  **๖.๑ หัวขอพื้นฐานสําหรับการบริหารความตอเนื่องในการดําเนินงานขององคกร (Information security aspects of activity continuity management)**  มีจุดประสงคเพื่อปองกันการติดขัดหรือการหยุดชะงักของกิจกรรมตางๆ อันเปนผลมาจากการลมเหลว หรือหายนะที่มี ตอระบบสารสนเทศ และเพื่อใหสามารถกูระบบกลับคืนมาไดภายในระยะเวลาอันเหมาะสม | - ยังขาดกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติราชการ อย่างเป็นรูปธรรม  - ยังไม่ได้ทำการประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับการปฏิบัติราชการ  - ยังไม่ได้ดำเนินการจัดทำแผนสร้างความต่อเนื่องให้กับการปฏิบัติราชการ  - ยังไม่ได้กำหนดกรอบสําหรับการวางแผนเพื่อสรางความตอเนื่องใหกับการปฏิบัติราชการ | O  O  O  O | ต่ำ  ต่ำ  ต่ำ  ต่ำ | - กระบวนการในการสรางความต่อเนื่องใหกับการปฏิบัติราชการ  - การประเมินความเสี่ยงในการสรางความตอเนื่องใหกับการปฏิบัติราชการ  - การจัดทําและใชงานแผนสรางความต่อเนื่องใหกับการปฏิบัติราชการ  - การกําหนดกรอบสําหรับการวางแผนเพื่อสรางความตอเนื่องใหกับการปฏิบัติราชการ | - มีการสำรองข้อมูลและขั้นตอนการเรียกคืนระบบ  - ยังไม่มีการควบคุม  - ยังไม่มีการควบคุม  - ยังไม่มีการควบคุม | - ความถี่ในการปฏิบัติยังน้อยอยู่  - ขาดแคลนกำลังพลในการดำเนินงาน  - ขาดแคลนกำลังพลในการดำเนินงาน  - ขาดแคลนกำลังพลในการดำเนินงาน | - ประชุมผู้ที่เกี่ยวข้องเพื่อจัดทำกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติราชการ  - ประชุมผู้ที่เกี่ยวข้องเพื่อจัดทำการประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับการปฏิบัติราชการ  - ประชุมผู้ที่เกี่ยวข้องเพื่อจัดทำแผนสร้างความต่อเนื่องให้กับการปฏิบัติราชการ  - ประชุมผู้ที่เกี่ยวข้องเพื่อกำหนดกรอบสําหรับการวางแผนเพื่อสรางความตอเนื่องใหกับการปฏิบัติราชการ |

- ๖ -

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| วัตถุประสงค์ของการควบคุม  (กระบวนการปฏิบัติงานโครงการ/กิจกรรม/ด้านของงานที่ประเมิน)  (๑) | ความเสี่ยงที่ยังมีอยู่และสาเหตุ  (๒) | วัตถุประสงค์ของการควบคุม (ด้าน)  (๓) | ระดับความเสี่ยง(พิจารณาโอกาสและผลกระทบ)  (๔) | การควบคุม  ที่มีอยู่  (๕) | การประเมินผล  การควบคุม  (๖) | จุดอ่อนและสาเหตุ  (๗) | การปรับปรุงการควบคุม  (๘) |
|  | - ยังไม่ได้กำหนดการทดสอบและการปรับปรุงแผนสร้างความตอเนื่องใหกับการปฏิบัติราชการ | O | ต่ำ | - การทดสอบและการปรับปรุงแผนสร้างความตอเนื่องใหกับการปฏิบัติราชการ | - ยังไม่มีการควบคุม | - ขาดแคลนกำลังพลในการดำเนินงาน | - ประชุมผู้ที่เกี่ยวข้องเพื่อกำหนดการทดสอบและการปรับปรุงแผนสร้างความตอเนื่องใหกับการปฏิบัติราชการ |

ชื่อผู้รายงาน น.อ.

ตำแหน่ง จนท.ติดตามประเมินผลฯ ด้านเทคโนโลยีสารสนเทศ

ในการบริหารจัดการ/ ผอ.กจก.อร.

วันที่ ต.ค.๕๙

**หมายเหตุ**

ช่องที่ (๑) ระบุวัตถุประสงค์ของกิจกรรมหรือด้านของงานที่กำลังประเมิน แต่ละขั้นตอนของการปฏิบัติงาน

ช่องที่ (๒) ระบุความเสี่ยงที่มีผลกระทบต่อความสำเร็จตามวัตถุประสงค์ของการควบคุมด้านใดด้านหนึ่งหรือหลายด้าน คือ

ด้านการดำเนินงาน (Operation) ด้านการรายงานทางการเงิน (Financial) และด้านการปฏิบัติตามกฎ ระเบียบ (Compliance)

ช่องที่ (๓) วัตถุประสงค์ของการควบคุม ระบุด้านใดด้านหนึ่งหรือหลายด้าน ด้านการดำเนินงาน (O = Operation) ด้านการรายงานทางการเงิน (F = Financial )

ด้านการปฏิบัติตามกฎ ระเบียบ ข้อบังคับ C = Compliance)

ช่องที่ (๔) ระบุระดับความเสี่ยง โดยพิจารณาโอกาสและผลกระทบ ๔ ระดับ สูงมาก สูง ปานกลาง ต่ำ

ช่องที่ (๕) การควบคุมที่มีอยู่ สรุปขั้นตอน/วิธีปฏิบัติงาน/นโยบาย/กฎเกณฑ์ที่เชื่อว่าจะลดแต่ละความเสี่ยงให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้

ช่องที่ (๖) ประเมินผลแต่ละกิจกรรมช่องที่ (๕) เพียงพอและมีประสิทธิภาพหรือไม่ โดยตอบคำถาม

1. การควบคุมเหมาะสมมีเหตุผลที่จะป้องกันหรือลดความเสี่ยงตามช่องที่ (๒) หรือไม่
2. มีการกำหนด/ส่งอย่างเป็นทางการให้ปฏิบัติตามการควบคุมหรือไม่
3. มีการปฏิบัติงานจริงตามระบบการควบคุมที่มีอยู่หรือไม่
4. ถ้ามีการปฏิบัติงานจริงระบบการควบคุมที่มีอยู่ การควบคุมได้รับผลสำเร็จตามวัตถุประสงค์ที่กำหนด หรือไม่
5. ประโยชน์ที่ได้รับ คุ้มค่ากับต้นทุนของการควบคุม หรือไม่

ช่องที่ (๗) จุดอ่อนและสาเหตุ ระบุสภาพปัญหาหรือจุดอ่อน พร้อมทั้งสาเหตุที่การควบคุม ช่องที่ (๖) ได้รับการประเมินว่าไม่เพียงพอ/ไม่มีประสิทธผล

ช่องที่ (๘) เสนอแนะการปรับปรุงการควบคุมเพื่อป้องกันหรือลดความเสี่ยงตามช่องที่ (๒) หรือช่องที่ (๗)