
# แผนบริหารความเสี่ยง
# ด้านเทคโนโลยีสารสนเทศ

**กรมเจ้าท่า**

**ปีงบประมาณ พ.ศ. ๒๕๖๒**

# คำนำ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมเจ้าท่า ประจำปีงบประมาณ พ.ศ. ๒๕๖๒ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น กลุ่มเทคโนโลยีสารสนเทศ สำนักแผนงาน หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ กรมเจ้าท่า ประจำปีงบประมาณ พ.ศ. ๒๕๖๒ นี้จะช่วยลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของกรมเจ้าท่าต่อไป

กลุ่มเทคโนโลยีสารสนเทศ สำนักแผนงาน

มีนาคม ๒๕๖๒

# สารบัญ

# บทสรุปผู้บริหาร

การจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีวัตถุประสงค์เพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม คำนึงถึงสิ่งที่อาจมีผลกระทบต่อการดำเนินงานพร้อมเตรียมมาตรการรองรับเพื่อจัดการความเสี่ยงไว้อย่างเป็นระบบ ทำให้การจัดการความเสี่ยงประสบความสำเร็จสามารถลดความสูญเสียที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิภาพ โดยได้ดำเนินการตามกระบวนการจัดการบริหารความเสี่ยง ๕ ขั้นตอน ได้แก่ ๑) ระบุปัจจัยเสี่ยง ๒) วิเคราะห์ความเสี่ยง ๓) กำหนดมาตรการจัดการความเสี่ยง ๔) ติดตาม รายงาน ประเมินผล ๕) ทบทวนการบริหารความเสี่ยง โดยสามารถระบุปัจจัยความเสี่ยงได้เป็น ๔ ด้าน ดังนี้

๑. ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ

๒. ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ

๓. ความเสี่ยงด้านความมั่นคงและปลอดภัยของระบบฐานข้อมูล

๔. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ

โดยได้วิเคราะห์และกำหนดมาตรการจัดการความเสี่ยง กำหนดเป็นแนวทางการควบคุม ดังนี้

๑. จัดทำการสำรองฐานข้อมูลสารสนเทศ รวมทั้งจัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้

๒. ดำเนินการทดสอบการกู้คืน ฐานข้อมูลสารสนเทศ และระบบสารสนเทศ

๓. ตรวจสอบระบบเครือข่ายสื่อสารหลัก ระบบสำรองไฟฟ้า (UPS) ระบบป้องกันการบุกรุกระบบ เครือข่าย(Firewall)

๔. ติดตั้งโปรแกรมป้องกันไวรัสและทำการปรับปรุง ฐานข้อมูล Anti Virus ให้ทันสมัย

๕. ตรวจสอบระบบรักษาความปลอดภัยในการเข้า-ออก ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

๖. ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง

๗. กำหนดสิทธิ์ในการเข้าถึงข้อมูลระหว่างผู้ใช้งาน และผู้ดูแลระบบเทคโนโลยีสารสนเทศ

รวมทั้งได้มีการติดตาม รายงาน ประเมินผล และทบทวนการบริหารความเสี่ยงเป็นประจำทุกปี โดยได้มีการดำเนินกิจกรรมเพื่อควบคุมความเสี่ยงในแต่ละปัจจัยเสี่ยงให้ลดลงในระดับที่คาดว่ากรมฯ ยอมรับได้ คือ อยู่ในระดับความเสี่ยงค่อนข้างต่ำ และความเสี่ยงต่ำ ตามลำดับ

## ๑. การบริหารความเสี่ยง (Risk Management)

การบริหารงานขององค์กรทุกประเภท ทั้งภาครัฐ และภาคเอกชน ต่างมีวัตถุประสงค์ของตนเอง และมุ่งหวังที่จะทำงานไปให้ถึงเป้าหมายที่วางไว้อย่างดีที่สุด สูญเสียทรัพยากรให้น้อยที่สุด แต่การดำเนินการใดๆ เพื่อบรรลุวัตถุประสงค์ที่วางไว้ มักจะต้องประสบความไม่แน่นอนที่จะประสบความสำเร็จมาก น้อยแล้วแต่สภาวะที่แวดล้อมอยู่ ดังนั้นความเสี่ยงจึงเป็นภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาสที่ทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อผลเสียหายแก่องค์กร ทั้งในด้านยุทธศาสตร์ การดำเนินงาน การเงิน ทรัพยากรต่างๆ หรือแม้แต่ชื่อเสียง ภาพลักษณ์

ประเด็นที่สำคัญในเรื่องความเสี่ยง (RISK) คือ ความไม่แน่นอน (Uncertainty) ของผลลัพธ์ที่อาจเป็นในเชิงบวก หรือเชิงลบก็ได้ หากองค์กรสามารถเข้าไปบริหารความเสี่ยงได้อย่างถูกต้อง ภาวะคุกคาม ปัญหา อุปสรรคทั้งหลายที่คาดไว้อาจก่อให้เกิดโอกาสและนำไปสู่นวัตกรรมได้ ทั้งยังเกิดโอกาสในการพัฒนาประสิทธิภาพในการทำงาน และการให้บริการ ความเสี่ยงเป็นเรื่องประกอบกันระหว่างองค์ประกอบที่สำคัญ ๒ ส่วน คือ โอกาสที่น่าจะเกิดขึ้นของสิ่งที่ไม่พึงประสงค์ กับผลกระทบที่ตามมา การบริหารความเสี่ยงอย่างเหมาะสมจะเป็นการสนับสนุน กลยุทธ์และแผนงานให้บรรลุเป้าหมายตามที่วางไว้ เข้าใจภัยคุกคามของการปฏิบัติงานในองค์กรมีประสิทธิภาพมากขึ้น สนับสนุนให้มีการปรับปรุงงานอย่างต่อเนื่อง มีการสื่อสารในองค์กรมากขึ้น ความสัมพันธ์ต่าง ๆ ก็ดีตามมา การบริหารความเสี่ยงระดับองค์กร เป็นการผสมผสานการบริหารความเสี่ยงโดยพิจารณาจากความเสี่ยงทั้งหมด เป็นกระบวนการเชิงระบบเพื่อระบุ ประเมิน ควบคุม และสื่อสารความเสี่ยง โดยให้คลอบคลุมทั้งองค์กร ให้มีกระบวนคิดในการที่จะมองไปข้างหน้า โดยได้รับการสนับสนุน และมีส่วนร่วมจากผู้บริหารในทุกระดับ และจากทุกคนในองค์กรนั้น ๆ

กรมเจ้าท่าตระหนักและเห็นความสำคัญของการบริหารความเสี่ยง จึงจัดให้มีการจัดทำระบบบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของกรมเจ้าท่าขึ้น เพื่อการบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนงานต่าง ๆ โดยลดโอกาส และผลกระทบที่อาจจะเกิดขึ้นในอนาคตให้อยู่ในระดับที่ยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามยุทธศาสตร์ เป็นอันดับแรก และเป้าหมายตามแผนการปฏิบัติราชการ

การบริหารความเสี่ยงเป็นการพิจารณาว่าจะมีสิ่งใด เหตุการณ์ใดที่อาจจะเป็นปัญหา อุปสรรค ทำให้ไม่สามารถบรรลุเป้าหมาย และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลักตามกฎหมายจัดตั้งส่วนราชการ และเป้าหมายตามแผนปฏิบัติราชการ

## ๒ กรมเจ้าท่า

เป็นหน่วยงานภายใต้สังกัดกระทรวงคมนาคมมีบทบาทและภารกิจเกี่ยวกับการควบคุม กำกับ ดูแล และพัฒนาส่งเสริมการคมนาคมทางน้ำให้ได้รับความปลอดภัย สะดวก รวดเร็ว และมีประสิทธิภาพ ตลอดจนการดูแลรักษาสิ่งแวดล้อมทางน้ำ รวมทั้งการผลิตและพัฒนาบุคลากรทุกประเภทที่เกี่ยวข้องกับการขนส่งทางน้ำให้เป็นไปตามมาตรฐานสากล รวมทั้งการส่งเสริมการพัฒนาระบบการขนส่งทางน้ำและการพาณิชย์นาวีให้มีการเชื่อมต่อกับระบบการขนส่งอื่น ๆ ทั้งการขนส่งผู้โดยสารและสินค้า ท่าเรือ อู่เรือ กองเรือไทย และกิจการ

เกี่ยวเนื่องเพื่อให้ประชาชนได้รับความสะดวก รวดเร็ว ทั่วถึง และปลอดภัย ตลอดจนการสนับสนุนภาคการส่งออกให้มีความเข้มแข็ง จึงได้จัดทำแผนปฏิบัติราชการประจำปีงบประมาณ ๒๕๖๒ สอดคล้องกับภารกิจและงบประมาณที่ได้รับจัดสรร เพื่อให้สามารถดำเนินการได้อย่างเป็นรูปธรรมและบรรลุตามเป้าหมายที่ได้กำหนดไว้

## ๒.๑ วิสัยทัศน์

"พัฒนาระบบขนส่งทางน้ำอย่างบูรณาการให้เกิดความมั่นคง ปลอดภัย
และเพิ่มศักยภาพการแข่งขันของประเทศ"

## ๒.๒ พันธกิจ

กำกับดูแล การส่งเสริมการพัฒนาระบบการขนส่งทางน้ำและการพาณิชยนาวีให้มีการเชื่อมต่อกับระบบการขนส่งอื่น ๆ ทั้งการขนส่งผู้โดยสาร และสินค้า ท่าเรือ อู่เรือ กองเรือไทย และกิจการเกี่ยวเนื่อง เพื่อให้ประชาชนได้รับความสะดวก รวดเร็ว ทั่วถึง และปลอดภัย ตลอดจนการสนับสนุนภาคการส่งออกให้มีความเข้มแข็ง โดยมีอำนาจหน้าที่ ดังนี้

๑. ดำเนินการตามกฎหมายว่าด้วยการเดินเรือในน่านน้ำไทย กฎหมายว่าด้วยเรือไทย กฎหมายว่าด้วยการป้องกันเรือโดนกัน กฎหมายว่าด้วยการส่งเสริมการพาณิชยนาวี กฎหมายว่าด้วยการขนส่งต่อเนื่องหลายรูปแบบ และกฎหมายอื่นที่เกี่ยวข้อง
๒. ศึกษาและวิเคราะห์เพื่อพัฒนาโครงสร้างพื้นฐานการขนส่งทางน้ำ
๓. ส่งเสริมและพัฒนาเครือข่ายระบบการขนส่งทางน้ำและการพาณิชยนาวี
๔. ดำเนินการจัดระเบียบการขนส่งทางน้ำและกิจการพาณิชยนาวี
๕. ร่วมมือและประสานงานกับองค์การและหน่วยงานที่เกี่ยวข้องทั้งในประเทศและต่างประเทศในด้านการขนส่งทางน้ำ การพาณิชยนาวี และในส่วนที่เกี่ยวกับอนุสัญญาและความตกลงระหว่างประเทศ

## ๒.๓ ค่านิยมองค์กร

ค่านิยมของกรมเจ้าท่า คือ STEPSS ได้แก่

๑. มีใจให้บริการ (Service Mind)
๒. ทำงานเป็นทีม (Teamwork)
๓. มุ่งผลสัมฤทธิ์ (Efficiency)
๔. ทำงานแบบมืออาชีพ (Professional)
๕. ตระหนักความปลอดภัย (Safety)
๖. มีใจใฝ่รู้ (Seek Learning)

## ๒.๔ ประเด็นยุทธศาสตร์ของกรมเจ้าท่า

ประเด็นยุทธศาสตร์ที่ ๑ พัฒนาและบำรุงรักษาโครงสร้างพื้นฐานทางน้ำตามธรรมชาติเพื่อสนับสนุนการขนส่งให้มีประสิทธิภาพ

ประเด็นยุทธศาสตร์ที่ ๒ การยกระดับความปลอดภัยและความมั่นคงด้านการขนส่งทางน้ำและการพาณิชยนาวี

ประเด็นยุทธศาสตร์ที่ ๓ การพัฒนาศักยภาพในการขนส่งทางน้ำและพาณิชยนาวีเพื่อเพิ่มขีดความสามารถในการแข่งขันของประเทศ

ประเด็นยุทธศาสตร์ที่ ๔ การส่งเสริม สนับสนุนความสามารถในการขับเคลื่อนยุทธศาสตร์

## ๒.๕ เป้าประสงค์ของกรมเจ้าท่า

๑. โครงสร้างพื้นฐานและบริการด้านการคมนาคมขนส่งทางน้ำมีความเชื่อมโยงและส่งเสริมระบบโลจิสติกส์อย่างบูรณาการ
๒. ระบบการขนส่งทางน้ำมีความปลอดภัย รวมทั้งสนับสนุนการพาณิชยนาวี
๓. โครงสร้างพื้นฐานทางน้ำและบริการมีความสะดวก ปลอดภัย สนับสนุนการขนส่งทางน้ำและพาณิชยนาวี
๔. บุคลากรด้านพาณิชยนาวีมีคุณภาพ เป็นไปตามเกณฑ์มาตรฐาน
๕. เสริมสร้างสมรรถนะการบริหารด้วยระบบการบริหารกิจการบ้านเมืองที่ดี

## ๒.๖ กลยุทธ์กรมเจ้าท่า

๑. พัฒนาและบำรุงรักษาโครงสร้างพื้นฐานเพื่อสนับสนุนระบบโลจิสติกส์ให้เพียงพอต่อเนื่องอย่างมีประสิทธิภาพ ตลอดจนเชื่อมโยงกับระบบการขนส่งระบบอื่น
๒. กำหนดมาตรการในการกำกับ ควบคุม ดูแล จัดทำระบบรองรับการปฏิบัติการและการให้บริการด้านความปลอดภัยทางน้ำสร้างข้อกำหนดมาตรฐานสำหรับบังคับใช้กับเรือ คนประจำเรือและโครงสร้างพื้นฐานทางน้ำ
๓. พัฒนาและบำรุงรักษาโครงสร้างพื้นฐานทางน้ำให้มีความสะดวก ปลอดภัย และเชื่อมโยงกับระบบการขนส่งอื่น
๔. พัฒนามาตรฐานหลักสูตร บุคลากรและจัดหาเครื่องมืออุปกรณ์ สถานที่ เพื่อการผลิตบุคลากร ด้านพาณิชยนาวี
๕. สร้างศักยภาพการบริหารจัดการด้านการขนส่งทางน้ำและการบริหารกิจการบ้านเมืองที่ดีให้มีประสิทธิภาพ

## ๒.๗ เป้าหมายการให้บริการกรมเจ้าท่า

๑. พัฒนาและบำรุงรักษาโครงสร้างพื้นฐานและบริการ เพื่อให้ประชาชนเกิดความสะดวก รวดเร็ว ปลอดภัยและเชื่อมโยงกับระบบการขนส่งอื่น สอดคล้องการพัฒนาอย่างบูรณาการ

๒. กำกับ ดูแล และให้บริการเพื่อให้เกิดความสะดวก และปลอดภัย

๓. ผลิตและพัฒนาบุคลากร เพื่อรองรับกิจการพาณิชยนาวี

๔. พัฒนาและบำรุงรักษาโครงสร้างพื้นฐานและบริการ เพื่อให้ประชาชนเกิดความสะดวก รวดเร็ว ปลอดภัยและเชื่อมโยงกับระบบการขนส่งอื่น สอดคล้องการพัฒนาอย่างบูรณาการ

๕. พัฒนาโครงสร้างพื้นฐานทางน้ำและบริการให้มีความคล่องตัวในการเดินทาง และขนส่งสินค้า

๖. ค่าใช้จ่ายในการดำเนินการภาครัฐ

## ๒.๘ วิสัยทัศน์ พันธกิจ ด้านเทคโนโลยีสารสนเทศสารสนเทศ กรมเจ้าท่า

### ๒.๘.๑ วิสัยทัศน์

*“ยกระดับคมนาคมขนส่งทางน้ำ สู่ยุค Digital Transport & Logistics”*

### ๒.๘.๒. พันธกิจ

๑. นำระบบไอซีทีมาเพิ่มศักยภาพในการบริหารจัดการและการบริการ

๒. พัฒนาและเพิ่มสมรรถนะด้านไอซีที ให้กับบุคลากรอย่างเป็นระบบและต่อเนื่อง

๓. กำหนดทิศทางการพัฒนาระบบไอซีทีของกรมให้เป็นเอกภาพ

### ๒.๘.๓ ยุทธศาสตร์การพัฒนาเทคโนโลยีสารสนเทศของกรม

ยุทธศาสตร์การพัฒนาระบบไอซีทีของกรมจะอยู่ในกรอบยุทธศาสตร์ไอซีที ของประเทศและของกระทรวง โดยมีเป้าประสงค์ กลยุทธ์ และตัวชี้วัด ดังนี้

๑. ยุทธศาสตร์ที่ ๑ : พัฒนา Digital Transport & Logistics เพื่อเพิ่มขีดความสามารถของการแข่งขันทางเศรษฐกิจในการคมนาคมขนส่งทางน้ำ

๒. ยุทธศาสตร์ที่ ๒ : เพิ่มศักยภาพ Digital Infrastructure & Safety เพื่อพัฒนาโครงสร้างพื้นฐานและมีความปลอดภัยในการคมนาคมและขนส่งทางน้ำ

๓. ยุทธศาสตร์ที่ ๓ : พัฒนา Digital Data Transport & Logistics เพื่อบูรณาการและเพิ่มคุณค่าข้อมูลสารสนเทศด้านการคมนาคมขนส่งทางน้ำ

๔. ยุทธศาสตร์ที่ ๔ : พัฒนา Digital Customer & Service เพื่อยกระดับคุณภาพการให้บริการประชาชนและผู้ประกอบการขนส่งทางน้ำ

๕. ยุทธศาสตร์ที่ ๕ : เพิ่มศักยภาพ Digital Government เพื่อเสริมสร้างความเข้มแข็งขององค์กรด้านการบริหารจัดการและบุคลากร

## ๓. นิยามศัพท์ความเสี่ยง

**๓.๑ ความเสี่ยง** คือ ความไม่แน่นอนที่อาจนำไปสู่ความสูญเสียทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ความเสี่ยงมีทั้งประเภทที่เป็นความเสี่ยงที่แท้จริงที่เป็นความเสี่ยงที่มีโดยธรรมชาติ และความเสี่ยงที่เกิดจากการเก็งกำไร ความหมายของความเสี่ยงอาจมีการตีความแตกต่างกันไปหลายอย่างตามแต่ความเชี่ยวชาญ และอาชีพของผู้ให้คำจำกัดความ

**๓.๒ การบริหารความเสี่ยง** เป็นการบริหารปัจจัย และควบคุมกิจกรรม หรือกระบวนการต่าง ๆ เพื่อลดโอกาสที่จะทำให้เกิดความเสียหาย หรือล้มเหลว ดังนั้นเพื่อควบคุมให้ระดับความเสียหาย และผลกระทบที่อาจจะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และสามารถตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามภารกิจหลักตามกฎหมายจัดตั้งส่วนราชการ และเป้าหมายตามแผนปฏิบัติราชการประจำปีงบประมาณของส่วนราชการ

**๓.๓ ความเสี่ยงในการบริหารองค์กร** หมายถึง เหตุการณ์ที่ไม่มีความแน่นอน ที่อาจเกิดขึ้นและส่งผลกระทบในเชิงลบต่อการบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กร

**๓.๔ ปัจจัยเสี่ยง** หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้

**๓.๕ การประเมินความเสี่ยง** หมายถึง การคาดคะเน หรือคำนวณโอกาสที่จะเป็นเหตุให้เกิดความเสียหายและหรือความเสียหายที่จะส่งผลกระทบต่อการทำงานที่ไม่บรรลุเป้าหมายที่วางไว้ เพื่อให้ทราบความสำคัญของความเสี่ยงที่แตกต่างกัน และใช้การพิจารณาในการกำหนดจุดควบคุมความเสี่ยงที่มีนัยสำคัญ

**๓.๖ กิจกรรมควบคุม** หมายถึง กระบวนการปฏิบัติที่ทุกคนในองค์กรร่วมกันพิจารณากำหนดขึ้นเพื่อสร้างความมั่นใจในระดับที่สมเหตุสมผล ในการบรรลุวัตถุประสงค์ของหน่วยงาน

**๓.๗ วัตถุประสงค์ของการบริหารความเสี่ยง**

๑. ให้มีการบริหารความเสี่ยงทั่วทั้งองค์กรแบบบูรณาการโดยมีการจัดการอย่างมีระบบและต่อเนื่อง
๒. ให้มีการกำหนดกระบวนการบริหารความเสี่ยงที่เป็นระบบมาตรฐานเดียวกันทั่วทั้งองค์กร
๓. ให้มีการติดตามประเมินผลการบริหารความเสี่ยงที่มีการทบทวนและปรับปรุงอย่างสม่ำเสมอ
๔. ให้มีการนำเทคโนโลยีสารสนเทศมาใช้เพื่อการจัดการที่ดี
๕. ให้มีการบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานตามปกติ

## ๔. การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ กระบวนการการทำงานที่ช่วยให้ ผู้บริหารด้านเทคโนโลยีสารสนเทศสามารถสร้างความสมดุลของต้นทุนเชิงเศรษฐศาสตร์ และการดำเนินธุรกิจ ระหว่างมาตรการในการป้องกันและการบรรลุผลสำเร็จของพันธกิจ ด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

### ๔.๑ หลักการและเหตุผล

กรมเจ้าท่า ได้นำเทคโนโลยีสารสนเทศมาใช้งานเพื่อช่วยเพิ่มประสิทธิภาพการดำเนินงาน และให้บริการประชาชนได้รับความสะดวก รวดเร็ว ขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอก ส่งผลกระทบต่อการดำเนินงานของกรมฯ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมฯ มีความมั่นคง กรมฯจึงได้มีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ และจัดทำแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ มีการปฏิบัติตามแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ ซึ่งผู้บริหาร เจ้าหน้าที่กลุ่ม

เทคโนโลยีสารสนเทศ ได้มีส่วนร่วมในการจัดทำแผนดังกล่าว และเมื่อมีแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศแล้ว จำเป็นต้องมีการปฏิบัติตามแผน รวมทั้งมีการทบทวนและปรับปรุงนโยบายและแผนดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

**๔.๒ วัตถุประสงค์**

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

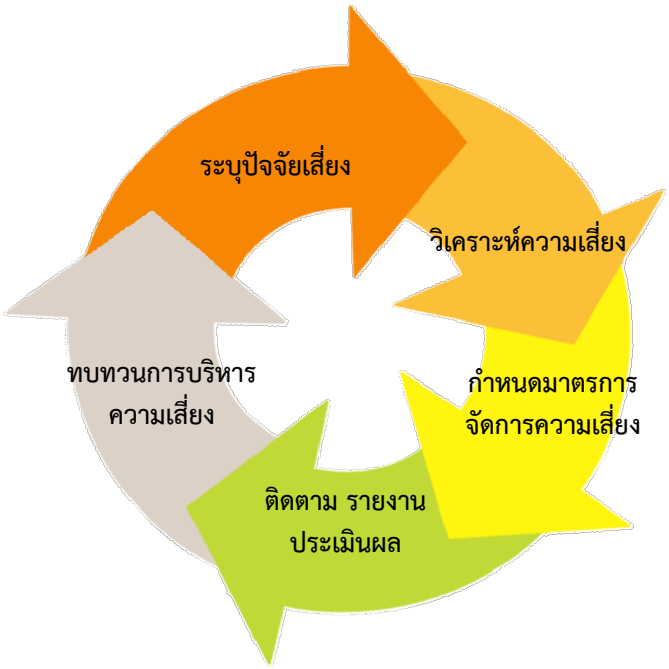
๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศดำเนินงานได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหาร และผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของกรมเจ้าท่า

## ๕. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้



๑. **ระบุปัจจัยเสี่ยงและผลกระทบด้านต่าง ๆ ที่จะเกิดขึ้น**

| ที่มาความเสี่ยง / ปัจจัยเสี่ยง | ผลกระทบต่อด้านต่าง ๆ | | |
|---|---|---|---|
| | ระบบ/อุปกรณ์สารสนเทศ | ผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย | เวลา |
| **๑. ด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ** | | | |
| ๑. ระบบฐานข้อมูล/ระบบงานที่ให้บริการเกิดความเสียหาย | - ทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงัก หรือหยุดทำงาน<br>- ข้อมูลของกรมเสียหาย | - ผู้ใช้งานไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศเพื่อการปฏิบัติงาน และให้บริการประชาชนได้อย่างเต็มประสิทธิภาพ | - กระบวนการดำเนินงานล่าช้า |
| ๒. ข้อมูลเสียหายเกิดจากอุปกรณ์บันทึกข้อมูล (Hard disk) ชำรุด | - ทำให้การปฏิบัติงานหรือการดำเนินงานด้านสารสนเทศของกรม หยุดชะงัก และข้อมูล ชำรุดสูญหาย | - ผู้บริหารมิได้รับข้อมูลที่ถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจในการดำเนินงาน | - กระบวนการดำเนินงานล่าช้า |
| **๒. ด้านภัยพิบัติระบบสารสนเทศ** | | | |
| ๑. ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม | - เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์และฐานข้อมูลถูกทำลายทั้งหมดการดำเนินงานหยุดชะงัก หยุดระบบประมวลผลทั้งระบบลง | - ผู้รับบริการไม่สามารถใช้งานระบบได้ | - กระบวนการดำเนินงานล่าช้า |
| ๒. ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง | - หยุดระบบประมวลผลทั้งระบบลง เกิดการชะงักทำให้ระบบเสียหาย ไม่สามารถใช้งานระบบได้อย่างเต็มประสิทธิภาพ | - ผู้รับบริการไม่สามารถใช้งานระบบได้<br>- สูญเสียเวลาของผู้รับบริการ | - กระบวนการดำเนินงานล่าช้า |
| ๓.สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง การชุมนุมประท้วง การจลาจล การก่อการร้าย | | - การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ | |
| **๓. ด้านความมั่นคงและปลอดภัยของระบบฐานข้อมูล** | | | |
| ๑. ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ | - ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการ<br>- ทำความเสียหายระยะยาวให้แก่อุปกรณ์ | - ผู้ใช้งาน (User) ไม่สามารถเข้ามาใช้งานในระบบได้ทั้งหมด | - กระบวนการดำเนินงานล่าช้า |

| ที่มาความเสี่ยง / ปัจจัยเสี่ยง | ผลกระทบต่อด้านต่าง ๆ | | |
|---|---|---|---|
| | ระบบ/อุปกรณ์สารสนเทศ | ผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย | เวลา |
| | คอมพิวเตอร์<br>- เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ชั่วคราว<br>- ทำให้เกิดความเสียหายที่ถาวรแก่ข้อมูลไม่สามารถกู้กลับข้อมูลได้ | | |
| ๒. การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server | - ข้อมูลและการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิ์แก่บุคคลที่มีหน้าที่รับผิดชอบทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์<br>- ขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ | - ถ้าบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำไปแสวงหาประโยชน์โดยมิชอบได้<br>- บุคคลที่มีหน้าที่รับผิดชอบทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ ส่งผลให้ไม่สามารถปฏิบัติงานได้ | |
| ๓. การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล | - ทำให้ข้อมูลและการทำงานของระบบเสียหาย ส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน<br>- สูญเสียค่าใช้จ่ายในการเก็บรวบรวมข้อมูล<br>- ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข | - ข้อมูลที่ได้รับไม่สอดคล้องกับความต้องการของผู้ใช้งาน | |
| ๔. ความเสียหายจากไวรัสคอมพิวเตอร์ | - ไวรัสรบกวนการทำงานของระบบและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ<br>- ปริมาณข้อมูลบนเครือข่ายที่สูงมากผิดปกติ อาจเกิดจากไวรัสกำลังแพร่กระจายอยู่<br>- มีการส่งหรือรับข้อมูลในเครือข่ายของหน่วยงานเป็นปริมาณสูง | | - จะมีผลทำให้การใช้งานเครือข่ายเป็นไปอย่างล่าช้าติดขัด หรืออาจไม่สามารถใช้งานได้ |

| ที่มาความเสี่ยง / ปัจจัยเสี่ยง | ผลกระทบต่อด้านต่าง ๆ | | |
|---|---|---|---|
| | ระบบ/อุปกรณ์สารสนเทศ | ผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย | เวลา |
| **ด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ** | | | |
| ๑. การแอบ/ลักลอบเข้าสู่ห้อง Server หรือไม่มีการควบคุม การเข้าออกห้อง Server | - หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงห้อง Server อาจจะทำลายอุปกรณ์คอมพิวเตอร์หรือฐานข้อมูลของระบบได้<br>- การขโมยข้อมูลหรืออุปกรณ์ | | |
| ๒. การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต | - บุคลากรที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูลและอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ<br>- ข้อมูลและการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลงได้ | - อาจมีการแก้ไขสิทธิ์ให้บุคคลที่มีอำนาจไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบทำให้ไม่สามารถปฏิบัติงานในระบบได้ | - กระบวนการดำเนินงานล่าช้า |

## ๒. ประเมินความเสี่ยง

| ประเภทความเสี่ยง | ปัจจัยเสี่ยง | รายละเอียดความสูญเสีย | โอกาส | ผลกระทบ | ระดับความเสี่ยง |
|---|---|---|---|---|---|
| ๑. ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ | ๑.๑ ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย | - ทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงัก หรือหยุดทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ | ๒ | ๔ | ๘ |
| | ๑.๒ ข้อมูลเสียหายเกิดจากอุปกรณ์ บันทึกข้อมูล (Hard disk) ชำรุด | - ทำให้การปฏิบัติงานหรือการดำเนินงานด้านสารสนเทศของ กรม หยุดชะงักกระบวนการดำเนินงานล่าช้าและข้อมูลชำรุด สูญหาย ผู้บริหารมิได้รับข้อมูลที่ถูกต้องและทันเวลาเพื่อใช้ประกอบ การตัดสินใจในการดำเนินงาน | ๒ | ๔ | ๘ |
| ๒. ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ | ๒.๑ ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม | - เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์และฐานข้อมูล ถูกทำลายทั้งหมดการดำเนินงานหยุดชะงัก หยุดระบบประมวลผลทั้งระบบลง ผู้รับบริการไม่สามารถใช้งานระบบได้ | ๑ | ๕ | ๕ |
| | ๒.๒ ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง | - หยุดระบบประมวลผลทั้งระบบลง ผู้รับบริการไม่สามารถใช้งานระบบได้ เกิดการชะงัก ทำให้ระบบเสียหาย ไม่สามารถใช้งานระบบได้อย่างเต็มประสิทธิภาพ<br>- สูญเสียเวลา ของผู้รับบริการ | ๑ | ๕ | ๕ |
| | ๒.๓ สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง การชุมนุมประท้วง การจลาจล การก่อการร้าย | - การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ | ๑ | ๕ | ๕ |
| ๓. ความเสี่ยงด้านความมั่นคง และปลอดภัยของระบบฐานข้อมูล | ๓.๑ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ | - ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการ<br>- ผู้ใช้งาน (User) ไม่สามารถเข้ามาใช้งานในระบบได้ทั้งหมด<br>- ทำความเสียหายระยะยาวให้แก่อุปกรณ์คอมพิวเตอร์<br>- เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ชั่วคราว<br>- ทำให้เกิดความเสียหายที่ถาวรแก่ข้อมูลไม่สามารถกู้กลับข้อมูลได้ | ๑ | ๕ | ๕ |
| | ๓.๒ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server | - ถ้าบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำไปแสวงหาประโยชน์โดยมิชอบได้ ข้อมูลและการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลงทำลายหรืออาจกระทำการแก้ไขสิทธิ์แก่บุคคลที่มีหน้าที่รับผิดชอบทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ส่งผลให้ไม่สามารถปฏิบัติงานได้<br>- ขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ | ๒ | ๔ | ๘ |

| ประเภทความเสี่ยง | ปัจจัยเสี่ยง | รายละเอียดความสูญเสีย | โอกาส | ผลกระทบ | ระดับความเสี่ยง |
|---|---|---|---|---|---|
| | ๓.๓ การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล | - ทำให้ข้อมูลและการทำงานของระบบเสียหาย ส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้<br>- สูญเสียค่าใช้จ่ายในการเก็บรวบรวมข้อมูล<br>- ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข | ๒ | ๔ | ๘ |
| | ๓.๔ ความเสียหายจากไวรัสคอมพิวเตอร์ | - มีไวรัสรบกวนการทำงานของระบบและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ<br>- ปริมาณข้อมูลบนเครือข่ายที่สูงมากผิดปกติ อาจเกิดจากไวรัสกำลังแพร่กระจายอยู่<br>- มีการส่งหรือรับข้อมูลในเครือข่ายของหน่วยงานเป็นปริมาณสูง ซึ่งปริมาณข้อมูลในเครือข่ายที่สูงเกิดไป จะมีผลทำให้การใช้งานเครือข่ายเป็นไปอย่างล่าช้า ติดขัด หรืออาจไม่สามารถใช้งานได้ | ๓ | ๔ | ๑๒ |
| ๔. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ | ๔.๑ การแอบ/ลักลอบเข้าสู่ห้อง Server หรือไม่มีการควบคุม การเข้าออกห้อง Server | - หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงห้อง Server ได้ อาจจะทำลายอุปกรณ์คอมพิวเตอร์หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ได้<br>- การขโมยข้อมูลหรืออุปกรณ์ | ๑ | ๔ | ๔ |
| | ๔.๒ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต | - บุคลากรที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูลและอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ<br>- ข้อมูลและการทำงานของระบบคอมพิวเตอร์ ถูกแก้ไขเปลี่ยนแปลงได้ อาจมีการแก้ไขสิทธิ์ให้บุคคลที่มีอำนาจไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบทำให้ไม่สามารถปฏิบัติงานในระบบได้ | ๑ | ๔ | ๔ |

**หมายเหตุ :** เกณฑ์การให้คะแนนโอกาสที่จะเกิดและผลกระทบจากต่ำไปสูงคือ ๑ ถึง ๕

๑ = รุนแรงน้อยที่สุด / โอกาสเกิดน้อยที่สุด ๒ = รุนแรงน้อย / โอกาสเกิดน้อย ๓ = รุนแรงปานกลาง / โอกาสเกิดปานกลาง

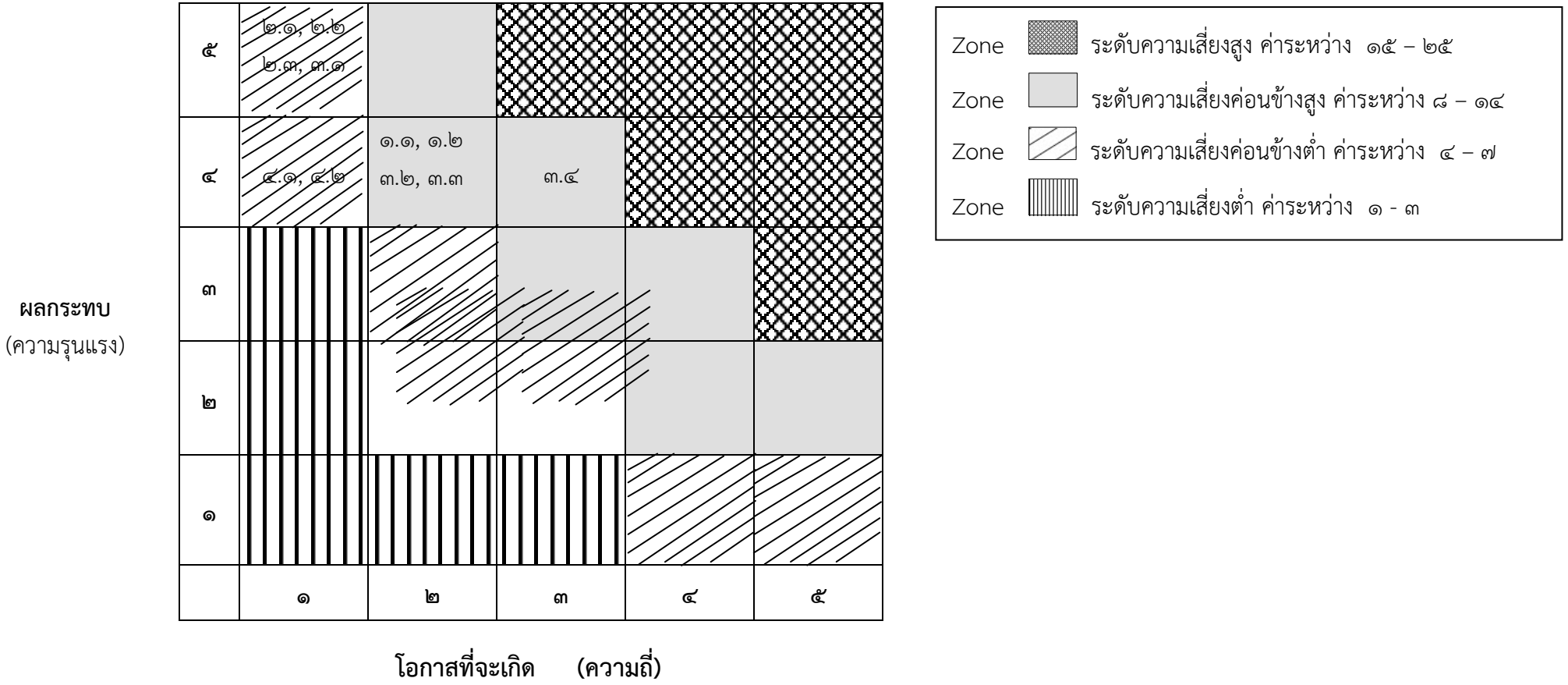
๔ = รุนแรงมาก / โอกาสเกิดมาก ๕ = รุนแรงมากที่สุด / โอกาสเกิดมากที่สุด

**๓. สรุปทางเลือกที่เหมาะสมในการจัดการความเสี่ยง**

| ปัจจัยเสี่ยง | ระดับความเสี่ยง | วิธีจัดการความเสี่ยง | ทางเลือกที่เหมาะสม |
|---|---|---|---|
| **ลำดับที่ ๑**<br>ความเสียหายจากไวรัสคอมพิวเตอร์ | ๑๒ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |
| **ลำดับที่ ๒**<br>การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล | ๘ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |
| **ลำดับที่ ๓**<br>การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server | ๘ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |
| **ลำดับที่ ๔**<br>ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย | ๘ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |
| **ลำดับที่ ๕**<br>ข้อมูลเสียหายเกิดจากอุปกรณ์ บันทึกข้อมูล (Hard disk) ชำรุด | ๘ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |

| ปัจจัยเสี่ยง | ระดับความเสี่ยง | วิธีจัดการความเสี่ยง | ทางเลือกที่เหมาะสม |
|---|---|---|---|
| **ลำดับที่ ๖**<br>ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ | ๕ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |
| **ลำดับที่ ๗**<br>ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม | ๕ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |
| **ลำดับที่ ๘**<br>ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง | ๕ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |
| **ลำดับที่ ๙**<br>สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง การชุมนุมประท้วง การจลาจล การก่อการร้าย | ๕ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |
| **ลำดับที่ ๑๐**<br>การแอบ/ลักลอบเข้าสู่ห้อง Server หรือ ไม่มีการควบคุม การเข้าออกห้อง Server | ๔ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |
| **ลำดับที่ ๑๑**<br>การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต | ๔ | หลีกเลี่ยง<br>ยอมรับ<br>ควบคุม<br>ถ่ายโอน | ควบคุม |

**การจัดทำแผนภูมิความเสี่ยง (Risk Map) ก่อนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ**



## ๔. การจัดการความเสี่ยง

| ประเภทความเสี่ยง | ปัจจัยเสี่ยง | ที่มาของความเสี่ยง | ความเสียหายที่อาจเกิดขึ้น | โอกาส (๑) | ผลกระทบ (๒) | ระดับคะแนน (๑) X (๒) | แนวทางการควบคุม |
|---|---|---|---|---|---|---|---|
| ๑. ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและ ข้อมูลสารสนเทศ | ๑.๑ ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย | ด้านการดำเนินการ | - ทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้เกิดการชะงัก หรือหยุดทำงาน ส่งผลให้ไม่สามารถใช้งาน ระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ | ๒ | ๔ | ๘ | - จัดทำการสำรองฐานข้อมูลสารสนเทศ<br>- ทดสอบการกู้คืนฐานข้อมูลสารสนเทศและระบบสารสนเทศ |
| | ๑.๒ ข้อมูลเสียหายเกิดจากอุปกรณ์ บันทึกข้อมูล (Hard disk) ชำรุด | ด้านการดำเนินการ | - ทำให้การปฏิบัติงานหรือการดำเนินงานด้านสารสนเทศของกรม หยุดชะงักกระบวนการดำเนินงานล่าช้าและข้อมูลชำรุดสูญหาย ผู้บริหารมิได้รับข้อมูลที่ถูกต้องและทันเวลาเพื่อใช้ประกอบ การตัดสินใจในการดำเนินงาน | ๒ | ๔ | ๘ | - จัดทำการสำรองฐานข้อมูลสารสนเทศ<br>- ทดสอบการกู้คืนฐานข้อมูลสารสนเทศและระบบสารสนเทศ |
| ๒. ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ | ๒.๑ ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม | ด้านกายภาพและสิ่งแวดล้อม | - เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์และฐานข้อมูล ถูกทำลายทั้งหมดการดำเนินงานหยุดชะงัก หยุดระบบประมวลผลทั้งระบบลง ผู้รับบริการไม่สามารถใช้งานระบบได้ | ๑ | ๕ | ๕ | - ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง<br>-จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้<br>-สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด |
| | ๒.๒ ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง | ด้านกายภาพและสิ่งแวดล้อม | - หยุดระบบประมวลผลทั้งระบบลง ผู้รับบริการไม่สามารถใช้งานระบบได้ เกิดการชะงัก ทำให้ระบบเสียหายไม่สามารถใช้งานระบบได้อย่างเต็มประสิทธิภาพ<br>- สูญเสียเวลา ของผู้รับบริการ | ๑ | ๕ | ๕ | - ตรวจสอบระบบเครือข่ายสื่อสารหลัก |

| ประเภทความเสี่ยง | ปัจจัยเสี่ยง | ที่มาของความเสี่ยง | ความเสียหายที่อาจเกิดขึ้น | โอกาส (๑) | ผลกระทบ (๒) | ระดับคะแนน (๑) X (๒) | แนวทางการควบคุม |
|---|---|---|---|---|---|---|---|
| | ๒.๓ สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง การชุมนุมประท้วง การจลาจล การก่อการร้าย | ด้านกายภาพและสิ่งแวดล้อม | - การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ | ๑ | ๕ | ๕ | -จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ |
| ๓. ความเสี่ยงด้านความมั่นคงและปลอดภัยของระบบฐานข้อมูล | ๓.๑ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ | ด้านกายภาพและสิ่งแวดล้อม | - ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่<br>- สามารถให้บริการ<br>- ผู้ใช้งาน (User) ไม่สามารถเข้ามาใช้งานในระบบได้ทั้งหมด<br>- ทำความเสียหายระยะยาวให้แก่อุปกรณ์คอมพิวเตอร์<br>- เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ชั่วคราว<br>- ทำให้เกิดความเสียหายที่ถาวรแก่ข้อมูลไม่สามารถกู้กลับข้อมูลได้ | ๑ | ๕ | ๕ | - ตรวจสอบระบบสำรองไฟฟ้า (UPS) |
| | ๓.๒ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server | ด้านภาพลักษณ์ | - ถ้าบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูลและอาจนำไปแสวงหาประโยชน์โดยมิชอบได้ ข้อมูลและการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิ์แก่บุคคลที่มีหน้าที่รับผิดชอบทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ ส่งผลให้ไม่สามารถปฏิบัติงานได้<br>- ขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ | ๒ | ๔ | ๘ | - ตรวจสอบระบบป้องกันการ บุกรุกระบบเครือข่าย(Firewall) |
| | ๓.๓ การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล | ด้านภาพลักษณ์ | - ทำให้ข้อมูลและการทำงานของระบบเสียหาย ส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้<br>- สูญเสียค่าใช้จ่ายในการเก็บรวบรวมข้อมูล<br>- ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข | ๒ | ๔ | ๘ | - ตรวจสอบระบบป้องกันการ บุกรุกระบบเครือข่าย(Firewall) |

| ประเภทความเสี่ยง | ปัจจัยเสี่ยง | ที่มาของความเสี่ยง | ความเสียหายที่อาจเกิดขึ้น | โอกาส (๑) | ผลกระทบ (๒) | ระดับคะแนน (๑) X (๒) | แนวทางการควบคุม |
|---|---|---|---|---|---|---|---|
| | ๓.๔ ความเสียหายจากไวรัสคอมพิวเตอร์ | ด้านการดำเนินการ | - มีไวรัสรบกวนการทำงานของระบบและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ<br>- ปริมาณข้อมูลบนเครือข่ายที่สูงมากผิดปกติ อาจเกิดจากไวรัสกำลังแพร่กระจายอยู่<br>- มีการส่งหรือรับข้อมูลในเครือข่ายของหน่วยงานเป็นปริมาณสูง ซึ่งปริมาณข้อมูลในเครือข่ายที่สูง เกินไปจะมีผลทำให้การใช้งานเครือข่ายเป็นไปอย่างล่าช้า ติดขัด หรืออาจไม่สามารถใช้งานได้ | ๓ | ๔ | ๑๒ | - มีโปรแกรมป้องกันไวรัสและทำการปรับปรุงฐานข้อมูล Anti Virus ให้ทันสมัย |
| ๔. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ | ๔.๑ การแอบ/ลักลอบเข้าสู่ห้อง Server หรือไม่มีการควบคุมการเข้าออกห้อง Server | ด้านภาพลักษณ์ | - หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงห้อง Server ได้ อาจจะทำลายอุปกรณ์คอมพิวเตอร์ หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ได้<br>- การขโมยข้อมูลหรืออุปกรณ์ | ๑ | ๔ | ๔ | - ตรวจสอบระบบรักษาความปลอดภัย ในการเข้า-ออก ห้อง Server |
| | ๔.๒ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต | ด้านการดำเนินการ | - บุคลากรไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูลและอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ<br>- ข้อมูลและการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลงได้อาจมีการแก้ไขสิทธิ์ให้บุคคลที่มีอำนาจไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ทำให้ไม่สามารถปฏิบัติงานในระบบได้ | ๑ | ๔ | ๔ | - กำหนดสิทธิ์ในการเข้าถึงข้อมูลระหว่างผู้ใช้งาน และผู้ดูแลระบบเทคโนโลยีสารสนเทศ |

**๕. รายการกิจกรรมในการจัดการความเสี่ยง**

| ประเภทความเสี่ยง/กิจกรรม | ปัจจัยเสี่ยง | ความเสียหายที่อาจเกิดขึ้น | ความสำคัญ | แนวทางการควบคุม | กิจกรรมในการควบคุม | หน่วยงานรับผิดชอบ | กำหนดการดำเนินการ |
|---|---|---|---|---|---|---|---|
| ๑. ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ | ๑.๑ ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย | - ทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักหรือหยุดทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ | ๘ | - จัดทำการสำรองฐานข้อมูลสารสนเทศ<br>- ทดสอบการกู้คืนฐานข้อมูลสารสนเทศและระบบสารสนเทศ | - มีการสำรองข้อมูลในฐานข้อมูลเป็นประจำทุกวัน เก็บไว้ในหน่วยเก็บสำรองข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายของระบบนั้นๆ<br>๑. ทำการสำรองข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด เป็นประจำทุกวัน โดยจะมีการสำรองข้อมูลที่เพิ่มเติมในแต่ละวัน โดยจัดเก็บไว้ที่หน่วยเก็บสำรองข้อมูล ที่ติดตั้ง ณ อาคาร ๖ ชั้น ๔ และศูนย์สำรองข้อมูลนอกสำนักงาน ณ ศูนย์ฝึกพาณิชย์นาวี จ.สมุทรปราการ<br>๒. ทำการสำรองข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด เป็นประจำทุกสัปดาห์ โดยในแต่ละสัปดาห์ระบบจะดำเนินการสำรองข้อมูลทั้งหมดใหม่ทุกครั้ง โดยจัดเก็บไว้ที่หน่วยเก็บสำรองข้อมูล ที่ติดตั้ง ณ อาคาร ๖ ชั้น ๔ และและศูนย์สำรองข้อมูลนอกสำนักงาน ณ ศูนย์ฝึกพาณิชย์นาวี จ.สมุทรปราการ | สผง.(ทส.) | - จัดทำการสำรองข้อมูลแบบอัตโนมัติ ทุกวัน ทุกสัปดาห์<br>- ทดสอบการกู้คืนข้อมูล (Data Recovery) ปีละ ๑ ครั้ง |

| ประเภทความเสี่ยง/กิจกรรม | ปัจจัยเสี่ยง | ความเสียหายที่อาจเกิดขึ้น | ความสำคัญ | แนวทางการควบคุม | กิจกรรมในการควบคุม | หน่วยงานรับผิดชอบ | กำหนดการดำเนินการ |
|---|---|---|---|---|---|---|---|
| | ๑.๒ ข้อมูลเสียหายเกิดจากอุปกรณ์บันทึกข้อมูล (Hard disk) ชำรุด | - ทำให้การปฏิบัติงานหรือการดำเนินงานด้านสารสนเทศของกรม หยุดชะงักกระบวนการดำเนินงานล่าช้าและข้อมูลชำรุด สูญหาย ผู้บริหารมิได้รับข้อมูลที่ถูกต้องและทันเวลา เพื่อใช้ประกอบ การตัดสินใจในการดำเนินงาน | ๘ | - จัดทำการสำรองฐานข้อมูลสารสนเทศ<br>- ทดสอบการกู้คืนฐานข้อมูลสารสนเทศ และระบบสารสนเทศ | - มีการทดสอบการ Recovery ข้อมูล,ฐานข้อมูล,โปรแกรมปฏิบัติการฐานข้อมูลและระบบปฏิบัติการของเครื่องแม่ข่ายต่างๆ ที่ได้ดำเนินการสำรองข้อมูลไว้ เพื่อทำการทดสอบการกู้คืนข้อมูล (Recovery) หากระบบงานหรือเครื่องแม่ข่ายหลักเกิดความเสียหาย | | |
| ๒. ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ | ๒.๑ ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม | - เกิดความเสียหายกับทรัพย์สินระบบเครือข่าย อุปกรณ์และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก หยุดระบบประมวลผลทั้งระบบลง ผู้รับบริการไม่สามารถใช้งานระบบได้ | ๕ | - ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง | - ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง และสัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งาน ณ ห้องควบคุมระบบ<br>- จัดทำแผนรองรับภาวะฉุกเฉินและภัยธรรมชาติ และมีการซักซ้อมแผน ปีละ ๑ ครั้ง | สผง.(ทส.) | - ทุก ๓ เดือน<br>- ปีละ ๑ ครั้ง |

| ประเภทความเสี่ยง/กิจกรรม | ปัจจัยเสี่ยง | ความเสียหายที่อาจเกิดขึ้น | ความสำคัญ | แนวทางการควบคุม | กิจกรรมในการควบคุม | หน่วยงานรับผิดชอบ | กำหนดการดำเนินการ |
|---|---|---|---|---|---|---|---|
| | ๒.๒ ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง | - หยุดระบบประมวลผลทั้งระบบลง ผู้รับบริการไม่สามารถใช้งานระบบได้ เกิดการชะงัก ทำให้ ระบบเสียหาย ไม่สามารถใช้งานระบบ ได้อย่างเต็มประสิทธิภาพ<br>- สูญเสียเวลา ของผู้รับบริการ | ๕ | - ตรวจสอบระบบเครือข่ายสื่อสารหลัก | - ตรวจสอบสถานะระบบเครือข่ายสื่อสารหลักภายในห้องควบคุมระบบ | สผง.(ทส.) | เดือนละ ๑ ครั้ง |
| ๓. ความเสี่ยงด้านความมั่นคง และปลอดภัยของระบบฐานข้อมูล | ๓.๑ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ | - ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการ<br>- ผู้ใช้งาน (User) ไม่สามารถเข้ามาใช้งานในระบบได้ทั้งหมด<br>- ทำความเสียหายระยะยาวให้แก่อุปกรณ์คอมพิวเตอร์<br>- เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ชั่วคราว<br>- ทำให้เกิดความเสียหายที่ถาวรแก่ข้อมูลไม่สามารถกู้กลับข้อมูลได้ | ๕ | - ตรวจสอบระบบสำรองไฟฟ้า (UPS) | - ตรวจสอบสถานะระบบสำรองไฟฟ้า อุปกรณ์ UPS ภายในห้องควบคุมระบบให้พร้อมสำรองไฟฟ้าเมื่อระบบไฟฟ้าภายในห้องควบคุมระบบขัดข้อง | สผง.(ทส.) | ทุก ๓ เดือน |
| | ๓.๒ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server | - ถ้าบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำไปแสวงหาประโยชน์โดยมิชอบได้ ข้อมูลและการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิ์แก่บุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ส่งผลให้ไม่สามารถปฏิบัติงานได้<br>- ขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ | ๘ | - ตรวจสอบระบบป้องกันการบุกรุก ระบบเครือข่าย (Firewall) | - ตรวจสอบสถานะระบบป้องกันการบุกรุก ระบบเครือข่ายจากอุปกรณ์ Firewall และระบบ IPS (Intrusion Prevention System) | สผง.(ทส.) | เดือนละ ๒-๔ ครั้ง |

| ประเภทความเสี่ยง/กิจกรรม | ปัจจัยเสี่ยง | ความเสียหายที่อาจเกิดขึ้น | ความสำคัญ | แนวทางการควบคุม | กิจกรรมในการควบคุม | หน่วยงานรับผิดชอบ | กำหนดการดำเนินการ |
|---|---|---|---|---|---|---|---|
| | ๓.๓ การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล | - ทำให้ข้อมูลและการทำงานของระบบเสียหาย ส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้<br>- สูญเสียค่าใช้จ่ายในการเก็บรวบรวมข้อมูล<br>- ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข | ๑๒ | - ตรวจสอบระบบป้องกันการบุกรุก ระบบเครือข่าย (Firewall) | - ตรวจสอบสถานะระบบป้องกันการบุกรุก ระบบเครือข่ายจากอุปกรณ์ Firewall และระบบ IPS (Intrusion Prevention System) | สผง.(ทส.) | เดือนละ ๑ ครั้ง |
| | ๓.๔ ความเสียหายจากไวรัสคอมพิวเตอร์ | - มีไวรัสรบกวนการทำงานของระบบและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ<br>- ปริมาณข้อมูลบนเครือข่ายที่สูงมากผิดปกติอาจเกิดจากไวรัสกำลังแพร่กระจายอยู่<br>- มีการส่งหรือรับข้อมูลในเครือข่ายของหน่วยงานเป็นปริมาณสูง ซึ่งปริมาณข้อมูลในเครือข่ายที่สูง เกินไปจะมีผลทำให้การใช้งานเครือข่ายเป็นไปอย่างล่าช้า ติดขัด หรืออาจไม่สามารถใช้งานได้ | ๑๒ | - มีโปรแกรมป้องกันไวรัสและทำการปรับปรุงฐานข้อมูล Anti Virus ให้ทันสมัย | - ตรวจสอบและปรับปรุงฐานข้อมูล Antivirus ภายในเครื่องแม่ข่าย Antivirus ณ ห้องควบคุมระบบ | สผง.(ทส.) | เดือนละ ๔ ครั้ง |
| ๔. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ | ๔.๑ การแอบ/ลักลอบเข้าสู่ห้อง Server หรือไม่มีการควบคุมการเข้าออกห้อง Server | - หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงห้อง Server ได้ อาจจะทำลายอุปกรณ์คอมพิวเตอร์ หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ได้<br>- การขโมยข้อมูลหรืออุปกรณ์ | ๔ | - ตรวจสอบระบบรักษาความปลอดภัยในการเข้า-ออก ห้อง Server | - ตรวจสอบระบบรักษาความปลอดภัย เครื่องสแกนลายนิ้วมือเพื่อจะเข้า-ออก ห้องควบคุมระบบ | สผง.(ทส.) | ทุก ๓ เดือน |

| ประเภทความเสี่ยง/กิจกรรม | ปัจจัยเสี่ยง | ความเสียหายที่อาจเกิดขึ้น | ความสำคัญ | แนวทางการควบคุม | กิจกรรมในการควบคุม | หน่วยงานรับผิดชอบ | กำหนดการดำเนินการ |
|---|---|---|---|---|---|---|---|
| | ๔.๒ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต | - บุคลากรที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูลและอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ<br>- ข้อมูลและการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลงได้ อาจมีการแก้ไขสิทธิ์ให้บุคคลที่มีอำนาจไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ทำให้ไม่สามารถปฏิบัติงานในระบบได้ | ๔ | - กำหนดสิทธิ์ในการเข้าถึงข้อมูลระหว่าง ผู้ใช้งานและผู้ดูแล ระบบเทคโนโลยีสารสนเทศ | กำหนดสิทธิ์ในการเข้าถึงข้อมูลผู้ใช้งาน และผู้ดูและระบบเทคโนโลยีสารสนเทศ ดังนี้<br>- เพิ่มข้อมูลการกำหนดสิทธิ์เมื่อเข้ารับราชการใหม่<br>- ปรับปรุงข้อมูลการกำหนดสิทธิ์เมื่อโยกย้ายตำแหน่ง หรือหน่วยงาน ลบข้อมูลการกำหนดสิทธิ์เมื่อเกษียณอายุหรือลาออกจากราชการ | สผง.(ทส.) | เมื่อแต่งตั้ง / โยกย้าย / ลาออก / เกษียณอายุราชการ |

กรมเจ้าท่าได้ดำเนินการวางแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยดำเนินการดังนี้

๑. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่าง ๆ ด้วยการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน หรือภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)

๓. มีการตรวจสอบควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย

๔. มีระบบการรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Anti-Virus, ระบบไฟฟ้าสำรอง, ระบบ Firewall, ระบบ Backup และระบบคอมพิวเตอร์เพื่อรองรับ พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เป็นต้น

๕. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access rights)

๖. มีการบันทึกเพื่อตรวจสอบ (audit logs) เช่น ให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก โดยการบันทึกการเข้าออกระบบ ( login-logout log)

**การประเมินสถานการณ์ความเสี่ยงแนวทางในการดำเนินการเพื่อลดความเสี่ยง**

จากการตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศ ของกรมเจ้าท่า พบว่ามีความเสี่ยงที่อาจเป็นอันตรายและมีแนวทางดำเนินการ ดังนี้

๑. เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) ขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศ จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรม สัมมนา ให้มีความรู้ความเข้าใจ ในด้าน Hardware และ Software เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด

๒. เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้

๒.๑. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสเสมอ

๒.๒. ติดตั้ง firewall ทำหน้าที่ป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟต์แวร์ป้องกันไวรัส ที่เครื่องให้บริการ (Server) และเครื่องลูกข่าย (Client) เพื่อทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย

๒.๓. แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านเครือข่าย internet รวมทั้งแนะนำวิธีการป้องกัน

๒.๔. การกำจัดภัยที่จะเกิดจากไวรัสต่างๆ ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

๒.๕. ใช้ซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ ไม่ติดตั้งหรือใช้งานซอฟท์แวร์อื่นใดที่ไม่มีลิขสิทธิ์

๒.๖. ไม่ให้ผู้ใช้งานดาวน์โหลดซอฟท์แวร์ ( ไม่ว่าจะผ่านโปรโตคอล FTP หรือ HTTP หรือโปรโตคอลอื่นๆ) และห้ามไม่ให้ผู้ใช้งานใช้โปรแกรมประเภท Peer-to-Peer เช่น Bit Torrent ต่างๆ

๓. เกิดจากระบบไฟฟ้าขัดข้อง โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง มีการดำเนินการดังนี้

๓.๑. ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งจะมีระยะเวลาในการสำรองไฟฟ้าได้ประมาณ ๒๐ - ๓๐ นาที

๓.๒. เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓.๓. เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์

๔. เกิดความเสียหายจากเพลิงไหม้ ได้ติดตั้งระบบดับเพลิงอัตโนมัติ (Fire Suppression System) ทั้งเหนือพื้นยกและบริเวณใต้พื้นยกโดยใช้ระบบ Inert Gas System ชนิด IG-๕๕ ซึ่งเป็นสารสะอาดดับเพลิงที่ไม่เป็นอันตรายต่อสิ่งมีชีวิตและสิ่งแวดล้อมไม่ทำความเสียหายต่ออุปกรณ์คอมพิวเตอร์, อิเลคทรอนิกส์ และได้ติดตั้งระบบตรวจจับควันความไวสูง (High Sensitivity Smoke Detect) บริเวณ Return air ของเครื่องปรับอากาศ ซึ่งจะมีการดำเนินการดังนี้

๔.๑. กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดป้ายเตือนต่างๆ

๔.๒. อบรมขั้นต้นสำหรับพนักงานทุกคนในแผนป้องกันและระงับอัคคีภัยและมีการซ้อมดับเพลิงหนีไฟ ให้มีการซักซ้อมอย่างน้อยปีละ ๑ ครั้ง

๔.๓. จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์แม่ข่ายเพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

๕. เกิดจากอุณหภูมิและความชื้น ได้ติดตั้งระบบเครื่องปรับอากาศแบบควบคุมความชื้น (Precision Air Conditioning Unit) ซึ่งจะปรับเปลี่ยนการทำงานของเครื่องปรับอากาศให้เหมาะสมอยู่ตลอดเวลา ด้วยระบบการควบคุมปริมาณลมของพัดลมชนิดปรับค่าได้ด้วยการควบคุมทางอิเลคทรอนิกส์ (Electrical Commuted Fan, EC Fan) และได้ติดตั้งระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detector System) โดยการตรวจจับจะใช้สายเคเบิ้ลในการตรวจจับซึ่งเมื่อเกิดการรั่วซึมของน้ำเข้ามาในพื้นที่จะทำการตรวจจับและแจ้งเตือนผ่านทางชุด Control ทันที

๖. เกิดจากการโจรกรรม การขโมยอุปกรณ์ ได้ติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) เพื่อควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย โดยจำแนกและกำหนดพื้นที่การติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) เป็น ๓ ส่วน โดยส่วนที่ ๑ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) บริเวณทางเข้าศูนย์คอมพิวเตอร์ส่วนที่ ๒ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และส่วนที่ ๓ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) ห้อง Facility เพื่อจุด

ประสงค์ในการควบคุมการเข้าออกของบุคคลภายนอกโดยใช้เทคโนโลยีระบบ Biometric Finger Scan และ Proximity Card มีการติดตั้งระบบกล้องวงจรปิดและอุปกรณ์บันทึกภาพ เพื่อจุดประสงค์ในการเฝ้าระวังควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

๗. เกิดจากการบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล มีการดำเนินการดังนี้

๗.๑. สแกนหาจุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยการใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

๗.๒. ติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๗.๓. ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตของกรมและกลั่นกรองข้อมูลที่มาทาง website ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๗.๔. ติดตั้ง IDS/IPS เพื่อใช้ในการตรวจจับการบุกรุกของผู้ที่ไม่ประสงค์ดี ซึ่งจะทำการวิเคราะห์ข้อมูลทั้งหมดที่ผ่านเข้า-ออกภายในเครือข่ายที่มีลักษณะการทำงานเป็นความเสี่ยง

๗.๕. ไม่ให้ผู้ใช้ นำอุปกรณ์ Wireless มาติดตั้งเปิดใช้เอง ไม่ว่าจะเป็น Access Point, Wireless Router หรือ Wireless Card เพราะผู้ใช้ส่วนใหญ่จะติดตั้งแค่ให้สามารถใช้งานได้เท่านั้น โดยไม่รู้ว่าเป็นทางผ่านให้ Hacker เข้ามาในระบบ Network

๘. เกิดจาก Hardware อุปกรณ์คอมพิวเตอร์ชำรุด อุปกรณ์คอมพิวเตอร์ถูกทำลายโดยสภาพแวดล้อมหรืออุปกรณ์คอมพิวเตอร์หมดอายุหรือเกิดจากกระบวนการจัดซื้อไม่ได้มาตรฐาน ส่งผลให้การทำงานด้านข้อมูลหยุดชะงัก ไม่สามารถให้บริการข้อมูลได้ ดังนั้นจึงควรมีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ ติดตั้งเครื่องคอมพิวเตอร์และServer ในสถานที่มั่นคงปลอดภัยและมีการเลือกใช้อุปกรณ์คอมพิวเตอร์ที่มีคุณภาพดีได้มาตรฐาน ทันสมัย

๙. เกิดจาก Software และข้อมูลสูญหาย Software ระบบปฏิบัติการไม่สามารถใช้งาน เกิดจากมีไวรัสเข้าสู่ระบบ มี Hacker/Spyware, หนอนอินเตอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan horse) หรือมี Software รบกวนการทำงานสามารถสร้างความเสียหายต่อระบบฐานข้อมูลได้ จึงเห็นควร มีการดำเนินการดังนี้

๙.๑. มีการตรวจสอบการทำงานของระบบปฏิบัติการอยู่เสมอ

๙.๒. มีการติดตั้งระบบป้องกันไวรัส / ไฟร์วอล ที่ทันสมัย

๙.๓. มีการจำกัดสิทธิในการเข้าใช้ระบบงานข้อมูล

๑๐. เกิดจากระบบเครือข่าย Internet ขัดข้อง อาจเกิดจากระบบแม่ข่ายล่ม มีผู้ใช้บริการจำนวนมาก มีผลให้การทำงานของระบบหยุดชะงักไม่สามารถให้บริการข้อมูลได้ จึงเห็นควร มีการดำเนินการดังนี้

๑๐.๑. ให้เจ้าหน้าที่ด้านเทคนิคตรวจสอบการทำงานของระบบเครือข่าย

๑๐.๒. มีการตรวจสอบบำรุงรักษาช่องสัญญาณเครือข่ายเดือนละ ๑ ครั้ง

**การกำหนดแบ่งอำนาจหน้าที่ผู้รับผิดชอบ**

การกำหนดแบ่งอำนาจหน้าที่ มีวัตถุประสงค์เพื่อลดความเสี่ยงด้านโครงสร้างพื้นฐาน ซึ่งมีแนวทางปฏิบัติดังนี้ คือ ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ ในส่วนการพัฒนาระบบงานออกจากบุคลากรที่ทำหน้าที่บริหารระบบ ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริงและต้องจัดให้มีการระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคน ภายในกลุ่มเทคโนโลยีสารสนเทศอย่างชัดเจนเป็นลายลักษณ์อักษร ซึ่งควรจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญ เพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น โดยกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

**๑. ระดับนโยบาย**

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

นายกริชเพชร ชัยช่วย รองอธิบดีด้านมาตรฐานการขนส่งทางน้ำ ทำหน้าที่ CIO กรมเจ้าท่า

นางชนินทร วรวนาวงศ์ ผู้อำนวยการสำนักแผนงาน

**๒. ระดับปฏิบัติ**

๒.๑. รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ

| | | |
|---|---|---|
| นางสาววิศัลยา | ปานเจริญ | หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ |
| นายอิทธิพล | พูลเขตร์กิจ | นักวิชาการคอมพิวเตอร์ชำนาญการ |

๒.๒. รับผิดชอบดูแลบำรุงรักษา ระบบเครื่อง ระบบเครือข่ายและการสำเนาฐานข้อมูล

| | | |
|---|---|---|
| นายอนุรักษ์ | จอมแปงทา | เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน |
| นายบดีณัฐ | นันทวัน ณ อยุธยา | เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน |
| นายมนตรพล | ลาชะเกตุ | เจ้าหน้าที่เครื่องคอมพิวเตอร์ |
| นายศิริศักดิ์ | นพศรี | เจ้าหน้าที่เครื่องคอมพิวเตอร์ |
| นายสุกฤษณ์ | ซ่อนกลิ่น | เจ้าหน้าที่เครื่องคอมพิวเตอร์ |

มีหน้าที่รับผิดชอบ ดังนี้

๒.๒.๑. ควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์ตามการกำหนดสิทธิการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์

๒.๒.๒. ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย(Server Computer) และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมด

๒.๒.๓. ควบคุม ติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

๒.๒.๔. ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๒.๒.๕. ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๒.๖. ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก

๒.๓. รับผิดชอบในการรักษาความปลอดภัย ระบบสารสนเทศ และระบบฐานข้อมูล

| | | |
|---|---|---|
| นางสาววิศัลยา | ปานเจริญ | หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ |
| นายอิทธิพล | พูลเขตร์กิจ | นักวิชาการคอมพิวเตอร์ชำนาญการ |
| นายอนุรักษ์ | จอมแปงทา | เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน |
| นายบดีณัฐ | นันทวัน ณ อยุธยา | เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน |

มีหน้าที่รับผิดชอบ ดังนี้

๒.๓.๑. ทำการสำรองข้อมูลและเรียกคืนข้อมูลของระบบฐานข้อมูลสารสนเทศ (Backup and Recovery)

๒.๓.๒. ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๔. รับผิดชอบในการรักษาความปลอดภัย ระบบอินเตอร์เน็ต

| | | |
|---|---|---|
| นายศุทธ์ธี | คงพารา | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |
| นางสาวพัชรา | แดงวงษ์ | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |
| นายสมโภช | วัฒนไวฑูรย์ชัย | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |
| ว่าที่ร้อยตรีสมพิศ | แกว่นธัญกิจ | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |
| นายกิตติพล | ภาษยะวัตร | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |

๒.๕. รับผิดชอบความปลอดภัยทั่วไป

| | | |
|---|---|---|
| นางสาวรุจิลาภา | เจริญเลิศ | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |
| นางสาวจันทร์เกตุ | เพ็งพานิช | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |
| นางสาวจารุวรรณ | จันทร์กลัด | เจ้าพนักงานธุรการชำนาญงาน |
| นางสาวสมจิต | เลิศธนาภรณ์ | เจ้าพนักงานธุรการชำนาญงาน |
| นางสาวสุธิดา | องค์จิรัฐติกาล | เจ้าพนักงานธุรการชำนาญงาน |

**แผนการซักซ้อมกรณีเกิดปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบฐานข้อมูลและสารสนเทศ**

**๑. แผนการซักซ้อมกรณีเกิดเพลิงไหม้** มีขั้นตอนการดำเนินการดังนี้

กรณีเพลิงไหม้ไม่รุนแรง

๑. ทำการปิดระบบไฟฟ้าหลักของอาคาร

๒. นำอุปกรณ์ดับเพลิง ฉีดพ่นเพื่อระงับไม่ให้ไฟไหม้ลุกลาม

๓. เมื่อสามารถระงับเพลิงไหม้แล้ว ให้ทำการตรวจสอบความเสียหายของอุปกรณ์ พร้อมทำการกู้คืนระบบให้สามารถทำงานได้ตามปกติ

กรณีเพลิงไหม้แบบลุกลาม

๑. ทำการปิดระบบไฟฟ้าหลักของอาคาร

๒. นำอุปกรณ์ดับเพลิง ฉีดพ่นเพื่อระงับไม่ให้ไฟไหม้ลุกลาม

๓. เมื่อสามารถระงับเพลิงไหม้แล้ว ให้ทำการตรวจสอบความเสียหายของอุปกรณ์ พร้อมทำการกู้คืนระบบให้สามารถทำงานได้ตามปกติ

๔. หากตรวจพบอุปกรณ์เกิดความเสียหายและไม่สามารถกู้คืนระบบได้ ให้ทำการประสานงานกับบริษัทผู้รับผิดชอบดูแลอุปกรณ์ที่เสียหาย เพื่อดำเนินการแก้ไขให้สามารถใช้งานได้ตามปกติ

**๒. แผนการซักซ้อมกรณีตรวจพบการถูกเจาะระบบฐานข้อมูลและสารสนเทศ**

ตรวจสอบ Log Server (IPS)

๑. ผู้โจมตีทำการ phf Attack เข้ามา

๒. ระบบตรวจจับการบุกรุกจะทำการคัดลอกข้อมูลทุกๆ Packet ที่วิ่งอยู่บนเน็ตเวิร์ค

๓. ระบบจะทำการประกอบ Packet ทุกๆ Packet เข้าด้วยกัน เพื่อทำการตรวจสอบ

๔. ทำการเปรียบเทียบ Packet ที่ประกอบแล้ว ว่ามีลักษณะเป็นความพยายามในการบุกรุกหรือไม่

๕. ระบบจะทำการแจ้งเตือนโดยผ่านจอภาพ หรือผ่านอิเล็กทรอนิกส์เมล์

๖. ผู้ดูแลระบบโดยเจ้าหน้าที่เครื่องคอมพิวเตอร์ของ ทส. ทำการตรวจสอบและปิดช่องทางการบุกรุก

## แผนปฏิบัติในการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

**๑. การเตรียมการเบื้องต้น**

**๑) รายละเอียดระบบสารสนเทศ** เพื่อให้ระบบสารสนเทศของกรมเจ้าท่าสามารถดำเนินงานได้อย่างต่อเนื่อง จึงได้มีการเตรียมการจัดทำรายละเอียดของระบบสารสนเทศต่าง ๆ เพื่อใช้ในการตรวจสอบความถูกต้องรายละเอียด และที่มาของอุปกรณ์ต่าง ๆ แสดงรายละเอียดใน **ภาคผนวก ก.**

**๒) การสำรองข้อมูล (Back up)** เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น เมื่อข้อมูลถูกทำลาย หรือเสียหาย โดยสามารถนำข้อมูลสำเนากลับมาใช้งานได้ มีการตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย โดยมีการสำรองข้อมูลผ่านโปรแกรม Symantec Backup Exec ตัวอย่างขั้นตอนการสำรองข้อมูล แสดงใน **ภาคผนวก ข.**

**๓) การกู้ข้อมูล (Recovery)** แสดงใน **ภาคผนวก ข.**

(๑) ทำการทดสอบ Recovery ข้อมูล โครงสร้างและโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้ทำการสำรองไว้

(๒) ทำการทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูลและระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้ทำการสำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

**๔) การป้องกันไวรัสคอมพิวเตอร์** มีการติดตั้งซอฟแวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย ผู้ใช้งานต้องระมัดระวังในการใช้งานคอมพิวเตอร์ โดยเฉพาะเมื่อเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้ มีวิธีป้องกันดังนี้

(๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมป้องกันไวรัส
- อัพเดตข้อมูลไวรัส (Signature) อยู่เสมอ
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

(๒) ระวังภัยเมื่อเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ เช่น แผ่นดิสก์ แผ่นซีดี เป็นต้น

- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์หรือดาวน์โหลดไฟล์ที่มีนามสกุลแปลก ๆ ที่ไม่รู้จัก หรือน่าสงสัย เช่น *.pif ,*.exe, *.com, *.scr ,*.cmd, *.bat, *.hta, *.reg, *.vbs, *.wsc, *.wsf, *.wsh
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

(๓) ใช้ความระมัดระวังในการเปิด E-mail

- อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

(๔) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet

- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น ICQ MSN
- ไม่ควรเข้า website ที่แนะนำจาก E-mail ที่ไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลด ไฟล์ จาก website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่าง ๆ อย่างสม่ำเสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

(๕) ไม่ใช้ E-mail ของกรม ไปใช้นอกเหนือจากวัตถุประสงค์ที่กรมกำหนด

**๕) การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง** เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ

(๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) โดยทั่วไประยะเวลาในการสำรองไฟฟ้าประมาณ ๒๐ - ๓๐ นาที

(๒) เปิดเครื่องสำรองไฟฟ้า ตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์

(๓) เครื่องสำรองไฟฟ้าการอยู่ในสภาพพร้อมใช้งานเสมอ

(๔) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และทำการปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

**๖) มีระบบป้องกันไฟไหม้** โดยมีระบบป้องกันไฟไหม้ติดตั้งที่ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย รวมทั้ง มีอุปกรณ์ดับเพลิงติดตั้งในทุกอาคาร และได้กำหนดแนวทางปฏิบัติดังนี้

(๑) ไม่กระทำการใด ๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

(๒) ศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

(๓) กำหนดหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบดูทางออกฉุกเฉินไม่ปิดตาย และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย

(๔) เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้ จากนั้นออกจากอาคารแล้วโทรศัพท์แจ้งหน่วยดับเพลิง โทร.๑๙๙ หรือ แจ้ง ๑๖๖๙

(๕) ถ้าเพลิงไหม้ในห้องทำงานให้หนีออกมาแล้วปิดประตูห้องทันที รีบแจ้งหน่วยดับเพลิงทันที

(๖) ถ้าเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนจะหนีออกมาให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อย ๆ เปิดประตู แล้วหนีไปยังทางหนีไฟฉุกเฉินทันที

(๗) เมื่อต้องเผชิญกับควันไฟที่ปกคลุม ให้ใช้วิธีคลานหนีไปทางฉุกเฉิน เพราะอากาศบริสุทธิ์ จะอยู่ด้านล่าง

(๘) ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

**๗) การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์** เป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

(๑) มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย โดยมีการติดตั้งเครื่องสแกนลายนิ้วมือ ให้สามารถเข้าได้เฉพาะผู้ที่มีสิทธิเท่านั้น หากจำเป็นจะต้องได้รับอนุญาตจากเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ และมีเจ้าหน้าที่เครื่องคอมพิวเตอร์คอยควบคุมดูแลตลอดหากเจ้าหน้าที่ภายใน หรือเจ้าหน้าที่บริษัทภายนอกมีความจำเป็นต้องเข้าใช้งานจะต้องลงรายละเอียดการขอเข้าใช้ห้องโดยมีแบบฟอร์มบันทึกการใช้งาน เช่น บันทึกชื่อผู้ขอเข้าใช้, ชื่อบริษัท, เบอร์โทรศัพท์ติดต่อกลับ และบันทึกรายละเอียดการใช้งานทุกครั้ง รวมทั้งภายในห้องมีการติดตั้งระบบกล้องวงจรปิดด้วย

(๒) ติดตั้ง Firewall ป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต เข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ ของกรม

(๓) ติดตั้งระบบ Antivirus Gateway ป้องกันไวรัส/เวิร์ม และสแปมเมล์ ตั้งแต่ปี ๒๕๕๑ ซึ่งสามารถกลั่นกรองไวรัส/เวิร์ม และสแปมเมล์ ที่มาจากเครือข่ายภายนอกได้ส่วนหนึ่ง ซึ่งเป็นการแบ่งเบาภาระในการบำรุงรักษาเครื่องคอมพิวเตอร์ ระบบเครือข่ายภายใน ที่เกิดปัญหาต่าง ๆ

(๔) ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ต และกลั่นกรองข้อมูลที่มาทาง Website

(๕) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตว่ามีปริมาณมากผิดปกติหรือไม่ หรือมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้หาสาเหตุและการป้องกันต่อไป ระบบเครือข่ายภายในมีการแบ่ง VLAN เพื่อป้องกัน Packet ที่จะเกิดการ Broadcast หรือเกิดการรบกวนกันภายในเครือข่าย

(๖) การเรียกใช้ระบบสารสนเทศของหน่วยงานต่าง ๆ ทั้งในส่วนกลาง และส่วนภูมิภาค ผู้ใช้ระบบจะต้องบันทึกชื่อผู้ใช้ (User name) และรหัสผ่าน (password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้

(๗) การจัดหา ระบบ IPS/IDS เพื่อนำมาใช้ในการตรวจสอบ และป้องกันผู้บุกรุกจากภายนอกในระดับที่ละเอียดมากขึ้น สามารถเฝ้าดู กลั่นกรองข้อมูล หรือ Packet ที่มีลักษณะพฤติกรรมผิดปกติที่ถูกส่งมาจากภายนอก ซึ่ง IPS จะปิดกั้น (drop packet) นั้น ๆ ไม่ให้ผ่านเข้ามาในเครือข่ายภายในของหน่วยงาน และจะส่งข้อความแจ้งเตือนให้ผู้ดูแลระบบทราบ

**๘) การจัดเตรียมอุปกรณ์ที่จำเป็น** ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ กลุ่มเทคโนโลยีสารสนเทศ ได้จัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็น ดังนี้

(๑) แผ่น boot disk

(๒) แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

(๓) แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

(๔) แผ่นโปรแกรม antivirus/spyware

(๕) แผ่น driver อุปกรณ์ต่างๆ

(๖) ระบบสำรองไฟฉุกเฉิน

**๙) การบำรุงรักษาเครื่อง** เนื่องจากเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เป็นระยะเวลานานมักจะเกิดปัญหาเครื่องทำงานช้าลง การเปิดโปรแกรมต่าง ๆ ไม่ทำงาน ทั้งนี้เนื่องจากการสะสมของไฟล์ที่เรียกว่าขยะ ทำให้การค้นหาไฟล์ที่ต้องการนานขึ้น อีกทั้งยังเป็นช่องทางหนึ่งที่ไวรัสคอมพิวเตอร์ต่าง ๆ จะแทรกเข้ามาให้เครื่องแล้วก่อให้เกิดความเสียหาย ซึ่งมีวิธีป้องกัน ดังนี้

(๑) การทำ Disk Cleanup ซึ่งเป็นการใช้งานโปรแกรมของ windows เองเป็นตัวจัดการไฟล์ขยะที่อยู่ในระบบ ลบทิ้งออกไปทำให้เนื้อที่ของ Hard disk เพิ่มขึ้น การประมวลผลของระบบก็จะเร็วขึ้น

(๒) การ Check Disk เป็นการเช็คสภาพ Hard disk ยังสามารถใช้งานได้ดีอยู่หรือไม่ และยังสามารถกันส่วนที่เสียหายไม่ให้เป็นอุปสรรคต่อการใช้งาน (Bad Sectors)

(๓) การทำ Defragment เป็นการจัดเรียงข้อมูลไม่ให้กระจัดกระจาย ยากต่อการสืบค้นข้อมูลและการเปิดโปรแกรมเพื่อใช้งาน

**๒. กรณีเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย**

๑) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๒) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว อีกทั้งในห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย มีการติดตั้งระบบป้องกันอัคคีภัย เมื่อเกิดควันไฟ จะมีเสียงกระดิ่งแจ้งเตือนรวมทั้งมีการส่งข้อความแจ้งเตือนผ่านโทรศัพท์มือถือ

๓) รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๔) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๕) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

**๓. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์** ให้ดำเนินการดังนี้

๑) ดาวน์โหลดโปรแกรม NOD๓๒ License (กรมเจ้าท่า) ที่เว็บไซต์ http://www.md.go.th/IT/

๒) ติดตั้งโปรแกรม NOD๓๒ License

๓) ใช้งานโปรแกรม NOD๓๒

รายละเอียดการดำเนินงานแสดงใน **ภาคผนวก ค**

**๔. กรณีเครื่องคอมพิวเตอร์ลูกข่ายที่ส่วนภูมิภาคใช้งานไม่ได้**

กรมเจ้าท่าเชื่อมต่อเครือข่ายของกระทรวงคมนาคมด้วยระบบ MOT NET ซึ่งหน่วยงานในส่วนภูมิภาคสามารถใช้งานระบบสารสนเทศผ่านระบบเครือข่าย MOT NET ได้ กรณีหน่วยงานในส่วนภูมิภาค ประสบกับเหตุทำให้ไม่สามารถใช้ระบบสารสนเทศ หรืออาจเกิดความเสียหายกับเครื่องลูกข่าย กรมฯมีโปรแกรมตรวจสอบและแก้ไขจากระบบ Remote ทางไกล (VNC) บริการ โดยมีขั้นตอนการติดตั้งโปรแกรม VNC ดำเนินการดังนี้

๑) ดาวน์โหลดโปรแกรม VNC

๒) ติดตั้งโปรแกรม VNC

รายละเอียดขั้นตอนดำเนินการแสดงใน **ภาคผนวก ง**

**๕. กรณีระบบสารสนเทศล่ม**

กรมฯ ไม่ได้รับสนับสนุนด้านงบประมาณบำรุงรักษาระบบเป็นสาเหตุหนึ่ง ที่ทำให้การใช้งานคอมพิวเตอร์มักเป็นปัญหา **ภาคผนวก จ** แสดงการแก้ปัญหากรณีระบบสารสนเทศล่ม

**๖. กรณีพิมพ์ Passbook แบบฉุกเฉิน**

กรณีหน่วยงานไม่สามารถพิมพ์หนังสือ Passbook จากระบบคนประจำเรือ หรือระบบทะเบียนเรือได้ กลุ่มเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดเตรียมแนวทางในการดำเนินการ โดยเรียกพิมพ์จากโปรแกรมประมวลผลคำแทน (Microsoft Word) รายละเอียดดังแสดงใน **ภาคผนวก ฉ**

**๗. การกำหนดนโยบายการใช้เครื่องคอมพิวเตอร์และเครือข่าย**

วินัยการใช้เครื่องคอมพิวเตอร์และเครือข่าย สามารถช่วยให้การใช้งานโดยรวมเป็นไปอย่างมีประสิทธิภาพ กรณีกำหนดนโยบายในการใช้เครื่องคอมพิวเตอร์และเครือข่าย จะทำให้การใช้งานเป็นไปอย่างมีระเบียบเรียบร้อย และเกิดประโยชน์สูงสุด ในเดือนสิงหาคม ๒๕๕๒ รองอธิบดีด้านความปลอดภัย ผู้รับผิดชอบเทคโนโลยีสารสนเทศระดับสูง (CIO) ได้ให้ความเห็นชอบตามนโยบายการใช้เครื่องคอมพิวเตอร์และเครือข่ายที่กลุ่มเทคโนโลยีสารสนเทศเสนอ (หนังสือที่ คค ๐๓๐๗.ทส/๐๐๙๑๐ ลงวันที่ ๑๑ สิงหาคม ๒๕๕๒) ดังแสดงใน **ภาคผนวก ช**

**๘. การดำเนินการตามแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ (IT Contingency Plan) และการวิเคราะห์ ทบทวนสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ**

ตามที่กรมฯ ได้นำระบบฐานข้อมูลและระบบสารสนเทศมาใช้ในการปฏิบัติงาน และให้บริการประชาชน ซึ่งหากระบบเกิดความเสียหายจะส่งผลต่อการปฏิบัติงานต่างๆ ภายในกรมฯ ดังนั้นจึงต้องให้ความสำคัญในการบริหารความเสี่ยงด้านระบบฐานข้อมูลและสารสนเทศ และได้ดำเนินการจัดทำแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ (IT Contingency Plan) ตั้งแต่ปี ๒๕๕๑ โดยทบทวนทุกปี และปฏิบัติตามแผนฯ อย่างต่อเนื่องซึ่งได้กำหนดไว้ ๔ ขั้นตอน ดังนี้

(๑) ปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ และรายงานผล

(๒) วิเคราะห์ ทบทวนสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ

(๓) หาแนวทางการป้องกันสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ และแนวทางแก้ไข เมื่อเกิดสถานการณ์ที่ส่งผลให้ระบบสารสนเทศเสียหาย เพื่อใช้เป็นข้อมูลในการปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(๔) ดำเนินการวิเคราะห์ ทบทวนสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ และหาแนวทางการป้องกันสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ และแนวทางแก้ไข เมื่อเกิดสถานการณ์ที่ส่งผลให้ระบบสารสนเทศเสียหาย เพื่อใช้เป็นข้อมูลในการปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ดังแสดงใน **ภาคผนวก ซ**

**๙. แผนการบำรุงรักษาเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง และการแก้ไขปัญหาระบบงาน ในส่วนกลาง**

ปัจจุบันกรมเจ้าท่าได้ดำเนินการพัฒนาระบบสารสนเทศและระบบเครือข่ายเพื่อใช้ภายในหน่วยงานภายในส่วนกลางและส่วนภูมิภาคในการปฏิบัติงานประจำ และให้บริการประชาชนส่งผลให้บุคลากรของกรมเจ้าท่าจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์ในการปฏิบัติงานมากขึ้น หากอุปกรณ์ดังกล่าวเกิดขัดข้อง ไม่สามารถใช้งานได้ จะส่งผลต่อการปฏิบัติงานการให้บริการประชาชน กลุ่มเทคโนโลยีสารสนเทศ เป็นหน่วยงานที่รับผิดชอบโดยตรงในการให้คำปรึกษาเกี่ยวกับระบบงานคอมพิวเตอร์ การตรวจสอบและการแก้ไขปัญหาระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศต่างๆ การซ่อมแซมเครื่องคอมพิวเตอร์ให้สามารถใช้งานได้ตามปกติ การที่จะทำให้ระบบเทคโนโลยีสารสนเทศกรมเจ้าท่าที่ได้

ลงทุนพัฒนาให้สามารถตอบสนองต่อความต้องการของผู้ใช้งาน และผู้บริหารขององค์การได้นั้น จำเป็นอย่างยิ่งที่อุปกรณ์คอมพิวเตอร์ต้องอยู่ในสภาพที่พร้อมใช้งานตลอดเวลา

ดังนั้นกลุ่มเทคโนโลยีสารสนเทศ โดยเจ้าพนักงานเครื่องคอมพิวเตอร์ และเจ้าหน้าที่เครื่องคอมพิวเตอร์จึงได้ดำเนินการจัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และเครือข่ายประจำปี ๒๕๖๒ ขึ้น ดังแสดงใน **ภาคผนวก ฌ**

# ภาคผนวก ก.

รายละเอียดระบบสารสนเทศ

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| ๑ | ระบบทะเบียนเรือ | เป็น Web Based Application สามารถบันทึก แก้ไข เรียกดู สืบค้น จัดทำข้อมูลทั่วไปของแต่ละลำเรือ เมื่อขอจดทะเบียนเรือครั้งแรก รวมทั้งเก็บประวัติการเปลี่ยนแปลงแก้ไขข้อมูลต่างๆ ในใบทะเบียนเรือไทย ใบอนุญาตใช้เรือ สามารถบันทึก แก้ไข ค้นหา ตรวจสอบ และจัดพิมพ์ข้อมูลใบทะเบียนเรือไทย จัดพิมพ์ข้อมูลใบอนุญาตใช้เรือ และใบแทนใบอนุญาตใช้เรือ สามารถคำนวณค่าธรรมเนียมและค่าปรับในแต่ละขั้นตอนได้โดยอัตโนมัติ | ฐานข้อมูล Oracle ๑๑ g | บ.ซีดีจี ซิสเต็มส์ จก. | App server -IBM –X๒๓๕<br>หมายเลขครุภัณฑ์ ๑๓.๑.๕๐/๔๗<br>Database server - IBM –X๒๓๕<br>หมายเลขครุภัณฑ์ ๑๓.๑.๕๐/๔๗<br>(APP ๑ )<br>App server - Sun Fire x๔๑๗๐<br>Database server -Sun Sparce Enterprize M๔๐๐๐ | พัฒนาปี ๒๕๔๖<br>ปรับปรุง ปี ๒๕๕๔ |
| ๒ | ระบบคนประจำเรือ | เป็น Web Based Application สามารถบันทึก แก้ไข เรียกดู สืบค้น จัดทำประวัติของคนประจำเรือแต่ละคน รวมทั้งเก็บประวัติการเปลี่ยนแปลงแก้ไขข้อมูลบางส่วนที่มีผลทางกฎหมาย สามารถทำการต่ออายุหนังสือคนประจำเรือ (Passbook หรือ Seaman Book) การออกใบแทนหนังสือคนประจำเรือ และการแก้ไขหนังสือคนประจำ สามารถจัดทำข้อมูลหนังสือสัญญาและบัญชีคนประจำเรือ รวมถึงการจัดเก็บข้อมูล | ฐานข้อมูล Oracle ๑๑ g | บ.ซีดีจี ซิสเต็มส์ จก. | App server IBM –X๒๓๕<br>หมายเลขครุภัณฑ์ ๑๓.๑.๕๐/๔๗<br>Database server IBM –X๒๓๕<br>หมายเลขครุภัณฑ์ ๑๓.๑.๕๐/๔๗<br>(APP ๑ )<br>App server - Sun Fire x๔๑๗๐<br>Database -Sun Sparce Enterprize M๔๐๐๐ | พัฒนาปี ๒๕๔๖<br>ปรับปรุง ปี ๒๕๕๔ |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| | | ประสบการณ์ การทำงานบนเรือเดินทะเล (Sea Service) ของคนประจำเรือแต่ละคน | | | | |
| ๓ | ระบบประกาศนียบัตร | เป็น Web Based Application สามารถ บันทึก แก้ไข เรียกดู สืบค้น จัดเก็บข้อมูล ตรวจสอบ เงื่อนไขเบื้องต้นของ ประกาศนียบัตรแต่ละชั้น และแต่ละประเภท เช่น การศึกษา หลักสูตรที่ต้องผ่านการ ฝึกอบรม ข้อกำหนดในการเลื่อนชั้น ประกาศนียบัตร สามารถบันทึก แก้ไข ค้นหา ตรวจสอบข้อมูล และจัดพิมพ์ ประกาศนียบัตรของผู้ทำการในเรือประวัติ การได้รับประกาศนียบัตรของผู้ได้รับ ประกาศนียบัตรผู้ทำการในเรือตั้งแต่เริ่ม สมัครครั้งแรก ต่ออายุ เลื่อนชั้น | ฐานข้อมูล Oracle ๑๑ g | บ.ซีดีจี ซิสเต็มส์ จก. | App server IBM –X๒๓๕ หมายเลขครุภัณฑ์ ๑๓.๑.๕๐/๔๗ Database server IBM –X๒๓๕ หมายเลขครุภัณฑ์ ๑๓.๑.๕๐/๔๗ (APP ๑ ) App server - Sun Fire x๔๑๗๐ Database -Sun Sparce Enterprize M๔๐๐๐ | พัฒนาปี ๒๕๔๖ ปรับปรุง ปี ๒๕๕๔ |
| ๔ | ระบบตรวจเรือ | เป็น Web Based Application ในการ ทำงานร่วมกับระบบฐานข้อมูล สามารถ ทั้งบันทึก แก้ไข เรียกดู สืบค้น หรือ แสดงผล สามารถจัดเก็บข้อมูลการตรวจ อนุมัติแบบต่าง ๆ, สามารถจัดเก็บข้อมูล ทั่วไปของการตรวจเรือแต่ละลำ, บันทึก | ฐานข้อมูล Oracle ๑๑ g | บ.ซีดีจี ซิสเต็มส์ จก. | App server IBM –X๒๓๕ หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๘/๔๗ Database server IBM –X๒๓๕ หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๙/๔๗ (APP ๒ ) App server - Sun Fire x๔๑๗๐ | พัฒนาปี ๒๕๔๗ ปรับปรุง ปี ๒๕๕๔ |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| | | แก้ไข ค้นหา ตรวจสอบ และดูประวัติการเปลี่ยนแปลงของข้อมูล, จัดพิมพ์ข้อมูลต่าง ๆ ตามที่ปรากฏในใบแจ้งให้แก้ไขเรือและสมุดบันทึกรายการตรวจเรือ, จัดพิมพ์ใบสำคัญรับรองการตรวจเรือ, คำนวณโครงสร้างเรือ การทรงตัวของเรือ ความแข็งแรงของเรือตามข้อกำหนดของอนุสัญญาระหว่างประเทศ ของ Class NK หรือของบริษัทผู้ผลิตซอฟท์แวร์ที่สอดคล้องได้ | | บ.ซีดีจี ซิสเต็มส์ จก. | Database -Sun Sparce Enterprize M๔๐๐๐ | |
| ๕ | ระบบตรวจการขนส่งทางน้ำ | เป็น Web Based Application สามารถบันทึก แก้ไข เรียกดู สืบค้น หรือ แสดงผล จัดทำเอกสารการปล่อยเรือเข้า-ออก บริเวณท่าเทียบเรือแต่ละแห่ง พร้อมจัดทำเอกสาร Port Clearance สำหรับการอนุญาตให้ปล่อยเรือออกจากท่าเรือได้, จัดทำแผน/ผลปฏิบัติงานประจำเดือน ตรวจตราปราบปรามผู้ละเมิดกฎหมายว่าด้วยการขนส่งทางน้ำ, การขนถ่ายน้ำมันเชื้อเพลิงและวัตถุอันตรายในเขตท่า, การตรวจการเดินเรือ, การตรวจวัดเสียงเรือ/ควัน, การระวังชี้แนวเขตที่ดิน, การประสบอุบัติเหตุ | ฐานข้อมูล Oracle ๑๑ g | บ.ซีดีจี ซิสเต็มส์ จก. | App server IBM –X๒๓๕ หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๘/๔๗ Database server IBM –X๒๓๕ หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๙/๔๗ (APP ๒ ) App server - Sun Fire x๔๑๗๐ Database -Sun Sparce Enterprize M๔๐๐๐ | พัฒนาปี ๒๕๔๗ ปรับปรุง ปี ๒๕๕๔ |

## รายละเอียดระบบสารสนเทศ
## กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| | | ของเรือ, การออกใบรับรองบรรจุภัณฑ์ที่ใช้ในการขนส่งสินค้าอันตราย | | | | |
| ๖ | ระบบนำร่อง | เป็น Web Based Application สามารถบันทึก แก้ไข เรียกดู สืบค้น หรือ แสดงผล สามารถรับคำร้องจากบริษัทตัวแทนเรือ (Agent) ในการจองการใช้บริการนำร่อง, จัดทำการมอบหมายงานนำร่องแก่เจ้าพนักงานนำร่อง, จัดเก็บข้อมูลการนำร่องเข้า-ออกในเขตท่า ข้อมูลการค้ำประกันและจัดเก็บรายได้ สามารถคำนวณค่าจ้างนำร่อง, สามารถจัดทำหรือตรวจสอบทะเบียนคุมของหนังสือค้ำประกัน ใบแจ้งหนี้ วงเงินที่จัดเก็บได้ วงเงินค้างชำระในแต่ละเดือน / ปี จำแนกตามเรือแต่ละลำหรือบริษัทตัวแทนเรือ, จัดเก็บข้อมูลการนำร่องของนิติบุคคลนำร่องเอกชน ตลอดจนข้อมูลการออกใบอนุญาตให้เจ้าพนักงานนำร่องเอกชน | ฐานข้อมูล Oracle ๑๑g | บ.ซีดีจี ซิสเต็มส์ จก. | App server IBM –X๒๓๕ หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๘/๔๗ Database server IBM –X๒๓๕ หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๙/๔๗ (APP ๒ ) App server - Sun Fire x๔๑๗๐ Database -Sun Sparce Enterprize M๔๐๐๐ | พัฒนาปี ๒๕๔๗ ปรับปรุง ปี ๒๕๕๔ |
| ๗ | ระบบสิ่งล่วงล้ำลำน้ำ | เป็น Web Based Application สำหรับการขอและอนุมัติใบอนุญาตกระทำสิ่งล่วงล้ำลำน้ำ, สามารถต่อใบอนุญาตให้ใช้ท่าเทียบเรือ, | ฐานข้อมูล Oracle ๑๑ g | บ.ซีดีจี ซิสเต็มส์ จก. | App server IBM –X๒๓๕ หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๘/๔๗ Database server IBM –X๒๓๕ | พัฒนาปี ๒๕๔๗ ปรับปรุง ปี |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| | | สามารถคำนวณค่าธรรมเนียมและค่าปรับ, สามารถเชื่อมโยงกับระบบ GIS เพื่อระบุตำแหน่ง/พิกัด และรายละเอียดตำบลที่ของสิ่งล่วงล้ำลำน้ำ | | | หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๙/๔๗<br>(APP ๒ )<br>App server - Sun Fire x๔๑๗๐<br>Database -Sun Sparce Enterprize M๔๐๐๐ | ๒๕๕๔ |
| ๘ | ระบบคุณภาพสิ่งแวดล้อม | เป็น Web Based Application สามารถบันทึก แก้ไข เรียกดู สืบค้น หรือแสดงผล สามารถจัดทำข้อมูลทั่วไปของแต่ละท่าเรือและสิ่งล่วงล้ำลำน้ำ เก็บข้อมูลการเปลี่ยนแปลงแก้ไขข้อมูลต่างๆ, สามารถจัดทำรายละเอียดของข้อมูลท่าเทียบเรือต่างๆ ได้ทั้งในรูปแบบ Text file และรูปภาพ, สามารถจัดเก็บข้อมูลการติดตามตรวจสอบคุณภาพสิ่งแวดล้อมของแต่ละท่าเทียบเรือและสิ่งล่วงล้ำลำน้ำ คุณภาพน้ำในแหล่งน้ำ และข้อมูลด้านสิ่งแวดล้อมอื่นๆ, สามารถเปรียบเทียบค่าผลการตรวจสอบคุณภาพสิ่งแวดล้อมกับค่ามาตรฐานคุณภาพสิ่งแวดล้อม, สามารถตรวจสอบท่าเทียบเรือที่ไม่ได้ปฏิบัติตามเงื่อนไขด้านสิ่งแวดล้อม รายงานผลการติดตามตรวจสอบ | ฐานข้อมูล Oracle ๑๐g | บ.ซีดีจี ซิสเต็มส์ จก. | App server IBM –X๒๓๕<br>หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๘/๔๗<br>Database server IBM –X๒๓๕<br>หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๙/๔๗<br>(APP ๒ )<br>App server - Sun Fire x๔๑๗๐<br>Database -Sun Sparce Enterprize M๔๐๐๐ | พัฒนาปี ๒๕๔๗ ปรับปรุง ปี ๒๕๕๔ |

## รายละเอียดระบบสารสนเทศ
## กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| ๙ | ระบบใบเสร็จรับเงิน | เป็นระบบเก็บข้อมูลการจัดเก็บค่าธรรมเนียม/ค่าปรับ เช่น<br>- การรับเงินที่เกิดจากค่าธรรมเนียม/ค่าปรับต่างๆ เช่น การจดทะเบียนเรือ, การต่อใบอนุญาตต่างๆ<br>- การออกใบเสร็จรับเงินต่างๆ เช่น ใบเสร็จรับเงินค่าจดทะเบียนเรือ , ใบเสร็จรับเงินค่าต่อใบอนุญาตใช้เรือ | ฐานข้อมูล Oracle ๑๑ g | บ.ซีดีจี ซิสเต็มส์ จก. | App server IBM –X๒๓๕<br>หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๘/๔๗<br>Database server IBM –X๒๓๕<br>หมายเลขครุภัณฑ์ ๑๓.๑.๑๙๙/๔๗<br>(APP ๒ )<br>App server - Sun Fire x๔๑๗๐<br>Database -Sun Sparce Enterprize M๔๐๐๐ | พัฒนาปี ๒๕๔๗<br>ปรับปรุง ปี ๒๕๕๔ |
| ๑๐ | ระบบข้อมูลเพื่อประกอบการตัดสินใจของผู้บริหารระดับสูง (COGNOS) | สามารถจัดการระบบสารสนเทศในการบริหารงานราชการ , วิเคราะห์ข้อมูลเพื่อประกอบการตัดสินใจที่มีความยืดหยุ่น และปรับเปลี่ยนรูปแบบของการวิเคราะห์ข้อมูลต่างๆได้ตามความต้องการที่เปลี่ยนไป , นำเสนอข้อมูลที่เป็นบทสรุปสำหรับผู้บริหารที่อยู่ในรูปกราฟ ตารางและภาพเคลื่อนไหว , Web Site ศูนย์รวมข้อมูลเพื่อการบริหารงานราชการ, มีคลังข้อมูลรวมของศูนย์ปฏิบัติการกรมฯ และฐานความรู้เพื่อการบริหารราชการ, มีระบบสั่งการ และติดตามผลการดำเนินงานของศูนย์ปฏิบัติการกรมฯ, มีระบบแจ้งเตือนสถานการณ์ที่ | ฐานข้อมูล Oracle๑๑g | Business Application Co,Ltd | Database Server IBM X series ๒๓๕<br>หมายเลขครุภัณฑ์ ๑๓.๑.๗/๔๙ วก. | พัฒนาปี ๒๕๔๙ |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| | | สำคัญแบบอัตโนมัติ, จัดทำแบบจำลองข้อมูลเพื่อประกอบการตัดสินใจ, เชื่อมโยงและแลกเปลี่ยนข้อมูลได้ในระดับตารางข้อมูล | | | | |
| ๑๑ | ระบบบริการข้อมูลข่าวสารและระบบ Internet/intranet | เป็น Web Based Application สามารถทั้งบันทึก แก้ไข เรียกดู สืบค้น หรือ แสดงผลจาก Web Site จัดทำข้อมูลที่ต้องการเผยแพร่แก่สาธารณะ, สามารถค้นหาข้อมูลต่างๆ, เว็บบอร์ด, อีเมล์, ทรัพยากรร่วม, ปฏิทิน, การค้นหาข้อมูลของกรมฯ ที่เผยแพร่ข้อมูลให้สาธารณะ ผ่านระบบเครือข่าย Internet ของกรมฯ | ฐานข้อมูล Oracle | บ.ซีดีจี ซิสเต็มส์ จก. | Acer Altos r๗๒๐<br>หมายเลขครุภัณฑ์<br>๑๓.๑.๑๐๐๐๐๐๐๐๑๘๖๗.๕๑ | |
| ๑๒ | ระบบสารบรรณอิเล็คทรอนิกส์ | เป็น Web Based Application สามารถบันทึกหนังสือ เข้า-ออก และลงทะเบียนหนังสือ ด้วยระบบอิเล็คทรอนิกส์ | ฐานข้อมูล Oracle๑๑g | บ.ซีดีจี ซิสเต็มส์ จก. | Database Server IBM System x๓๖๕๐<br>หมายเลขครุภัณฑ์<br>๑๓.๑.๑๐๐๐๐๐๐๐๓๔๖๑.๕๓<br>App Server IBM System x๓๖๕๐<br>หมายเลขครุภัณฑ์<br>๑๓.๑.๑๐๐๐๐๐๐๐๓๔๖๒.๕๓<br>Report Server IBM System x๓๖๕๐<br>๑๓.๑.๑๐๐๐๐๐๐๐๓๔๖๓.๕๓ | พัฒนาปี ๕๑ |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| ๑๓ | ระบบการประเมินผลสัมฤทธิ์การพัฒนาระบบการขนส่งทางน้ำ (KPI) | จัดเก็บข้อมูลในรูปฐานข้อมูลต่างๆ เช่น ฐานข้อมูลการขนส่งผู้โดยสารทางน้ำ ฐานข้อมูลความพึงพอใจของผู้ใช้บริการ ฐานข้อมูลการเกิดอุบัติเหตุ ฐานข้อมูลปริมาณเรือและสินค้าท่าเรือเชียงแสน/ข้อมูลระดับน้ำในแม่น้ำโขง ฐานข้อมูลร่องน้ำ ฐานข้อมูลเขื่อน ฐานข้อมูลท่าเรือและระบบเชื่อมต่อ ฐานข้อมูลผู้ประกอบการเรือ ฐานข้อมูลผู้ประกอบการท่าเรือ ฐานข้อมูลผู้ประกอบการขนส่งทางน้ำ ฐานข้อมูลเป้าหมายการปฏิบัติงาน ฐานข้อมูลการขนส่งสินค้าทางน้ำ ฐานข้อมูลอู่คานเรือ ฐานข้อมูลแผนและผลการใช้จ่ายเงินงบประมาณ ฐานข้อมูลพัฒนาบุคลากร เพื่อใช้ในการประเมินความสัมฤทธิ์ การพัฒนาระบบการขนส่งทางน้ำตามเป้าหมายการให้บริการของหน่วยงาน | ฐานข้อมูล SQL | บ.ทีไอเอส จำกัด | | |
| ๑๔ | ระบบ DPIS | เป็นซอฟต์แวร์ที่พัฒนาโดย กพ. จัดเก็บข้อมูลต่างๆ ของข้าราชการ เช่น ข้อมูลส่วนบุคคล (ชื่อ-สกุล, เลขบัตรประชาชน, การศึกษา ฯลฯ) , เงินเดือน ,เครื่องราชฯ | ฐานข้อมูล Oracle ๙i | สำนักงาน ก.พ. | Dell Power Edge ๔๖๐๐ หมายเลขครุภัณฑ์ ๑๓-๑-๒๕/๔๖ | |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| | | เป็นต้น สามารถจัดเก็บค้นหา, เปลี่ยนแปลงข้อมูลต่างๆ และจัดทำรายงานได้ | | | | |
| ๑๕ | ระบบอนุสัญญาระหว่างประเทศ | เป็นซอฟต์แวร์ขององค์การทางทะเลระหว่างประเทศ (IMO) จัดเก็บข้อกำหนดกฎเกณฑ์ต่าง ๆ เกี่ยวกับคุณสมบัติของเรือ ซึ่งเป็นไปตามข้อตกลงของอนุสัญญาระหว่างประเทศ ที่สามารถสืบค้นและสอบถามข้อมูลในแง่มุมต่าง ๆ | - | โปรแกรมสำเร็จรูป | | |
| ๑๖ | ระบบ GFMIS | ระบบการจัดสรรงบประมาณ, ระบบบริหาร/ติดตามการใช้งบประมาณ ระบบบัญชีแยกประเภทแบบเกณฑ์คงค้าง, ระบบบัญชีบริหาร/บัญชีต้นทุน, ระบบบัญชีเจ้าหนี้, ระบบบัญชีทรัพย์สินถาวร, ระบบบริหารเงินสด ระบบบริหารทรัพยากรบุคคล | ฐานข้อมูล Oracle ๑๑g | กรมบัญชีกลาง | | |
| ๑๗ | ระบบห้องสมุด ระบบห้องสมุดอัตโนมัติ Lspider ๓.๐ | เป็น Web Based Application สามารถบันทึก แก้ไข เรียกดู สืบค้น ข้อมูลเกี่ยวกับรายละเอียดต่างๆของหนังสือ และข้อมูลข่าวสารต่างๆ ที่มีให้บริหารในห้องสมุด เช่น ชื่อหนังสือ ผู้แต่ง สถานที่พิมพ์ บริษัทที่ | ฐานข้อมูล Oracle ๙i | โปรแกรมสำเร็จรูป | IBM system X๓๕๐๐<br>หมายเลขครุภัณฑ์<br>จอ ๑๓.๘.๑๐๐๐๐๐๐๐๑๙๖๖๕๑<br>เครื่อง ๑๓.๑.๑๐๐๐๐๐๐๐๑๙๖๔.๕๑ | พัฒนาปี ๔๘ |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| | | จัดพิมพ์ ปีที่พิมพ์ สาระสังเขป และเลขเรียกหนังสือ เป็นต้น<br>เป็นโปรแกรมที่ทำงานทั้งในลักษณะ Client/Server เชื่อมต่อกับฐานข้อมูลกลาง และเป็นแบบ Web Based ในการสืบค้นผ่านระบบเครือข่าย ประกอบด้วย ระบบงานด้านวิเคราะห์หมวดหมู่และทำรายการ , ระบบทำรายการสื่อแบบเท็มเพลท , ระบบพิมพ์บาร์โค้ด , ระบบบัตรสมาชิก , ระบบสืบค้นข้อมูลออนไลน์ , ระบบให้บริการยืม-คืนสื่อ , ระบบสร้างคำค้น , ระบบควบคุมสิ่งพิมพ์ต่อเนื่อง และระบบการทำรายงาน | | | | |
| ๑๘ | ระบบ E-learning | เป็นระบบงานเพื่อสร้างศักยภาพในการบริหารจัดการความรู้ใช้ในการสร้างหลักสูตรการเรียนต่างๆ ให้บุคลากรได้เข้าไปเรียนรู้ สามารถใช้ในการฝึกอบรมต่างๆ และสามารถบันทึกบทเรียนได้หลากหลาย เช่น บทเรียนภาษาอังกฤษ, บทเรียนด้าน IT หรือบทเรียนอื่นๆที่กระทรวงกำหนดให้จำเป็นต้องเรียนเพื่อลด Competency Gap | ฐานข้อมูล Oracle ๑๐g, DB๒,Excel | มหาวิทยาลัยรามคำแหง | HP Proliant ML ๓๕๐ | |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| | | เป็นต้น สามารรถกำหนดกลุ่ม แบ่งหลักสูตร สร้างหลักสูตรได้ไม่จำกัด ซึ่งช่วยประหยัดค่าใช้จ่ายในเรื่องการอบรม และสามารถประเมินผลการฝึกอบรมได้เป็นอย่างรูปธรรม | | | | |
| ๒๐ | ระบบบริการสถานศึกษา | สามารถจัดทำประวัติบุคลากร (นักเรียน อาจารย์) การลงทะเบียน การจัดทำแผนการสอน จัดทำตารางสอนและตารางสอบ บันทึกและประมวลผลการสอบ การรับสมัครนักศึกษาใหม่ | ฐานข้อมูล Oracle ๑๑g | บ.ซีดีจี ซีสเต็มส์ จำกัด | | |
| ๒๑ | ระบบ e-Service | เป็นการเชื่อมโยงและบูรณาการบริการในลักษณะแบบเบ็ดเสร็จ ณ จุดเดียว )Single Point of Services หรือ One Stop Service) ในรูปแบบของศูนย์บริการร่วมอิเล็กทรอนิกส์ผ่านระบบเว็บท่าคมนาคม และให้เป็นไปในทิศทางเดียวกัน สามารถสร้างความสอดคล้อง เชื่อมโยง สนับสนุนซึ่งกันและกัน และให้สามารถตอบสนองความต้องการของผู้รับบริการกลุ่มต่างๆ ได้อย่างมีประสิทธิภาพ และประสิทธิผลสูงสุด โดยมีบริการประชาชนในด้านการขนส่งทางน้ำใน | ฐานข้อมูล Oracle Database ๑๒c Standard Edition ONE | บ.ซีดีจี ซีสเต็มส์ จำกัด | Oracle รุ่น SPARC T๕-๒ | พัฒนาปี ๒๕๕๘ |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| ๒๒ | โครงการพัฒนาปรับปรุงระบบคนประจำเรือและระบบประกาศนียบัตรเพื่อรองรับอนุสัญญา STCW และ MLC | ส่วนของกรมเจ้าท่า ผ่านระบบอิเล็กทรอนิกส์ ๔ด้าน คือ ด้านตรวจเรือ ด้านทะเบียนเรือ ด้านคนประจำเรือ และด้านจดทะเบียนผู้ประกอบการพาณิชยนาวี<br><br>เป็นการปรับปรุงระบบคนประจำเรือและระบบประกาศนียบัตร เพื่อรองรับระบบอิเล็กทรอนิกส์ที่ประเทศภาคีสมาชิก STCW และ MLC รวมทั้งบริษัทเจ้าของเรือสามารถตรวจสอบการออกประกาศนียบัตรและสถานะของประกาศนียบัตรต่างๆได้และมีการจำแนกชั้นประกาศนียบัตรผู้ทำการในเรือให้เป็นไปตาม STCWพร้อมทั้งจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่เหมาะสม เพียงพอและมีประสิทธิภาพสำหรับใช้ในการปรับปรุงฐานข้อมูลระบบข้อมูลและสำหรับการปฏิบัติงานของเจ้าหน้าที่เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องมีความรู้และศักยภาพ ในการใช้งานอย่างมีประสิทธิภาพเพื่อการใช้งานโปรแกรมมีความสะดวกรวดเร็วเพิ่มประสิทธิภาพในการปฏิบัติงาน | ฐานข้อมูล Oracle ๑๑g | บ.ซีดีจี ซีสเต็มส์ จำกัด | | พัฒนาปี ๒๕๕๘ |

# รายละเอียดระบบสารสนเทศ
# กรมเจ้าท่า

| ลำดับที่ | ระบบงาน | คำอธิบาย | การจัดเก็บข้อมูล | บริษัท,ผู้พัฒนา | อุปกรณ์ที่ใช้ ,หมายเลขครุภัณฑ์ | หมายเหตุ |
|---|---|---|---|---|---|---|
| ๒๓ | ระบบจัดเก็บเอกสารทะเบียนอิเล็กทรอนิกส์ E-DOC | เป็น Web based Application เพื่อใช้ในการจัดการเอกสารเกี่ยวกับทะเบียนเรือโดยจัดเก็บเอกสารในรูปแบบอิเล็กทรอนิกส์เพื่อลดค่าใช้จ่ายในการจัดเก็บเอกสารแบบ Manual สามารถเรียกดูเอกสารที่ใช้ในการทำรายการต่างๆได้ | ฐานข้อมูล MySQL | บ.ซีดีจี ซีสเต็มส์ จำกัด | Dell PowerEdge R๗๒๐ | พัฒนาปี ๒๕๕๗ |
| ๒๔ | ระบบซอฟต์แวร์ส่วนขยายเพิ่มเติมระบบที่เกี่ยวกับการขนส่งทางน้ำเพื่อรองรับระบบ Transport Single Window e-Logistics | สามารถเชื่อมโยงแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับกระบวนการรับ-ส่งข้อมูลของสายเรือกับระบบ National Single Window e-Logistic ผ่านระบบ Transport Single Window e-Logistic | ฐานข้อมูล Oracle ๑๑b | บ.คอมพิวเตอร์ ยูเนี่ยน จำกัด | HP Proliant DL๓๘๐P Gen ๘ Cloud ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) | พัฒนาปี ๒๕๕๗ ปรับปรุงปี ๒๕๖๐ |
| ๒๕ | ระบบ Single Window ๔ Fishing Fleet | เป็นระบบการออกใบอนุญาตให้ทำการงานในเรือ ตามมาตรา ๒๘๕ แห่ง พระราชบัญญัติการเดินเรือในน่านน้ำไทย พระพุทธศักราช ๒๕๔๖ ด้วยระบบอิเล็กทรอนิกส์ | ฐานข้อมูล SQL | บริษัท อานเซอร์ เซอร์วิส จำกัด | Cloud ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) | พัฒนาปี ๒๕๖๐ |

# ภาคผนวก ข

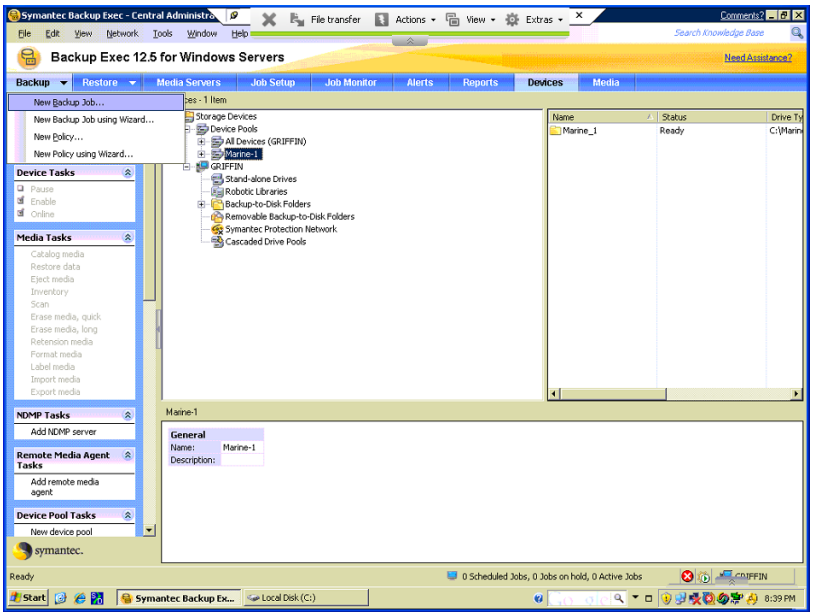
การสำรองข้อมูล (Back up)การกู้คืนระบบ (Recovery)

# การสำรองข้อมูล (Back up)

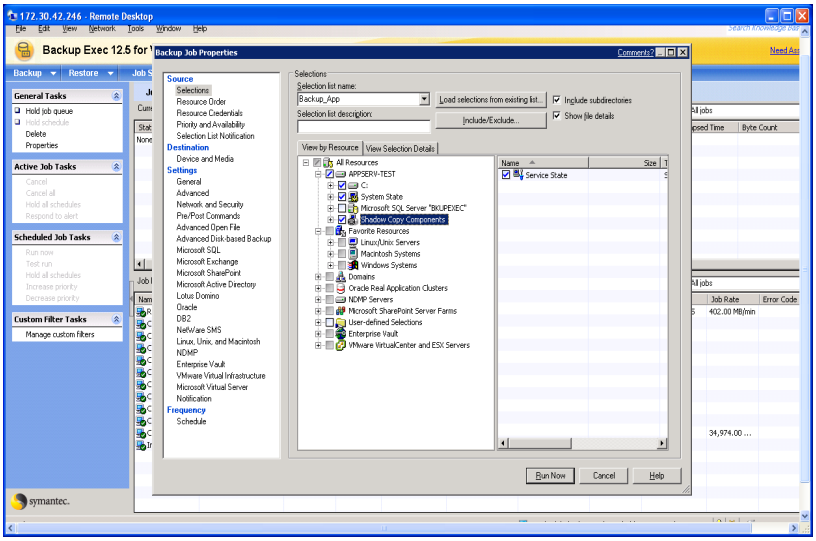
## การสำรองข้อมูล และการกู้คืนระบบ

### ๑. Create Job Back up System State

๑.๑เปิด Program Symantec Backup Exec



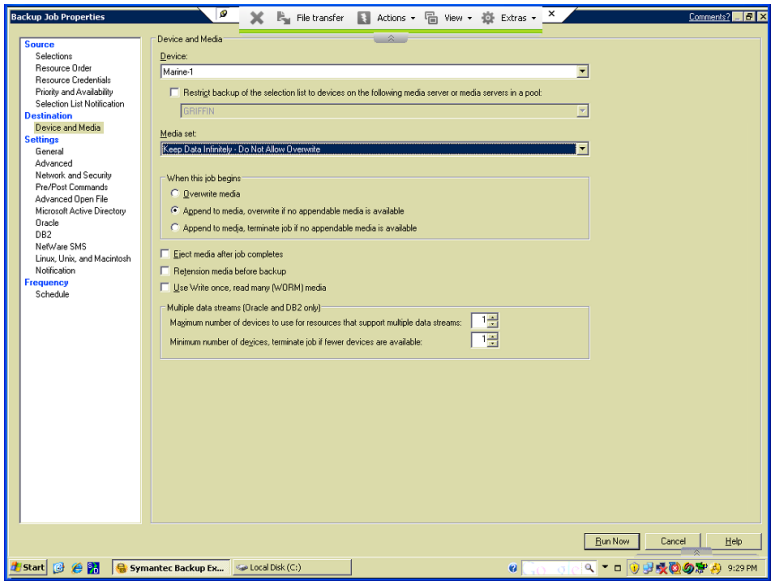

๑.๒เลือก Tab “ Backup ” แล้วเลือก “ New Backup Job”



๑.๓หัวข้อ  Source  เลือก Selections จะแสดง list ในช่อง Selections ด้านขวา

- เลือก Selection list names = ตั้งชื่อสำหรับทำการ Backup

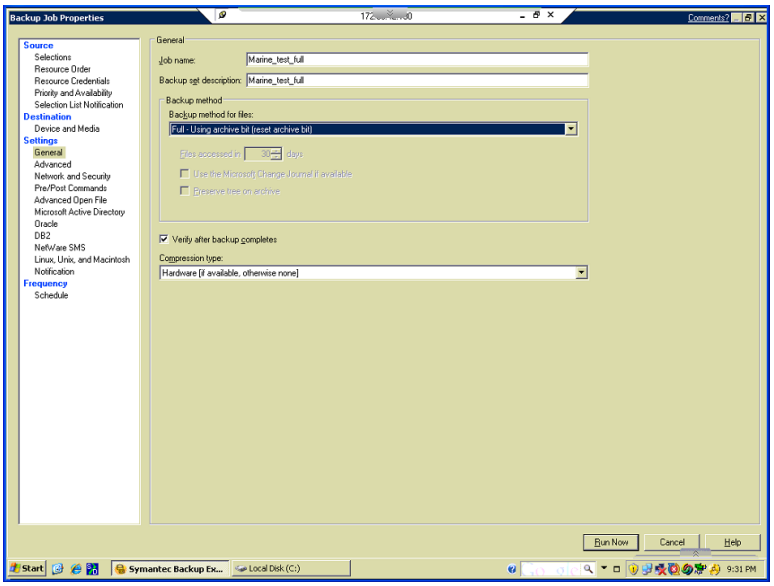
- เลือก Viwe by Resource = ทำการเลือก Backup Drive C ,System State ,Shadow Copy Components




๑.๔หัวข้อ Destination เลือก Device and Media จะแสดง list ในช่อง Device and Media ด้านขวา

- เลือก Device  = เลือก Device ที่ต้องการให้ Backup สามารถเลือกเป็น default หรือ กำหนดใหม่

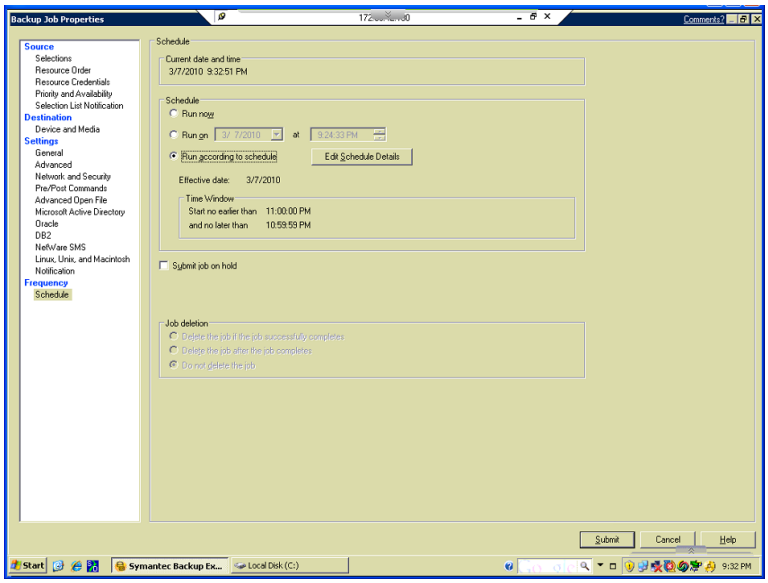
- เลือก Media set = เลือกMedia set ที่ต้องการให้ Backup สามารถเลือกเป็น default หรือ กำหนดใหม่



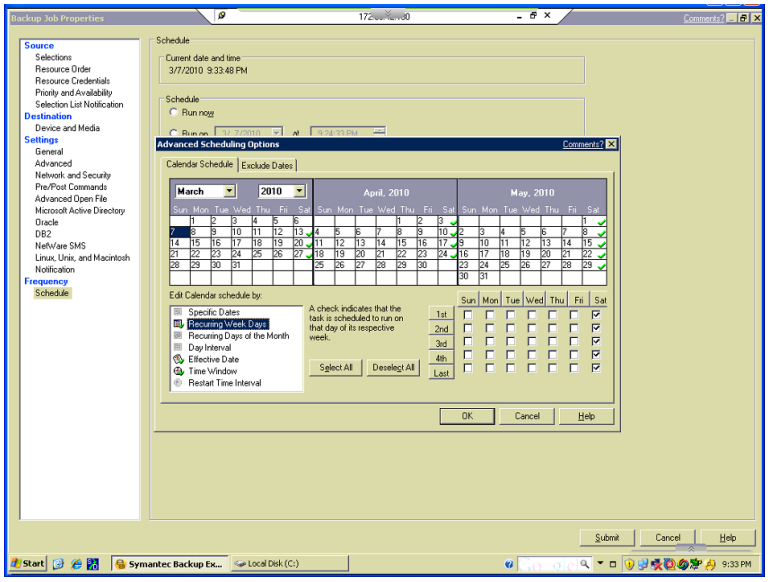
๑.๕หัวข้อ Settings เลือก General

- Job Name = ตั้งชื่อ Job Backup

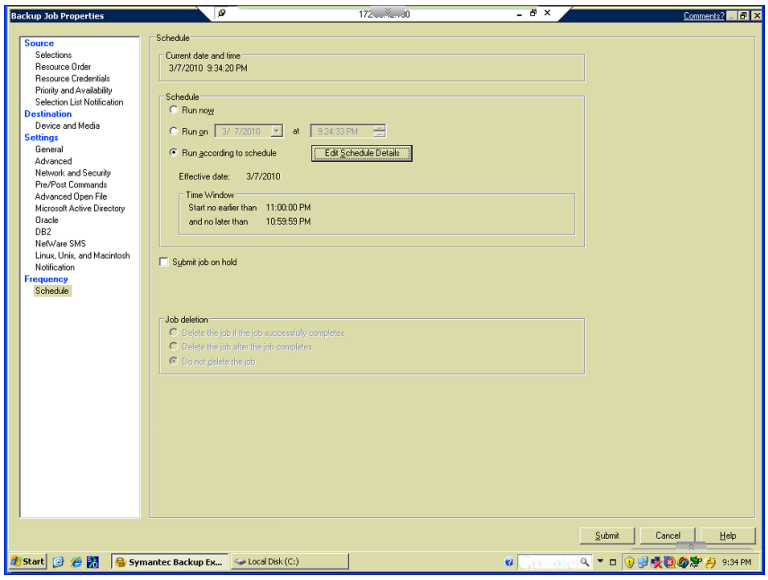
- Backup Method = เ ลือกวิธีการ Backup เป็น Full,Different หรือ Imcremental



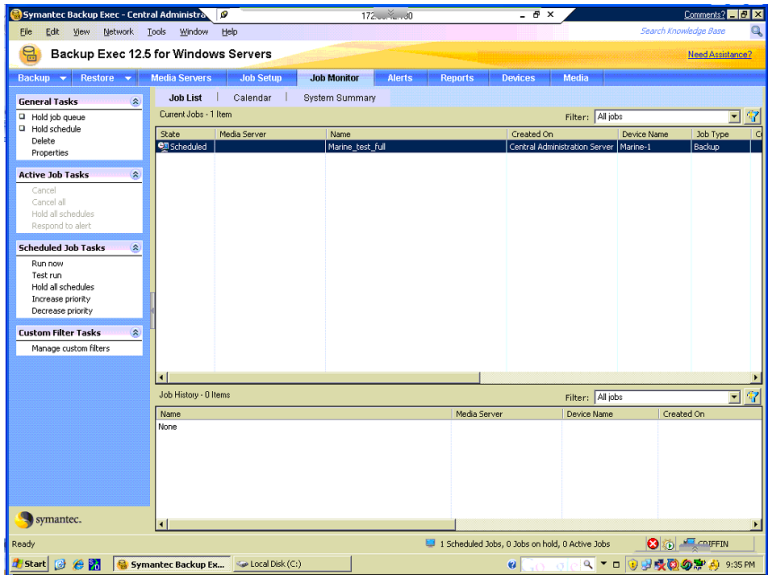

๑.๖หัวข้อ Frequency เลือก Schedule สามารถเลือก Run now เพื่อสั่งให้ทำ Backup โดยไม่ตั้ง Schedule หรือเลือกRun according schedule เพื่อตั้ง วัน,เวลาที่จะให้ Job ทำ Schedule




๑.๗เลือก วัน,เวลา ที่ตั้งการจะให้ Job Backup ทำงาน จากนั้นเลือก OK

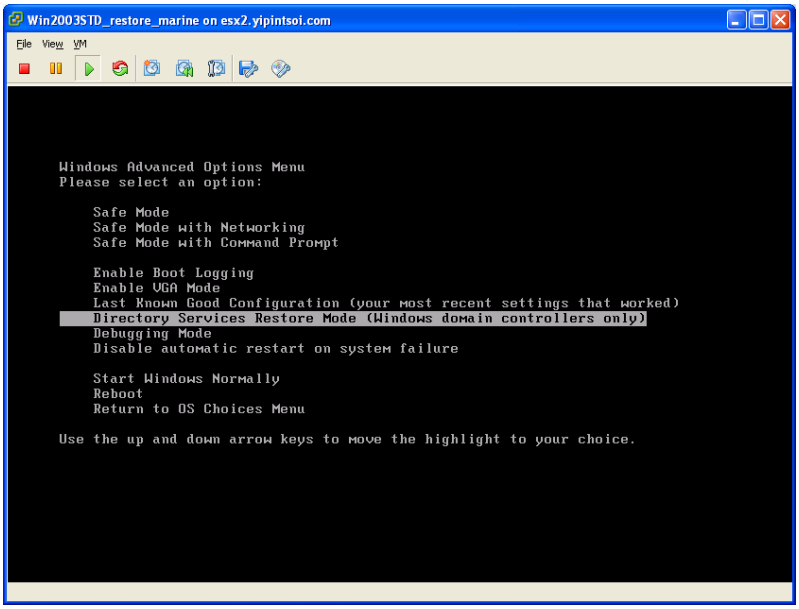



๑.๘ตรวจเช็ค Schedule เมื่อได้วัน,เวลาที่ถูกต้องแล้ว เลือก Submit



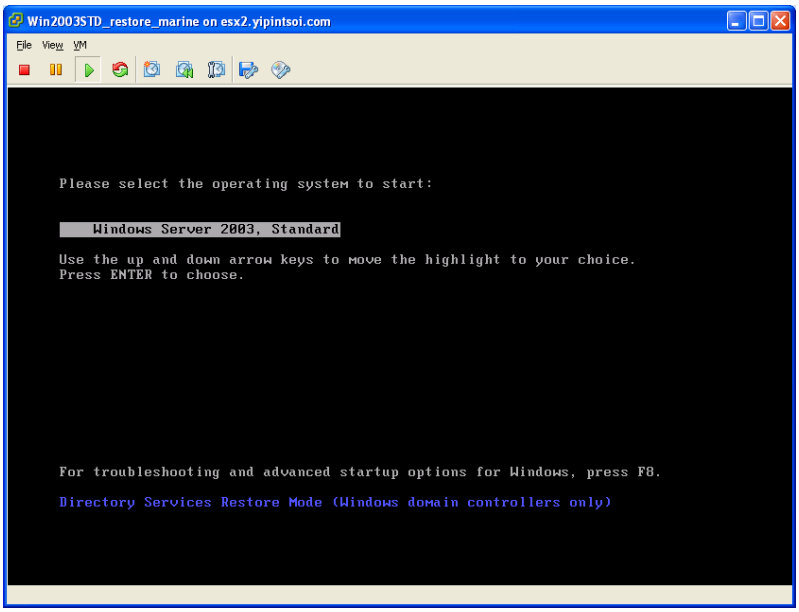

๑.๙ใน Tab “Job Monitor” จะแสดง Job Backup Schedule ขึ้นมา และสามรถทำการแก้ไข Configure ได้โดย Click ขวา เลือก Properties

## ๒. Job Restore System

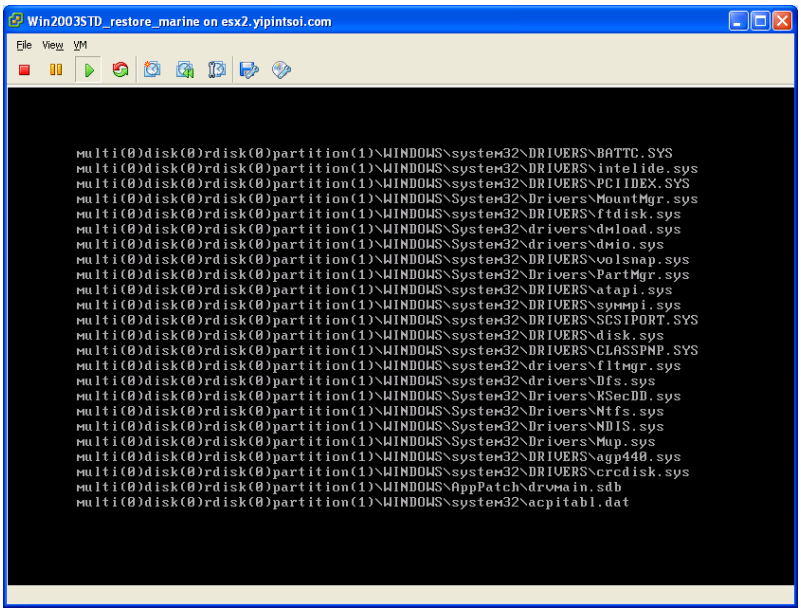



๒. ทำการ Reboot Server กด F๘ เพื่อเข้า “ Windows Advanced Options “

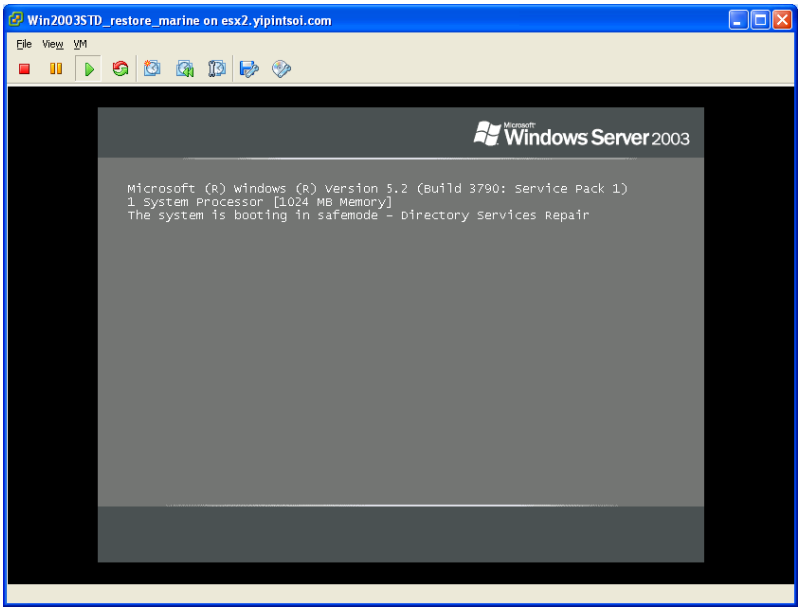
๓. เลือก “Directory Services Restore Mode (Windows domain comtrollers only)”



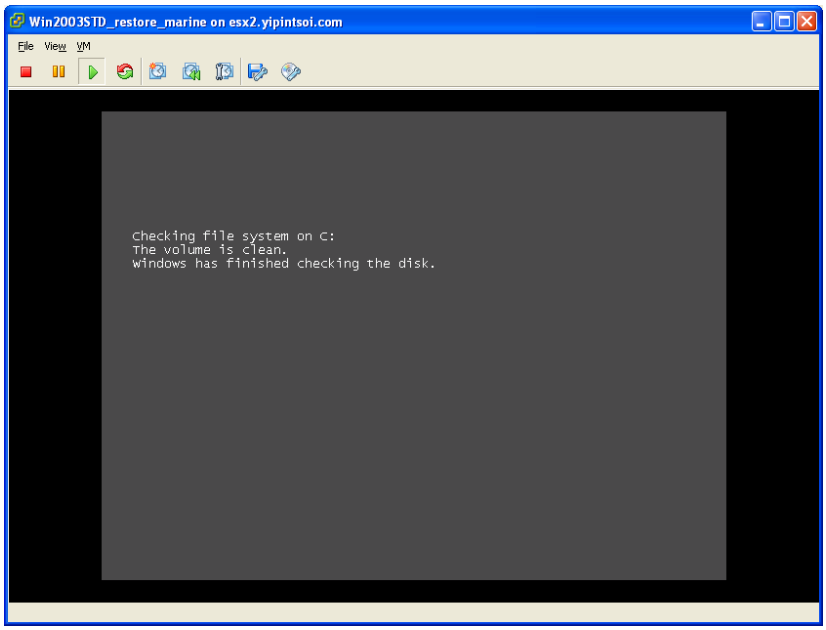

๔. เลือก “ Windows Server ๒๐๐๓ , Standard ”



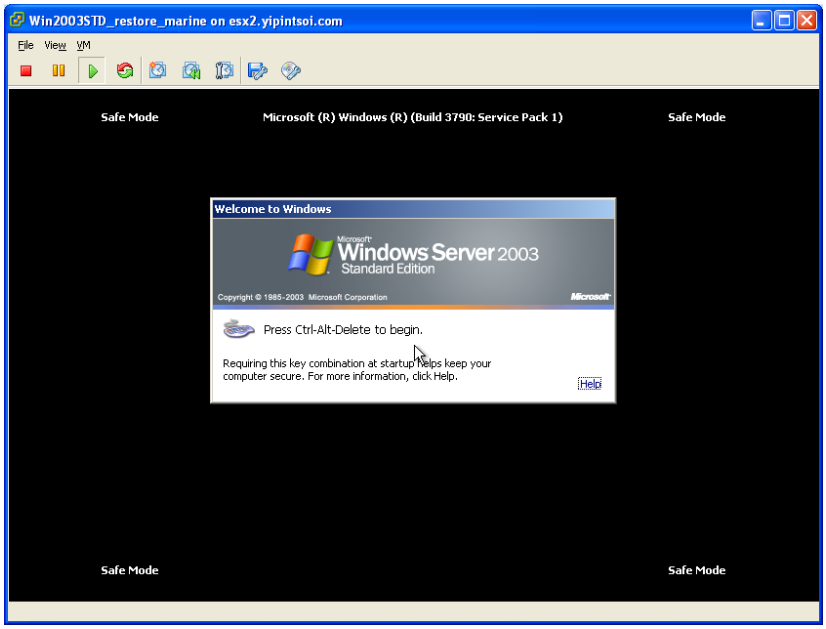

๕. Page แสดงการ Boot เข้าระบบ



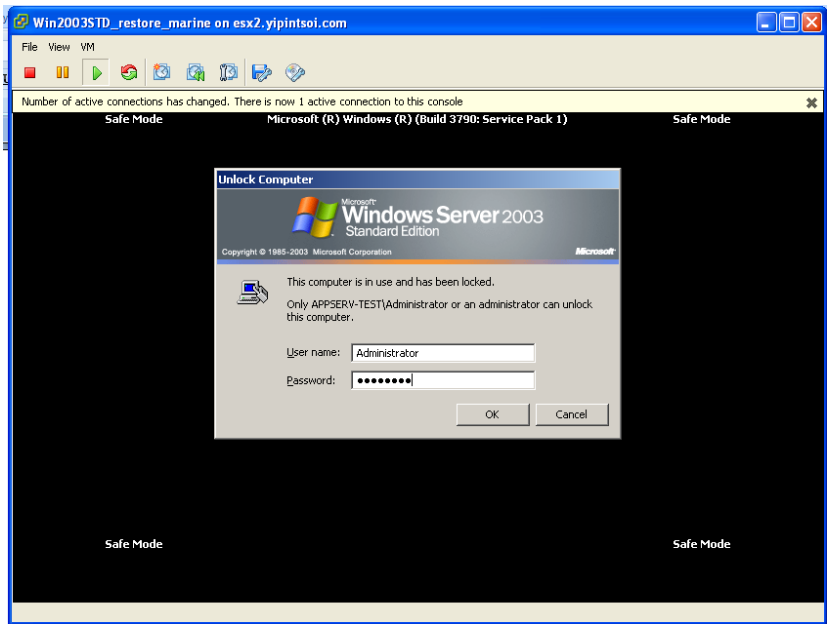

๖. Page แสดง Windows Version




๗. Page แสดง Checking  file system on Drive C

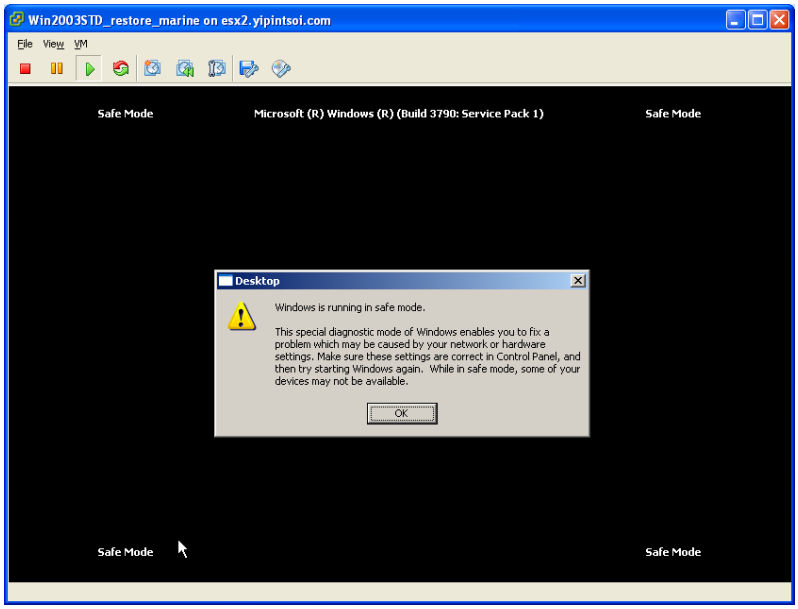



๘. ทำการ Login เข้า Windows

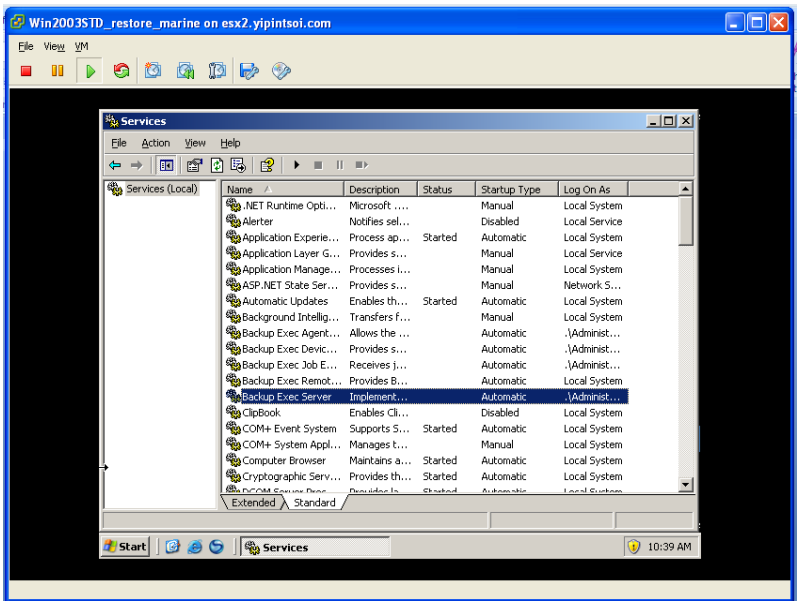



๙. Login User name = Administratos

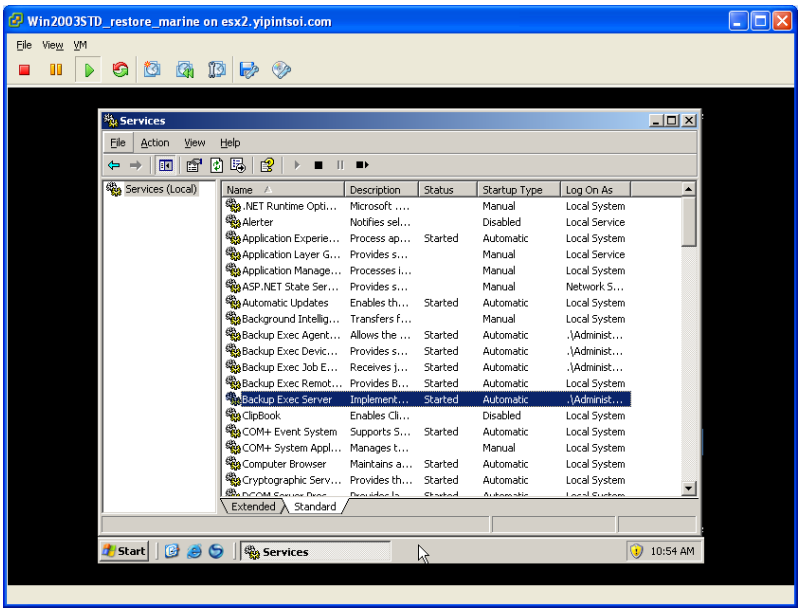
Password = cm&drgdsv๒๐๐๕



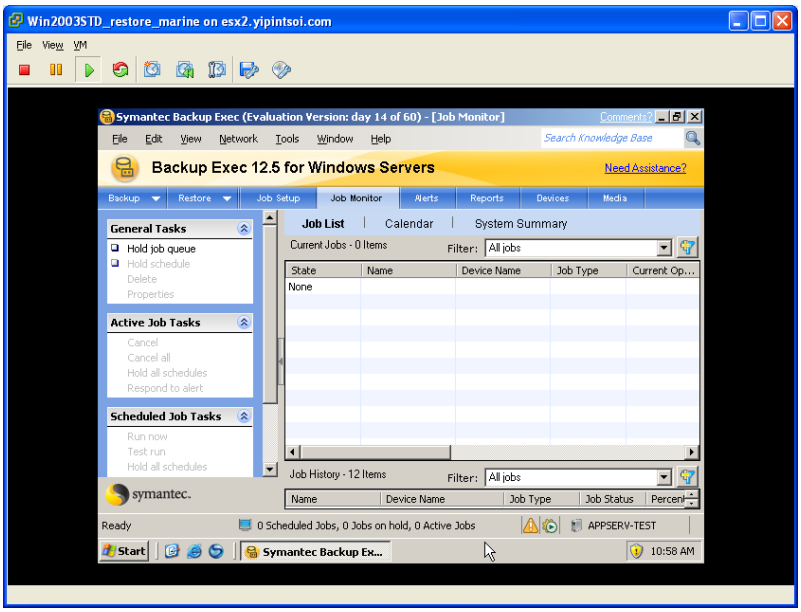

๑๐. Page แสดง Worning ในการเข้า Safe Mode เลือก “ OK “



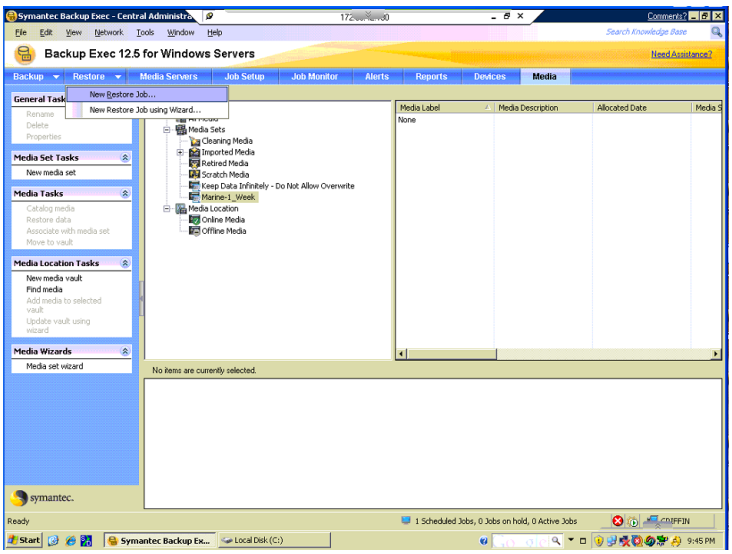

๑๑.เมื่อเข้า Windows ทำการ เปิด windows services เลือกservice ของ Backup Exec



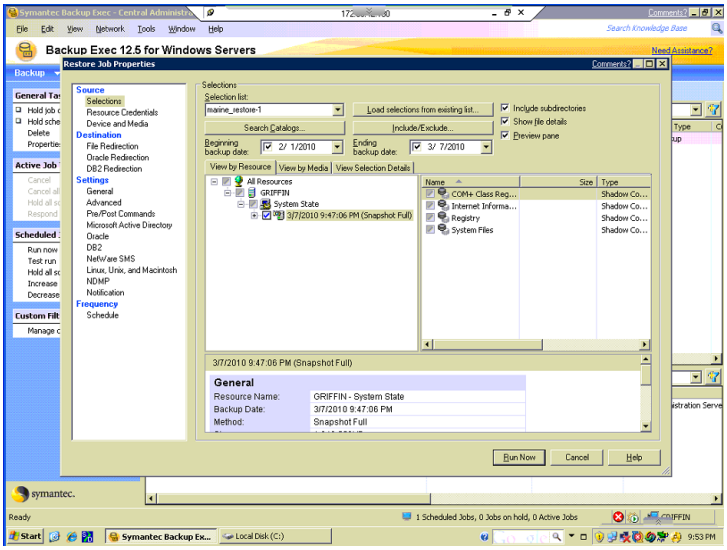

๑๒.ทำการ Start  Services ของ Backup Exec  ให้ครบทุก service




๑๓.เปิก Program Symantec Backup Exec



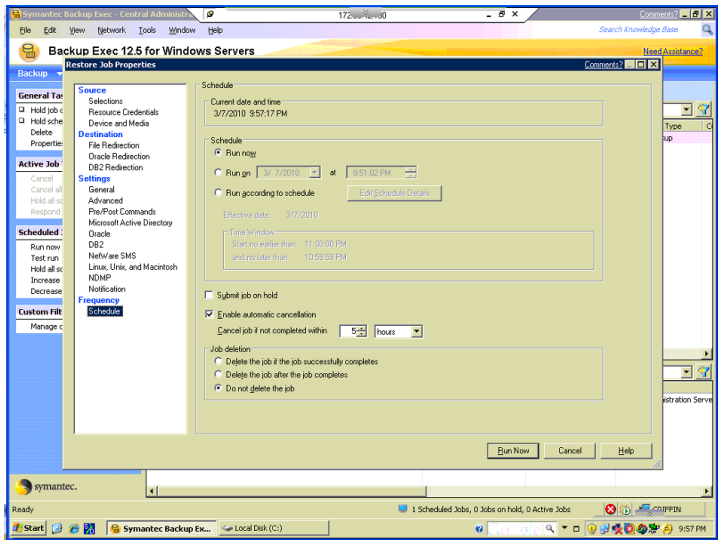

๑๔.เลือกTab เลือก “ New Restore Job ”




๑๕.แสดง Page “Restore Job Properties” หัวข้อ “Source” เลือก “Selections”

- Selection list = ตั้งชื่อ Job Restore

- View by resource = เลือก vertions ของbackup ที่ต้องการ restoreโดยเลือก Drive C , System Stat และ Chadow copy Components

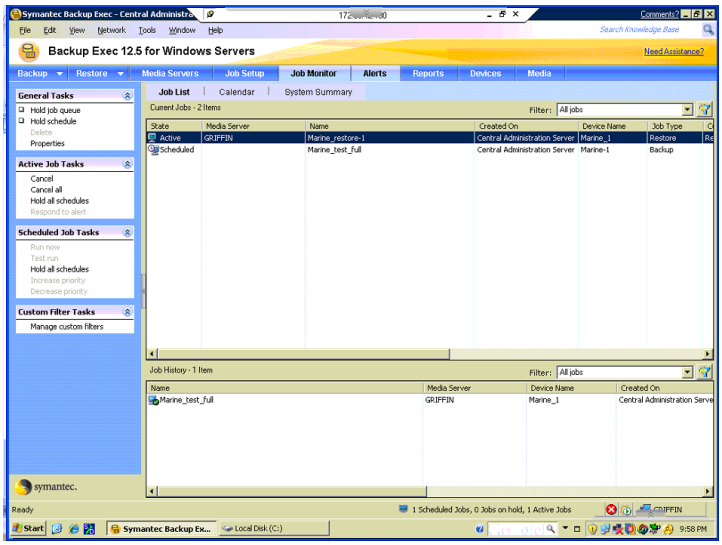



๑๖.หัวข้อ “Frequency” เลือก “Schedule ”

- Run now = เลือกให้ทำ Job Restore ทันที

- Run on = เลือกให้ทำ Job Restore โดยระบุ วัน ,เวลา

- Run according to schedule = เลือกให้ทำ Job Restore ตาม Schedule



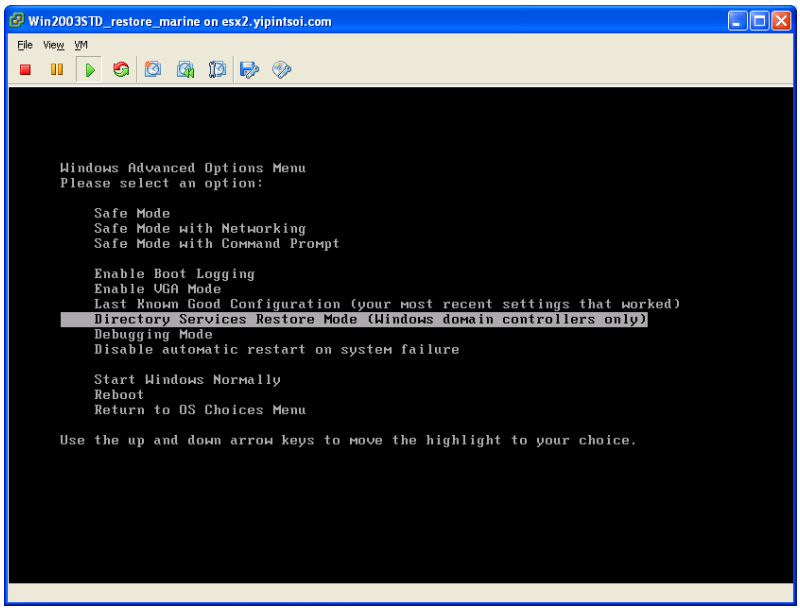

๑๗. Page แสดง Job restore stauts Active

# **การกู้คืนระบบ (Recovery) โดยใช้โปรแกรม** Symantec Backup Exec

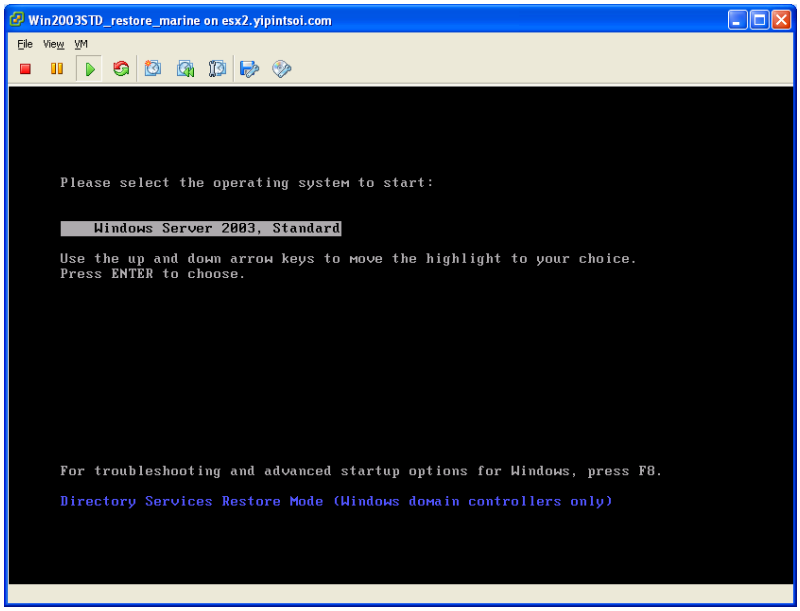
## ๑. Job Restore System

๑. ทำการ Reboot Server กด F๘ เพื่อเข้า “ Windows Advanced Options

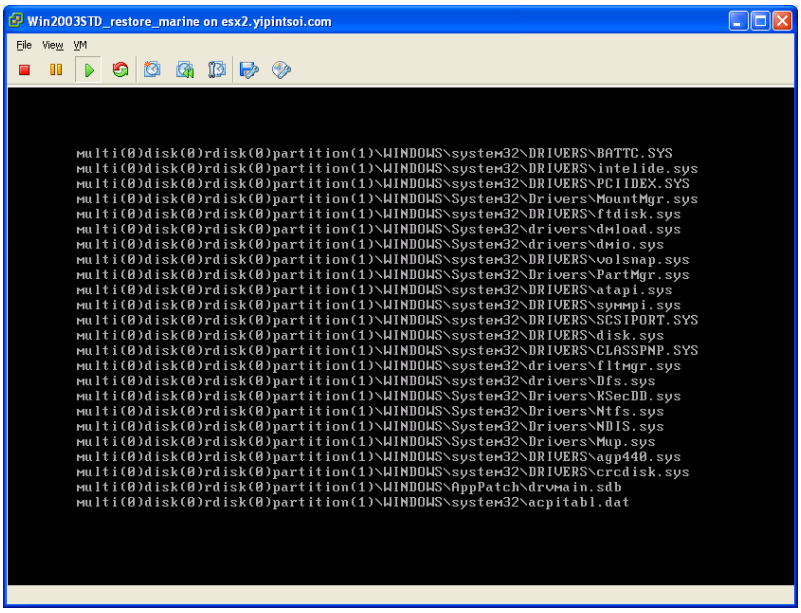
๒. เลือก “Directory Services Restore Mode (Windows domain comtrollers only)”



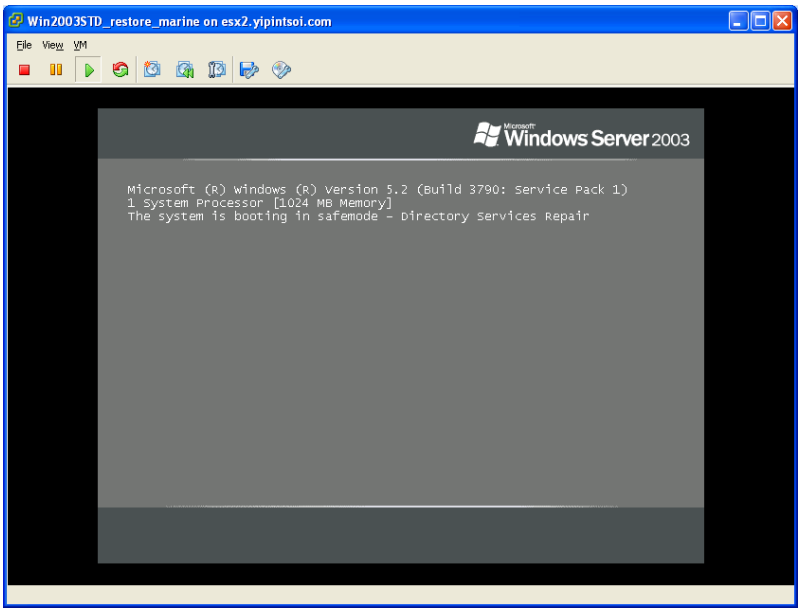

๓. เลือก “ Windows Server ๒๐๐๓ , Standard ”



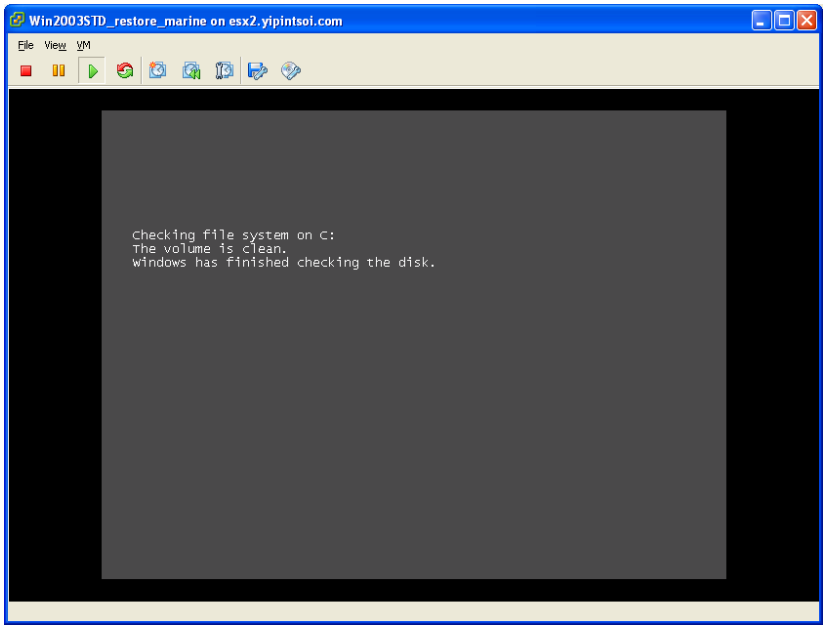
๔. Page แสดงการBootเข้าระบบ



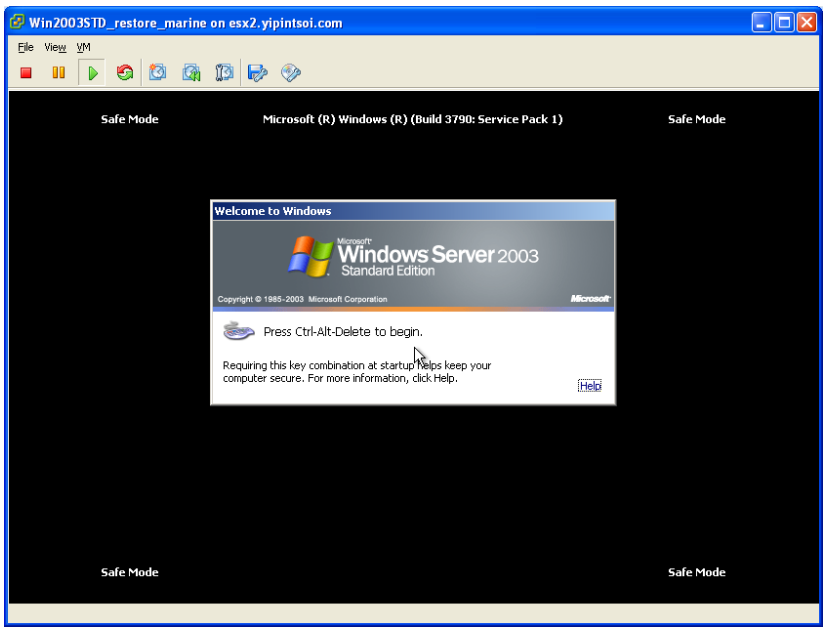

๕. Page แสดง Windows Version

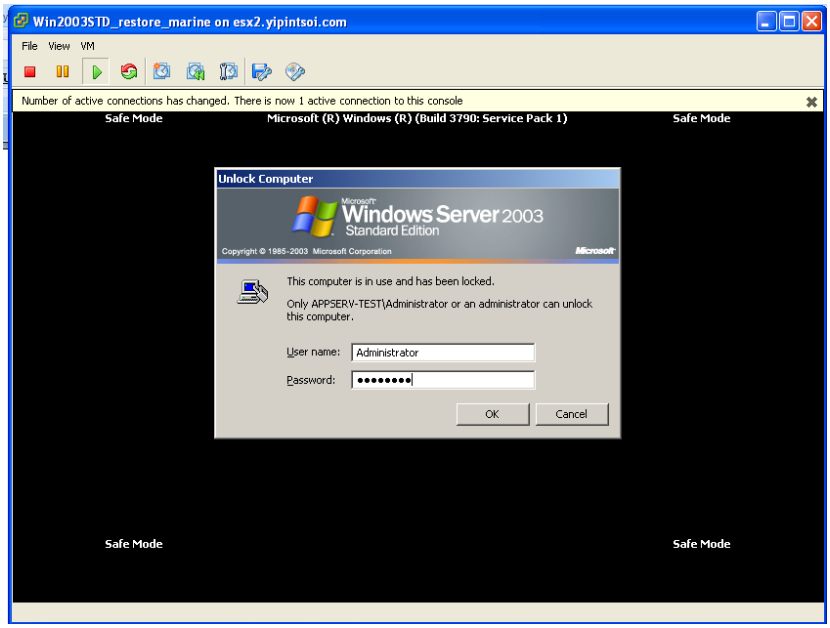


๖. Page แสดง Checking file system on Drive C

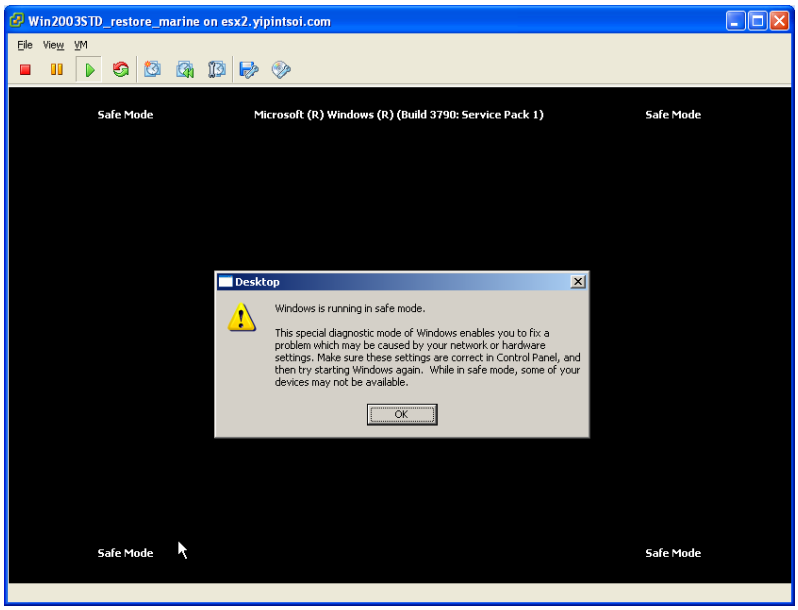



๗. ทำการ Login เข้า Windows

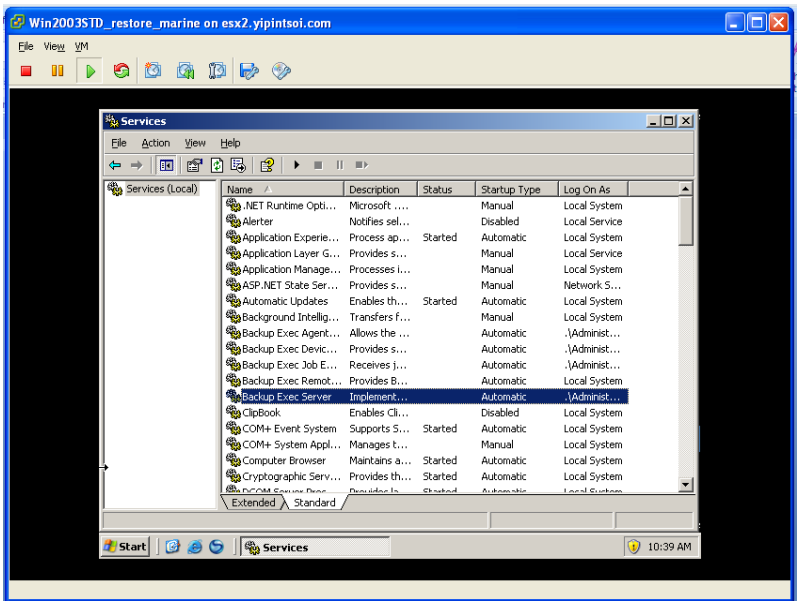




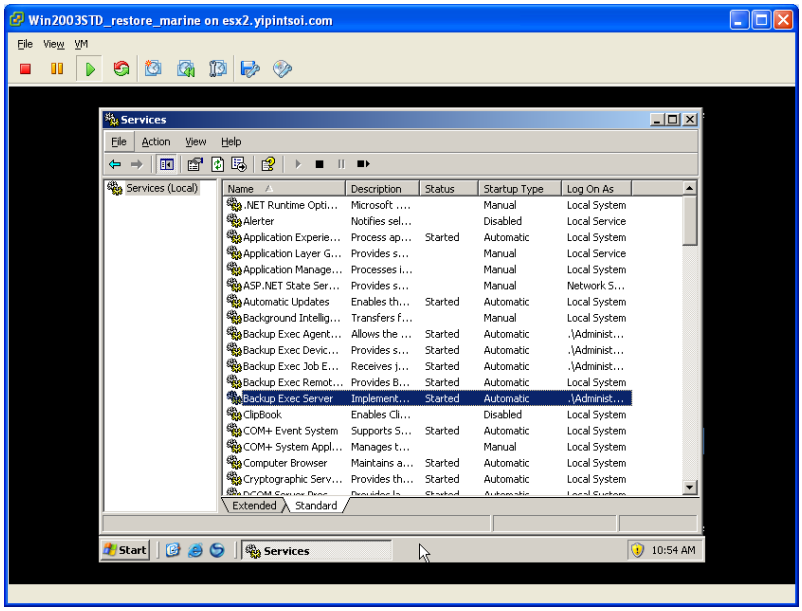

๘. Page แสดง Warning ในการเข้า Safe Mode เลือก “ OK “



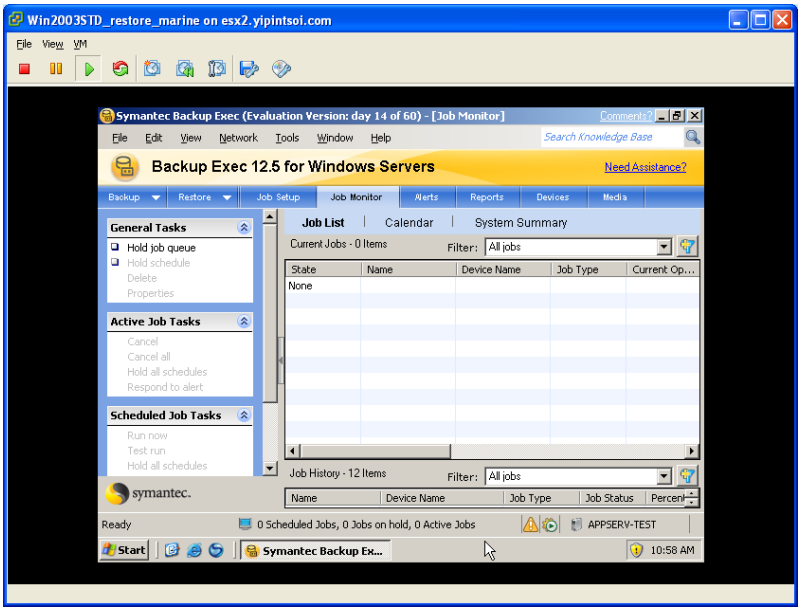
๙. เมื่อเข้า Windows ทำการ เปิด windows services เลือกservice ของ Backup Exec



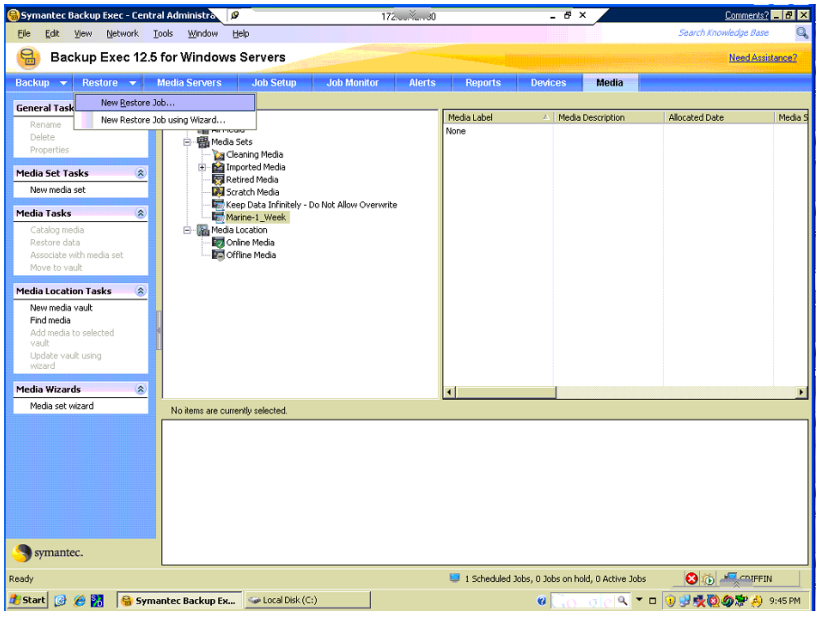

๑๐. ทำการ Start Services ของ Backup Exec ให้ครบทุก service



๑๑. เปิก Program Symantec Backup Exec



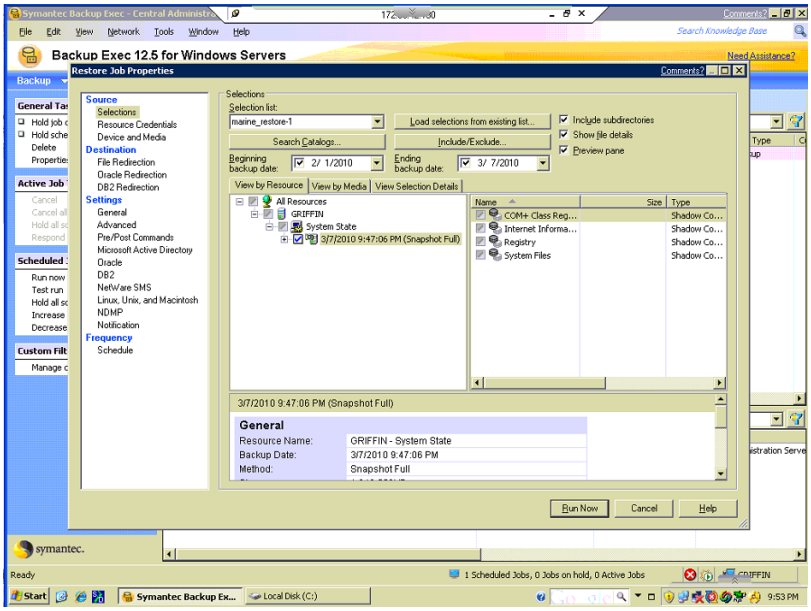

๑๒. เลือกTab เลือก “ New Restore Job ”



๑๓. แสดง Page “Restore Job Properties” หัวข้อ “Source” เลือก “Selections”

- Selection list = ตั้งชื่อ Job Restore

- View by resource = เลือก vertions ของbackup ที่ต้องการ restoreโดยเลือก Drive C , System Stat และ Chadow copy Components

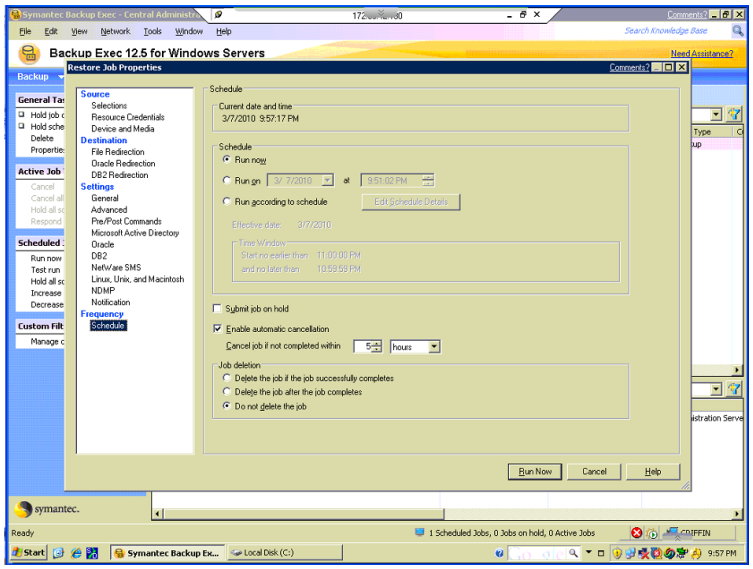



๑๔. หัวข้อ “Frequency” เลือก “Schedule ”

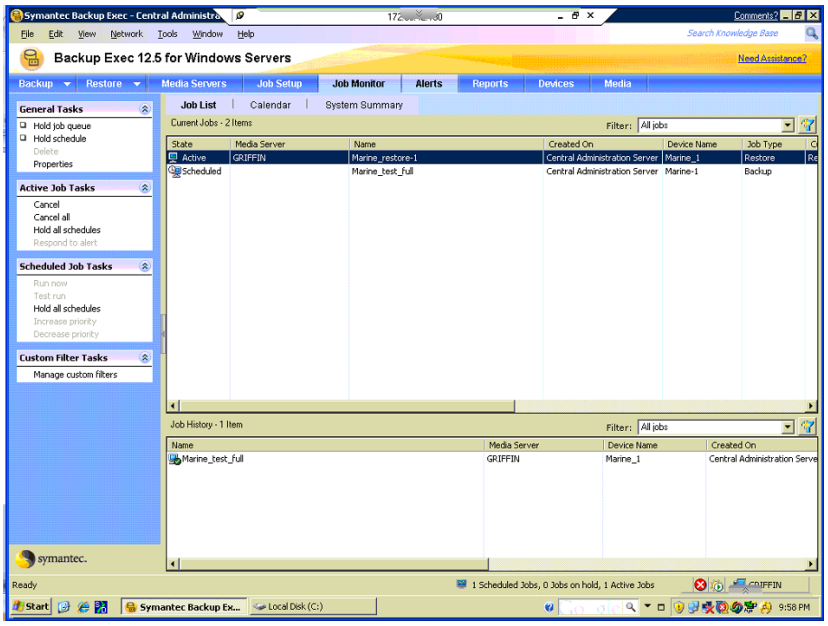
- Run now =เลือกให้ทำ Job Restore ทันที

- Run on =เลือกให้ทำ Job Restore โดยระบุ วัน ,เวลา

- Run according to schedule =เลือกให้ทำ Job Restore ตาม Schedule



๑๕ .Page แสดง Job restore stauts Active



# ภาคผนวก ค

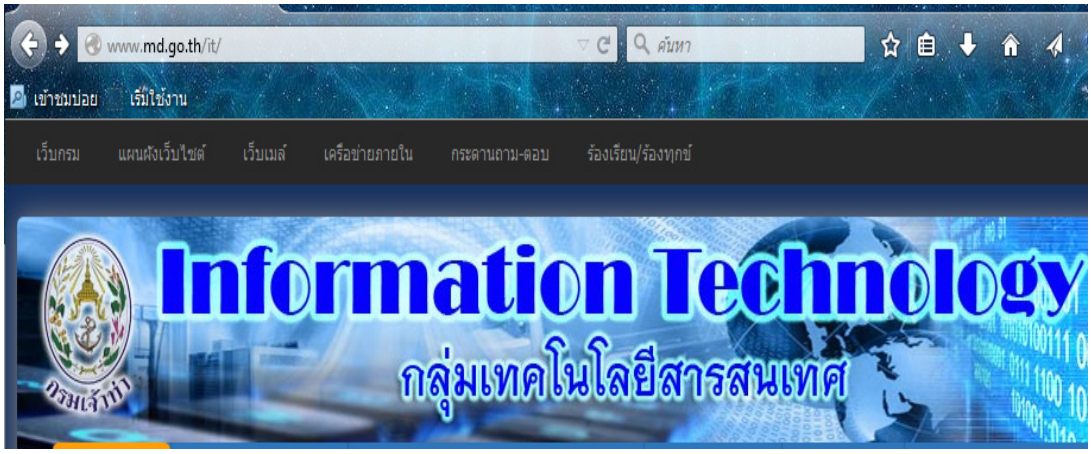
กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์

## กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์

**ปฏิบัติดังนี้**

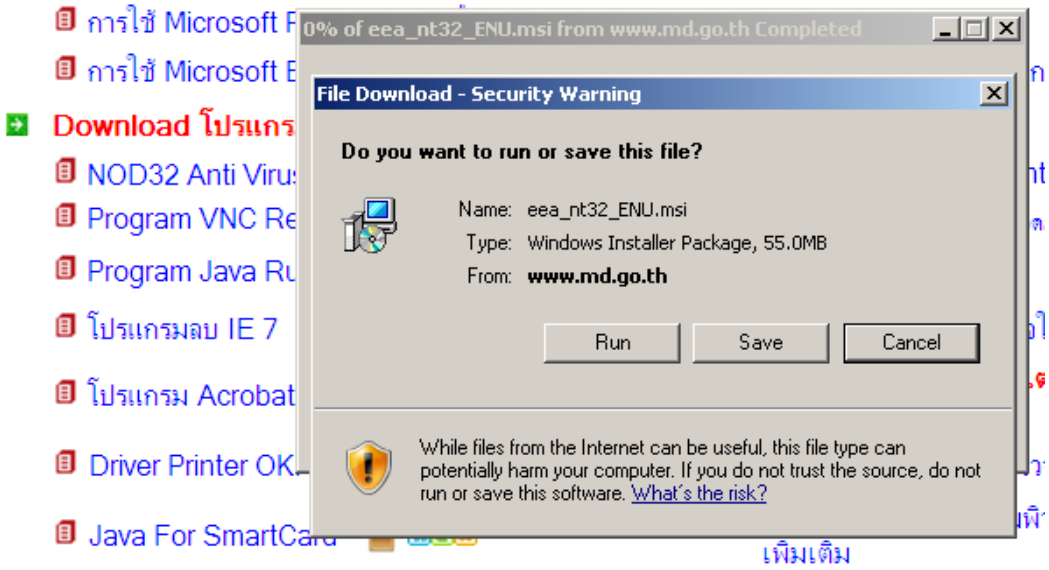
๑. ดาวน์โหลดโปรแกรม ESET Endpoint Antivirus (กรมเจ้าท่า) ดังนี้

- วิธีที่ ๑ เข้าไปยังเว็บไซต์ กรมเจ้าท่า URL คือ http://www.md.go.th กดปุ่ม Enter เพื่อเข้าสู่หน้าหลักเว็บไซต์ กรมเจ้าท่า และไปที่เมนูชื่อ เครือข่ายภายใน ให้เลือกเมนูย่อยชื่อ บริการด้านไอที เพื่อเข้าสู่หน้างานบริการด้านไอที
- วิธีที่ ๒ เปิดใช้งาน Internet Explorer พิมพ์ URL ในช่อง Address: http://www.md.go.th/IT/ แล้วกด Enter เพื่อเข้าสู่หน้า บริการด้านไอที

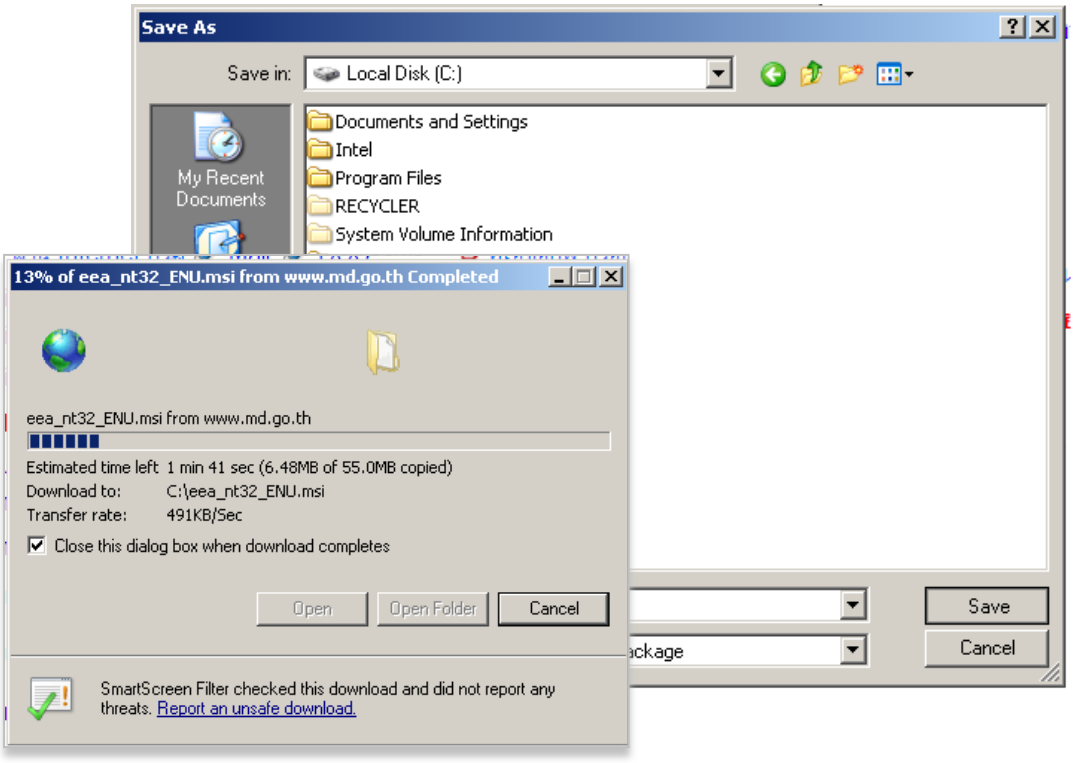



๒. ให้ทำการดาวน์โหลดโดยไปที่หัวเรื่องหลักชื่อ **ดาวน์โหลด** กดปุ่มเลือกที่ หัวข้อย่อยชื่อ โปรแกรมป้องกันไวรัส ESET Endpoint Antivirus ๓๒ เพื่อทำการ Download โปรแกรม

๓. เมื่อกดปุ่มเลือกที่ หัวข้อย่อยชื่อ โปรแกรมป้องกันไวรัส ESET Endpoint Antivirus แล้วจะมีปุ่ม เพื่อทำการ Download โปรแกรม ESET Endpoint Antivirus ในไฟล์ชื่อ Eset32.exe สามารถกดปุ่ม Run เพื่อทำการติดตั้งโปรแกรม หรือกดปุ่ม Save เพื่อทำการ Download โปรแกรม มาเก็บไว้ยังเครื่อง ในที่นี้ ให้เลือกปุ่ม Save ให้เก็บโปรแกรมมาไว้ที่เครื่องก่อน เพื่อลดปัญหา ข้อผิดพลาด ที่จะตามมา (ดังภาพด้านล่าง)

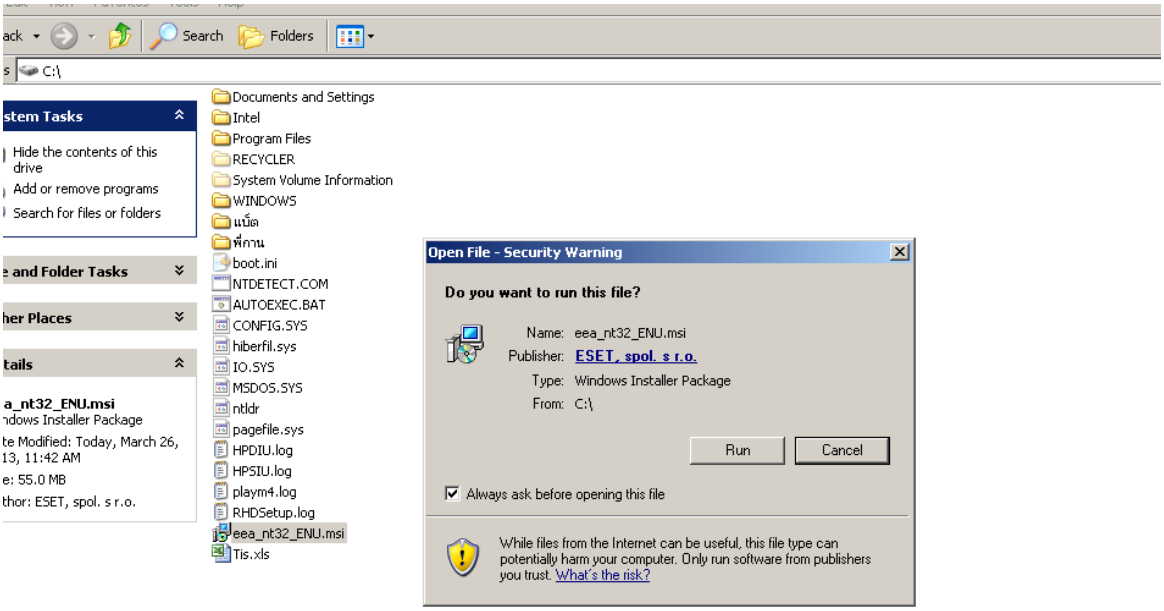



๔. ขั้นตอนต่อไปให้ทำการเลือก ไดร์ฟ ที่จะทำการดาวน์โหลดโปรแกรมมาเก็บไว้ ให้เลือกไดร์ฟ C:\ หลังจากนั้นให้กดปุ่ม Save เครื่อง Computer จะทำการดาวน์โหลดโปรแกรมลงใน ไดร์ฟ C:\ ระบบจะดำเนินการ Download โปรแกรมไฟล์ชื่อ Eset32.exe และนำไปไว้ที่ไดร์ฟ C:\ จนสิ้นสุดการ Download โปรแกรม ขั้นตอนต่อไปเป็นการติดตั้งโปรแกรม



**ขั้นตอนการติดตั้งโปรแกรม** ESET Endpoint Antivirus **(กรมเจ้าท่า)**

๑. ให้ทำการดับเบิ้ลคลิกที่ไฟล์ชื่อ Eset32.exe ในการ Download โปรแกรมมาข้างต้นและเก็บไว้ที่ไดร์ฟ C:\ ให้ทำการกดปุ่ม Run เพื่อเริ่มดำเนินการติดตั้งโปรแกรม



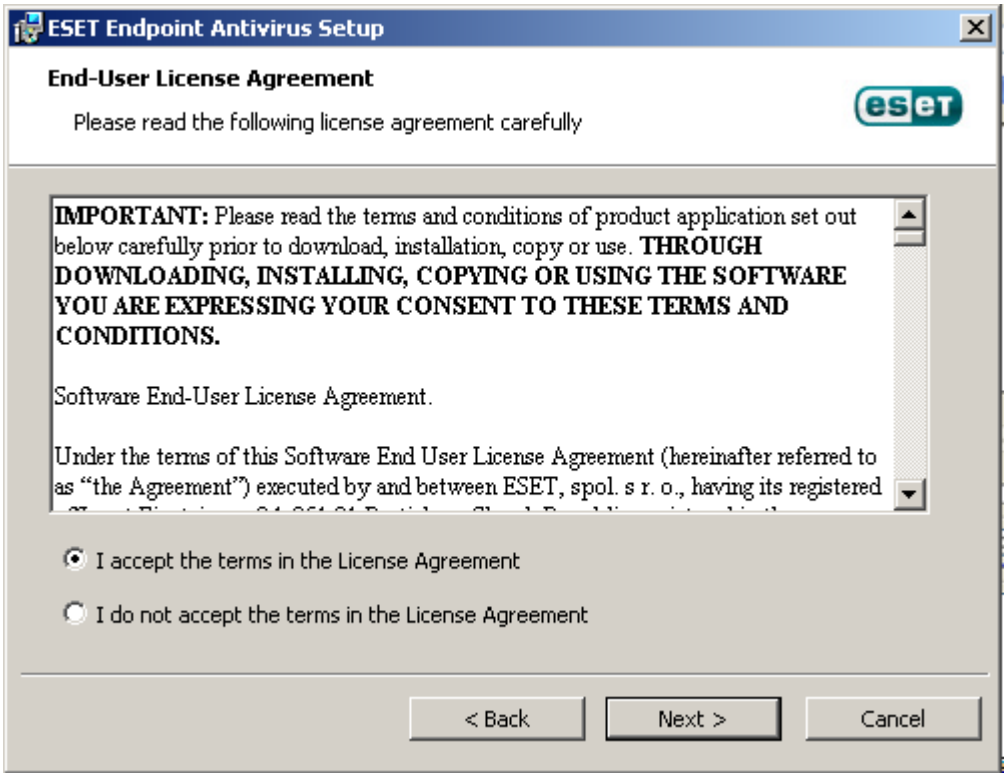

๒. กดปุ่ม  Next



๓. กดเลือกเพื่อยอมรับในรายระเอียดผลิตภัณฑ์ของโปรแกรมที่ 

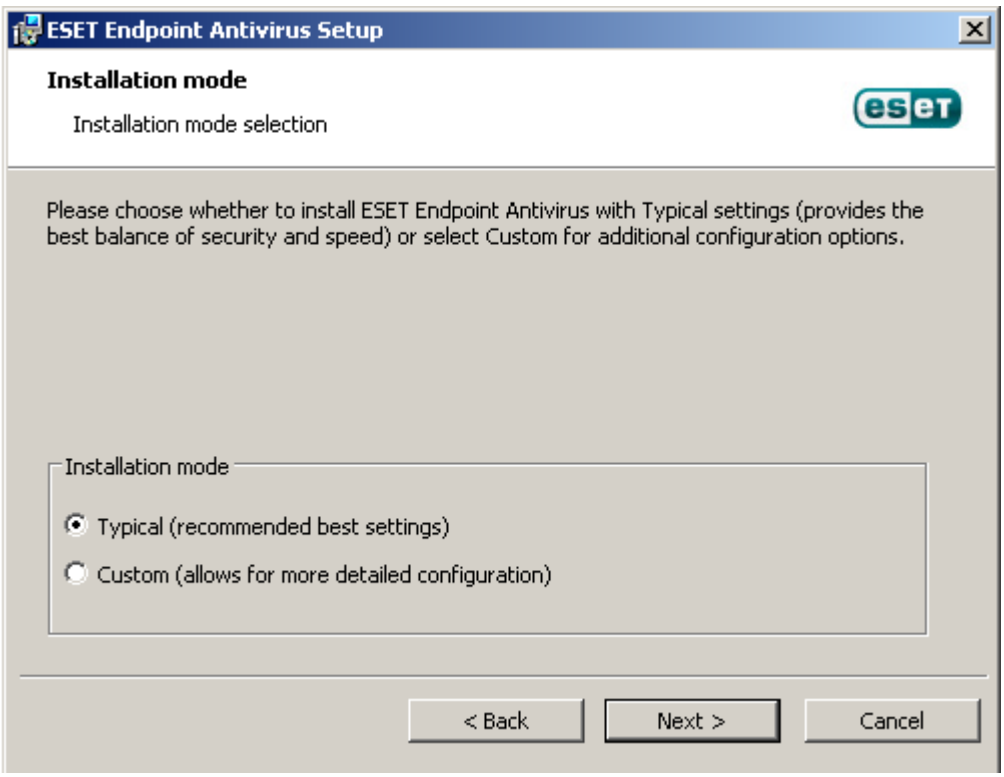
จากนั้น กดเลือกปุ่ม 

(ดังภาพด้านล่าง)

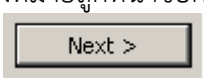



๔ กดปุ่ม 

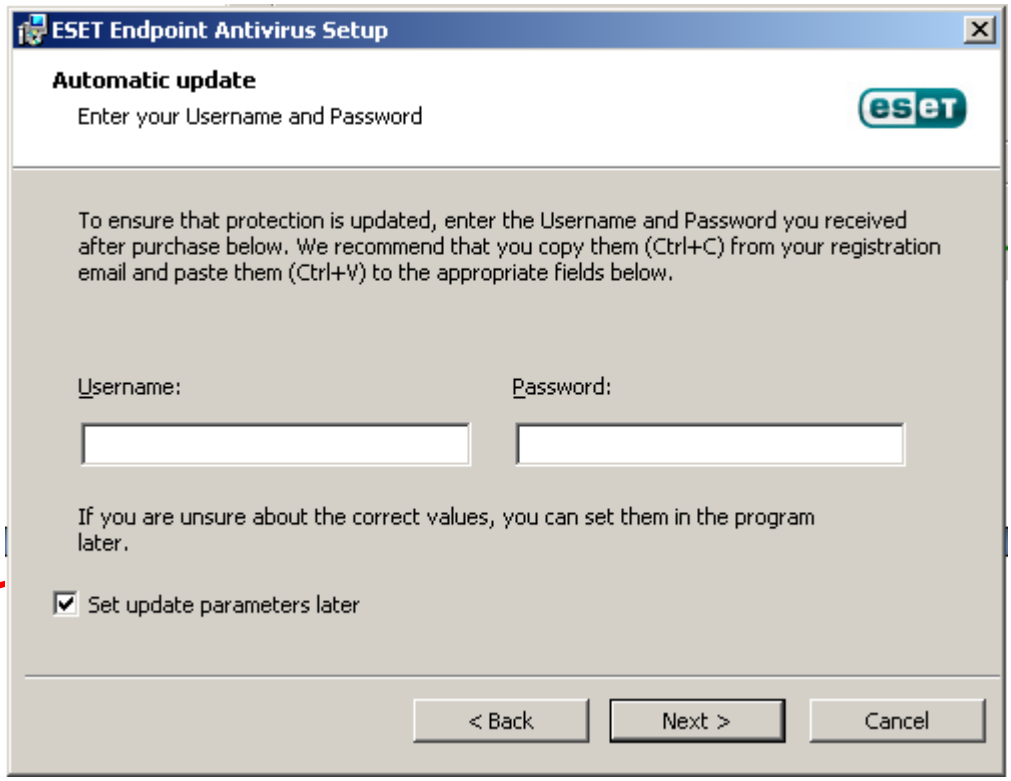
Next



๕. ทำเครื่องหมายถูกหน้าข้อความ Set update parameters later 

จากนั้น กดเลือกปุ่ม 

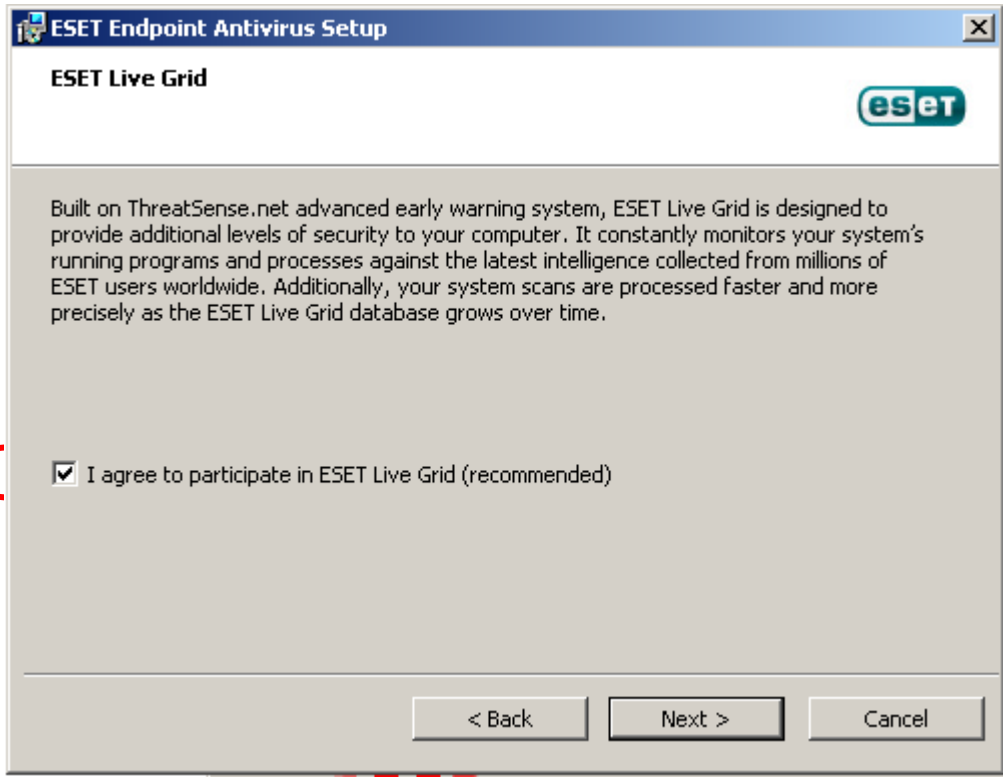
(ดังภาพด้านล่าง)




๖. ทำเครื่องหมายถูกหน้าข้อความ I agree to participate in ESET Live Grid (recommended) 

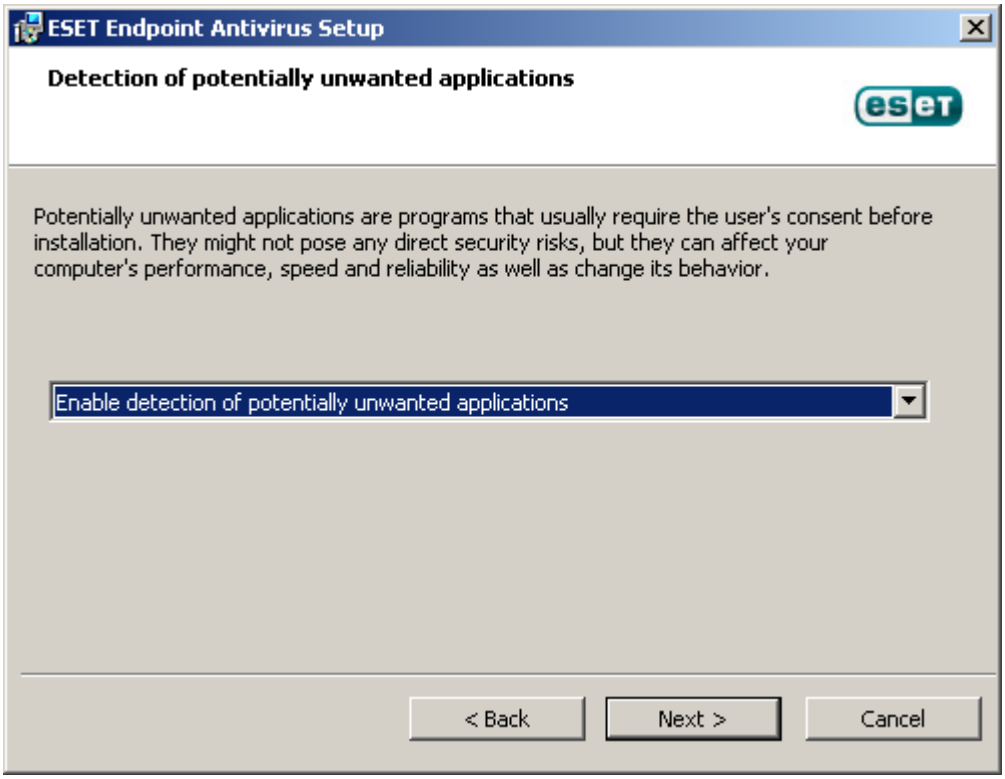
จากนั้น กดเลือกปุ่ม 

(ดังภาพด้านล่าง)

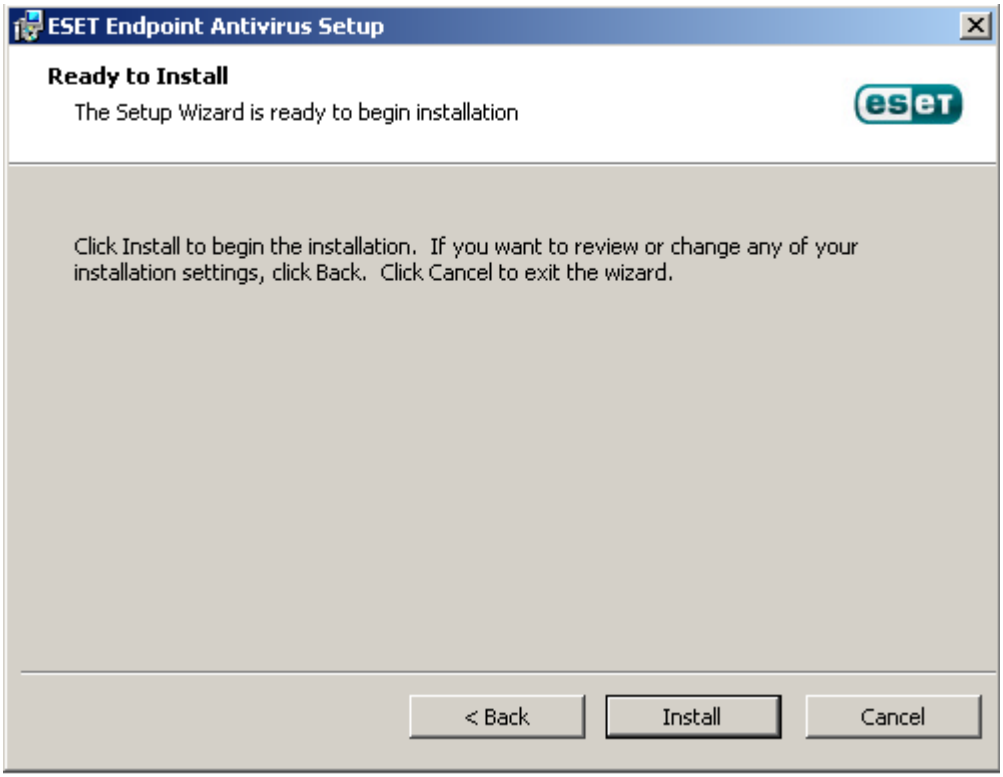


๗. คลิกเลือกเมนูข้อความไปที่ Enable detection of potentially unwanted applications

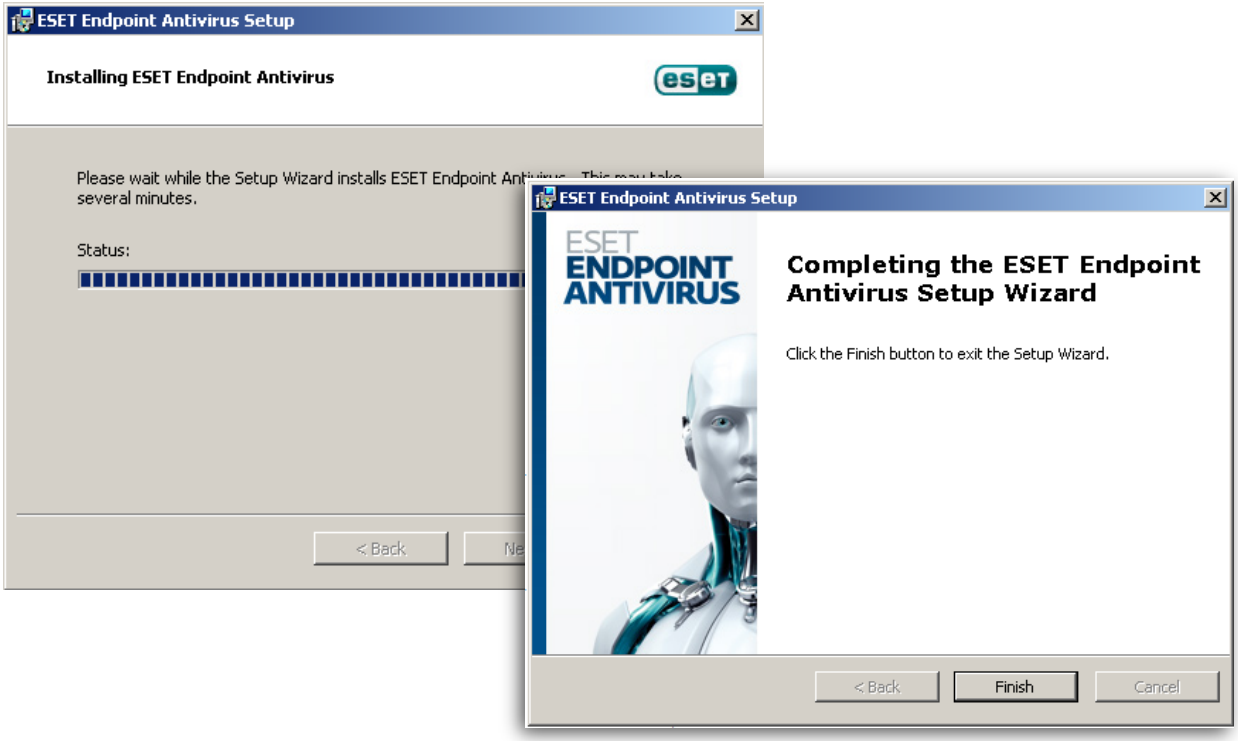

จากนั้นกดเลือกปุ่ม  (ดังภาพด้านล่าง)


**๘.กดปุ่ม Install เพื่อทำการติดตั้งโปรแกรมลงภายในเครื่องคอมพิวเตอร์**



๙. ระบบจะดำเนินการโดยอัตโนมัติจนเสร็จเรียบร้อย จากนั้นให้ทำการ กดปุ่ม Finish

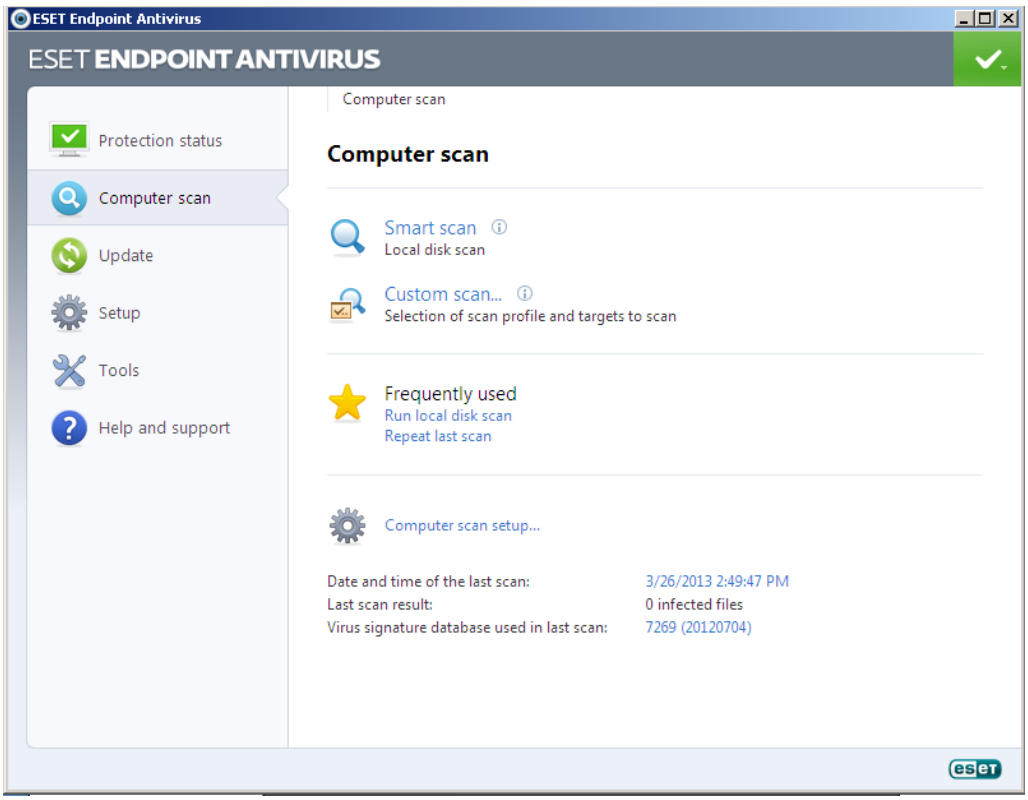



๑๐. มีไอคอนที่มุมขวาของจอแสดงผล (ทาสก์บาร์ (Taskbar)) มีลักษณะเป็นสีเหลืองส้ม ให้ทำการ Restart เครื่อง ๑ ครั้ง

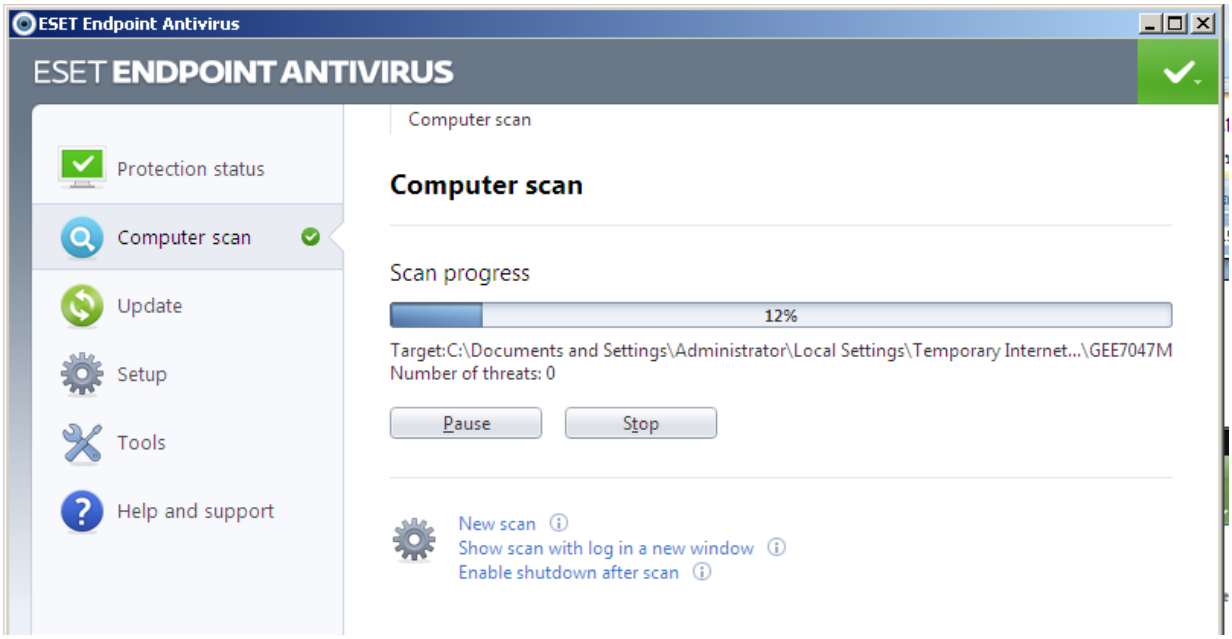

๑๑. หลังทำการ Restart เครื่อง ๑ ครั้งแล้วให้สังเกตไอคอนจะเปลี่ยนลักษณะเป็นสีฟ้าเทา เป็นอันว่าทำการติดตั้งเสร็จสมบูรณ์เรียบร้อย จากนี้เป็นขั้นตอนการปฏิบัติใช้งาน


## ขั้นตอนการปฏิบัติมีดังนี้

๑. ดับเบิ้ลคลิก  ที่ไอคอน จะปรากฏตามภาพที่แสดง แล้วเลือกรูปแบบการแสกนไวรัส




๒. ระบบจะทำการ Scan & Clean อัตโนมัติ




๓. หากมีไวรัสในเครื่องระบบจะมีการแจ้งเตือน และทำการ Clean อัตโนมัติ

****หมายเหตุ**** โปรแกรม ESET Endpoint Antivirus (กรมเจ้าท่า) มีการ Update อยู่ตลอดเวลา User ทุกท่านไม่ต้อง Update โปรแกรมจะทำการ Update เองโดยอัตโนมัติ

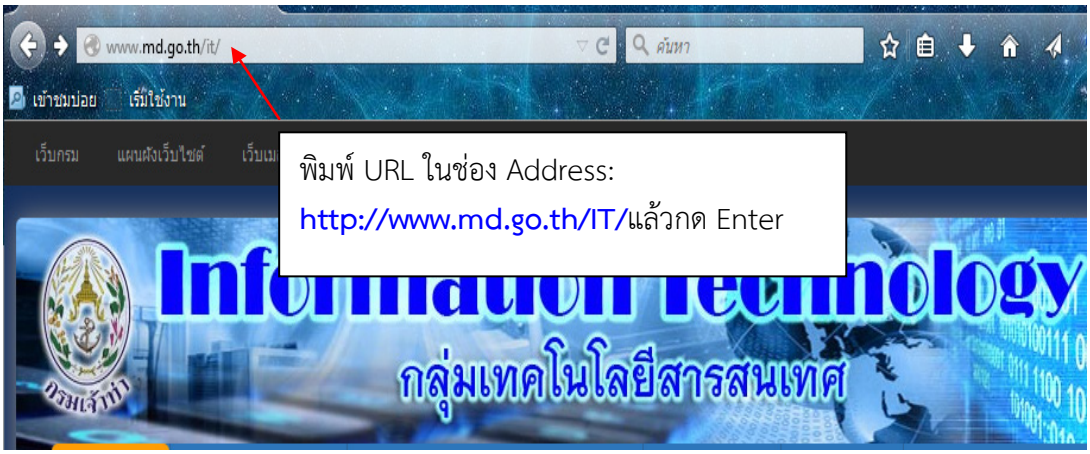
# ภาคผนวก ง

กรณีเครื่องคอมพิวเตอร์ลูกข่ายที่ส่วนภูมิภาคไม่สามารถใช้ระบบงานไม่ได้

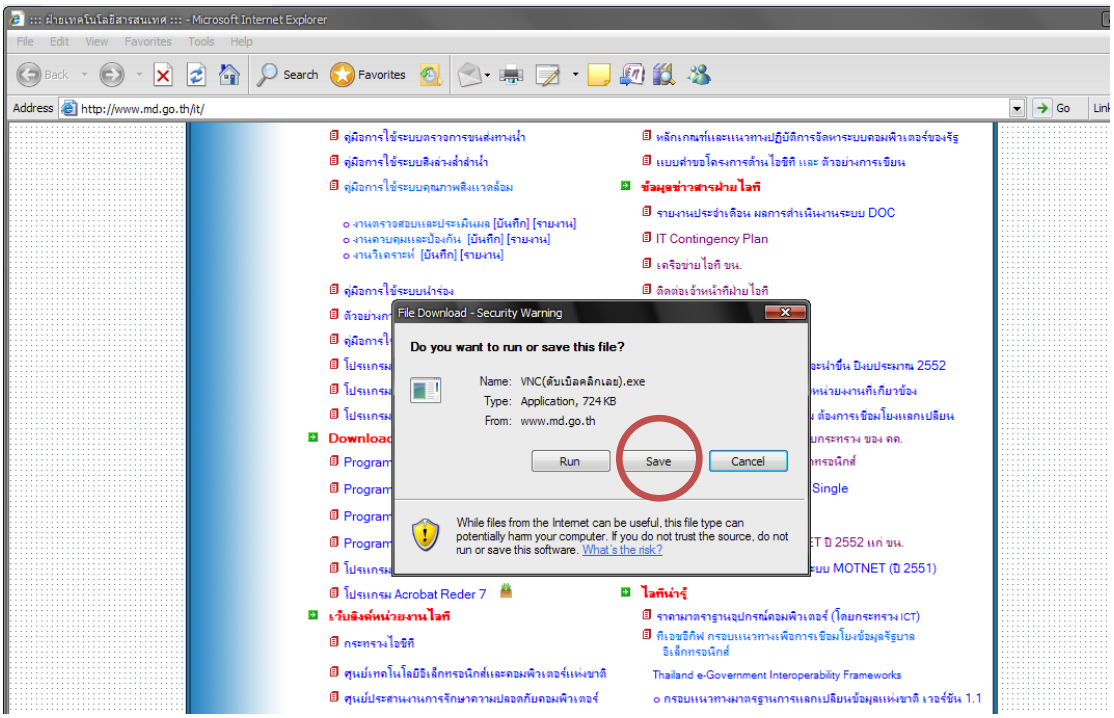
**กรณีเครื่องคอมพิวเตอร์ลูกข่ายที่ส่วนภูมิภาคไม่สามารถใช้ระบบงานไม่ได้**

- **เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศตรวจสอบเบื้องต้นว่าเครื่องในส่วนภูมิภาคนั้นเปิดใช้งานและเชื่อมต่อเครือข่ายได้หรือไม่ โดยการ ping ไปยังไอพีปลายทาง**
- **หากเชื่อมต่อได้แจ้งให้ผู้ใช้งานในส่วนภูมิภาคติดตั้งโปรแกรม VNC เพื่อให้เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศสามารถรีโมทเข้าไปดูเครื่องนั้นๆได้ และ ตรวจสอบแก้ไข หรือแนะนำการใช้งาน การแก้ไขปัญหา ต่อไป โดยมีขั้นตอนดังนี้**

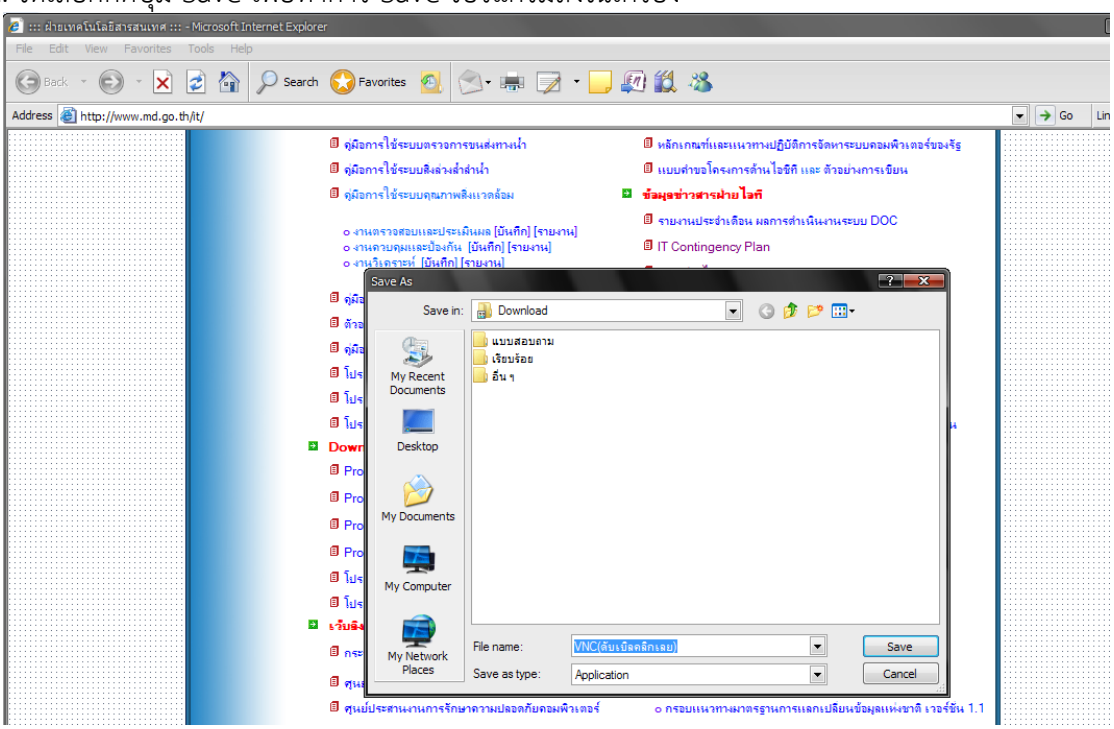
๑. เปิดใช้งาน Internet Explorer พิมพ์ URL ในช่อง Address: http://www.md.go.th/IT/ แล้วกด Enter เพื่อเข้าสู่หน้า บริการด้านไอที




๒. ให้ทำการดาวน์โหลดโดยไปที่หัวเรื่องหลักชื่อ **ดาวน์โหลด** กดปุ่มเลือกที่ หัวข้อย่อยชื่อโปรแกรม VNC สำหรับ Windows xp เพื่อทำการ Download โปรแกรม




๓. ให้เลือกกดปุ่ม Save เพื่อทำการ Save โปรแกรมลงในเครื่อง

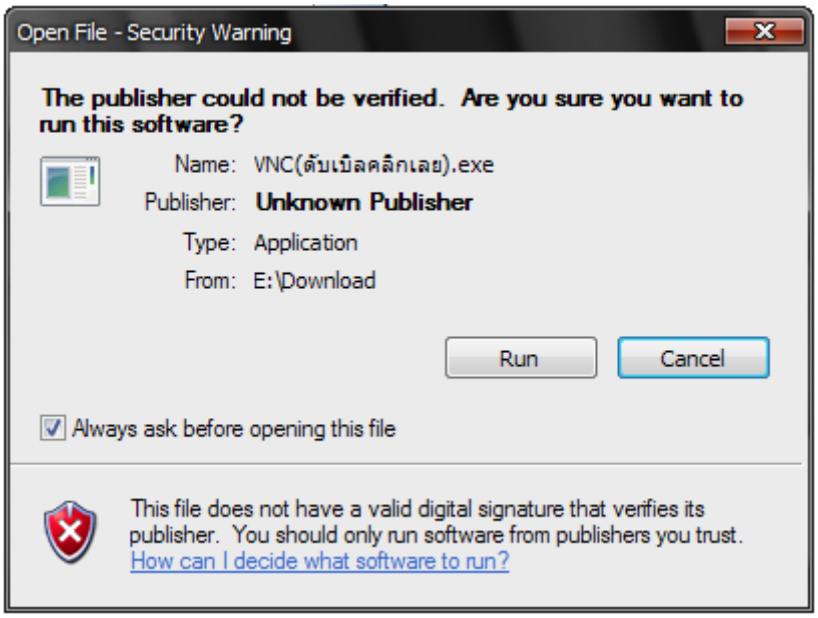



๔. ขั้นตอนต่อไปให้ทำการเลือก ไดร์ฟ ที่จะทำการดาวน์โหลดโปรแกรมมาเก็บไว้ ให้เลือกไดร์ฟที่ต้องการหลังจากนั้นให้กดปุ่ม Save เครื่อง Computer กำลังทำการดาวน์โหดโปรแกรมลงใน ไดร์ฟที่ต้องการ

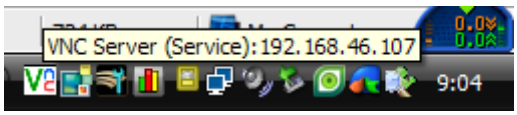
๕. ขั้นตอนต่อไป ให้ดับเบิ้ลคลิกที่ My Computer และเข้าไปในไดร์ฟที่ได้เซฟไว้ จะเห็นไฟล์ชื่อ VNC_win๓๒.exe

**ขั้นตอนการติดตั้งโปรแกรม** VNC 

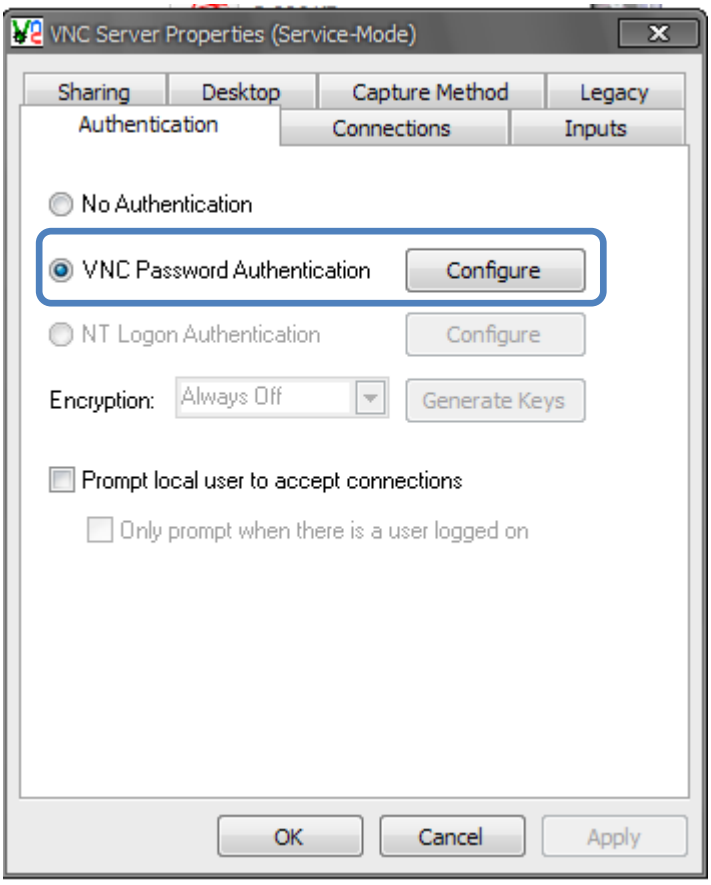

**๑.** ให้ทำการดับเบิ้ลคลิกที่ไฟล์ที่ชื่อ VNC



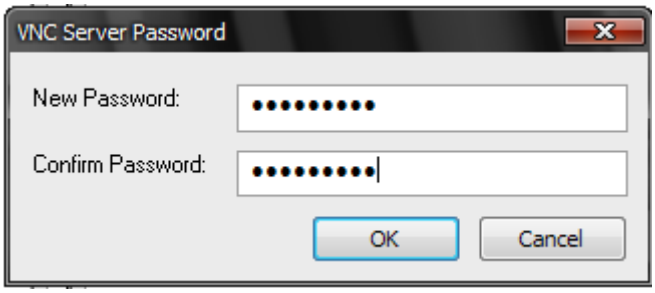

- กดปุ่มRun ระบบจะทำการติดตั้งให้แล้วเสร็จโดยอัตโนมัติ




- เมื่อติดตั้งเสร็จจะปรากฏสัญลักษณ์เพื่อ Auto Service




- ต่อจากนั้นให้ทำการ Configure Password เพื่อใช้โปรแกรม




- ใส่รหัสตามต้องการ แล้วกด OK เป็นการเสร็จการติดตั้งโปรแกรม

# ภาคผนวก จ

กรณีระบบสารสนเทศล่ม

# กรณีระบบสารสนเทศล่ม

**๑. <u>ระบบงานกรม (http://app.md.go.th)</u>**

ระบบงานของกรมได้ปรับปรุงประสิทธิภาพเมื่อ ปี ๒๕๕๔ เสร็จเรียบร้อย โดยมี Application Server ที่ใช้งาน จำนวน ๒ เครื่อง เครื่อง Data Base ๑ เครื่อง โดยมีเครื่อง Load balance ทำหน้าที่แบ่งงานให้ Application Server แต่ละเครื่องสลับกันทำงาน

กรณีระบบล่มไม่สามารถใช้งานได้ มีขั้นตอนการแก้ไข ดังนี้

๑. ตรวจเช็คระบบไฟฟ้าเป็นปกติหรือไม่

๒. ตรวจเช็คเครื่อง Load balance (ip ๑๙๒.๑๖๘.๔๖.๕๗) ให้ทำงานเป็นปกติ

๓. ตรวจเช็คเครื่อง Data Base (ip ๑๙๒.๑๖๘.๔๖.๕๕) ให้ทำงานเป็นปกติ

๔. ตรวจเช็คเครื่อง Application Server เครื่องที่ ๑ (ip ๑๙๒.๑๖๘.๔๖.๕๔) ให้ทำงานเป็นปกติ

๕. ตรวจเช็คเครื่อง Application Server เครื่องที่ ๒ (ip ๑๙๒.๑๖๘.๔๖.๕๒) ให้ทำงานเป็นปกติ

กรณีไม่สามารถออกรายงาน หรือไม่สามารถพิมพ์เอกสารจากระบบได้

๑. ตรวจเช็คเครื่อง Report Server เครื่องที่ ๑ (ip ๑๙๒.๑๖๘.๔๖.๘๗) ให้ทำงานเป็นปกติ

หากตรวจสอบในเบื้องต้นแล้วยังไม่สามารถใช้งานได้อีก แจ้งบริษัทผู้ดูแล บำรุงรักษา

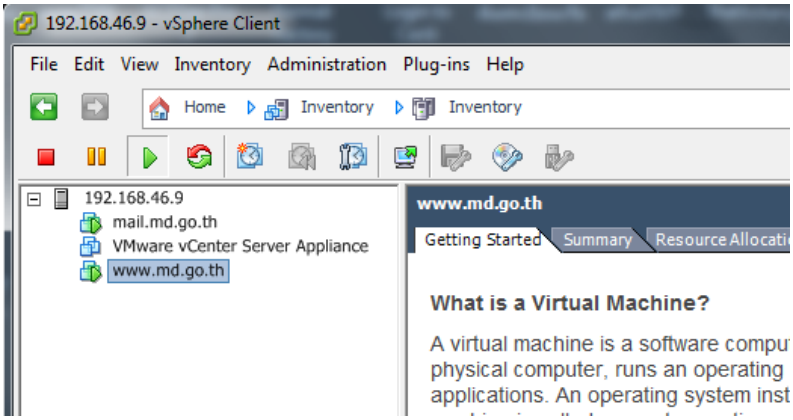
**๒. <u>ระบบ Website กรม ฯ (www.md.go.th)</u>**

ขั้นตอนการแก้ไขเมื่อเกิดปัญหาระบบไม่สามารถใช้งานได้ หรือไฟดับ ดังนี้

**กรณีระบบ Website กรม ล่ม**

๑. ตรวจเช็คระบบไฟฟ้าเป็นปกติหรือไม่

๒. ให้ทำการ Start & Stop ที่ Server “www.md.go.th” เพื่อเป็นการรีเซต Server ใหม่



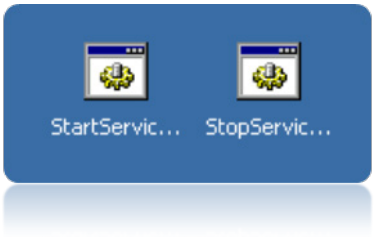

**กรณีไฟฟ้าดับ**

ให้ทำการปิดงานทุกอย่างที่ใช้งานอยู่ในหน้าจอแล้วทำการปิดเครื่อง Server

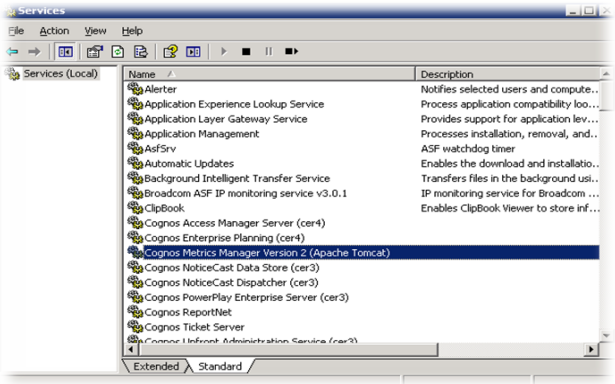
## ๓. ขั้นตอนการแก้ไข เมื่อเกิดปัญหาระบบปฏิบัติการ DOC ใช้ไม่ได้ หรือไฟฟ้าดับ

### ❖ ไม่สามารถเข้าใช้ระบบงานได้

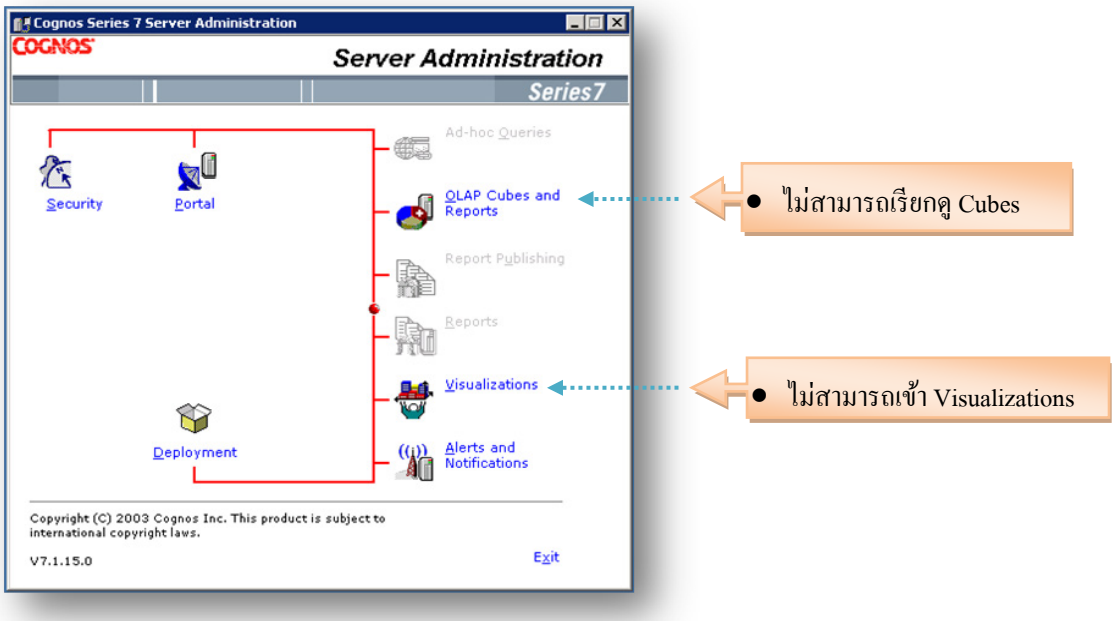
- ให้ทำการ Star & Stop Service.bat เพื่อทำการรีเซตใหม่ทั้งระบบ




- ให้ดูตัว Service Cognos Metrics Manager Version ๒ (Apache Tomcat) แล้วทำการ Start Service ใหม่



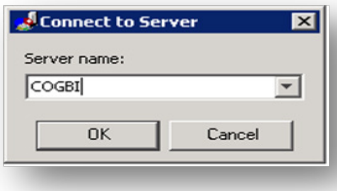

- กรณีที่ Cubes และ Visualizations ไม่สามารถเข้าใช้งานได้ ให้เข้าทำการรีสตาร์ทระบบใหม่ ดังนี้
  ๑. ให้คลิกที่ไอคอนดังรูป 
  ๒. เมื่อเข้ามาแล้วจะได้โปรแกรมดังรูป โดยมีรายละเอียด ดังนี้



๓. เลือกระบบที่เป็นปัญหาในการใช้งาน ดังนี้

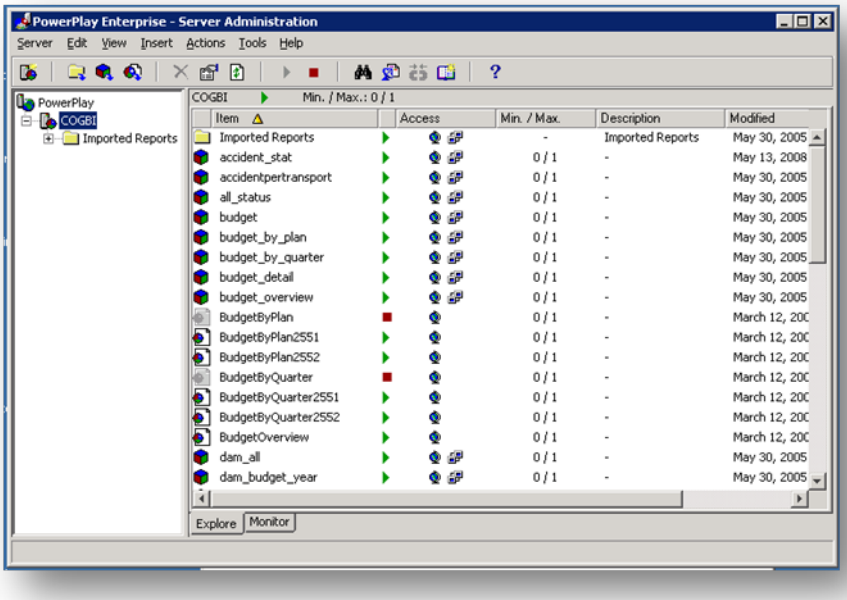
- ไม่สามารถเรียกดู Cubes ได้ โดยปฏิบัติตามขั้นตอนดังนี้

๑. กดเลือกระบบที่ต้องการ



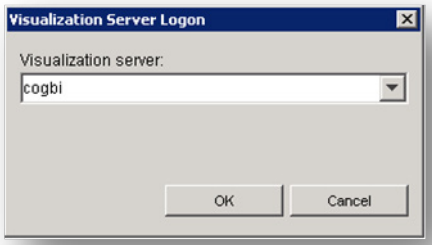

๒. ใส่ชื่อผู้ใช้ และรหัสผ่าน


๓. จากนั้นจะเข้ามาสู่การรีเซตระบบงานใหม่อาจจะ Start & Stop ทุกระบบ หรือเลือกเพียงระบบเดียว



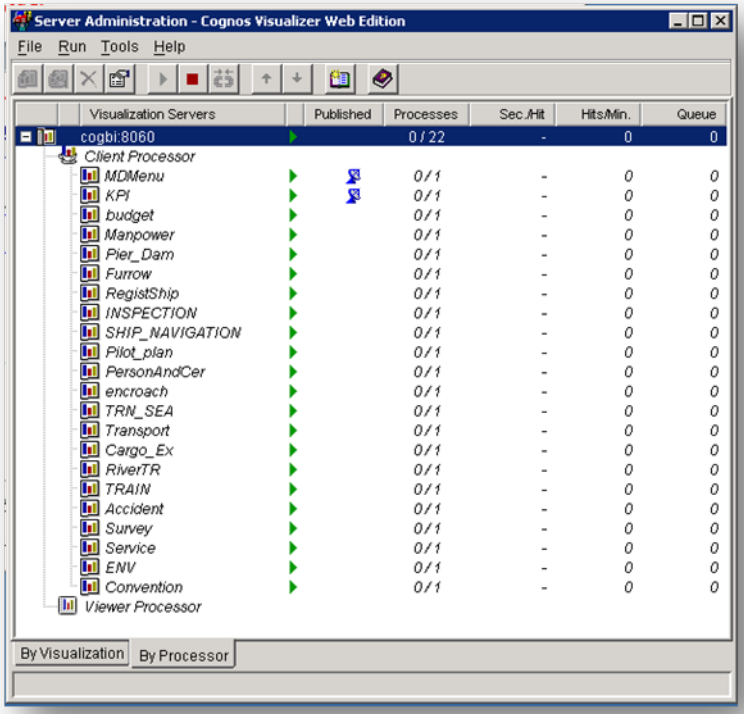

- ไม่สามารถเรียกดู Visualizations ได้ โดยปฏิบัติตามขั้นตอน ดังนี้

๑. กดเลือกระบบที่ต้องการ



๒. ใส่ชื่อผู้ใช้ และรหัสผ่าน


๓. จากนั้นจะเข้ามาสู่การรีเซตระบบงานใหม่อาจจะ Start & Stop ทุกระบบ หรือเลือกเพียงระบบเดียว




**ระบบงานอื่น ๆ** ได้แก่ E-mail, Antivirus หากระบบงานใช้ไม่ได้ให้ทำการ Restart Server ใหม่ จากนั้นเครื่องจะทำงานปกติ เนื่องจากระบบได้ตั้ง Service เป็นแบบ Automatic อยู่แล้ว

# ภาคผนวก ฉ.

## การพิมพ์ SEAMAN PASSBOOK แบบฉุกเฉิน

# การพิมพ์ SEAMAN PASSBOOK แบบฉุกเฉิน

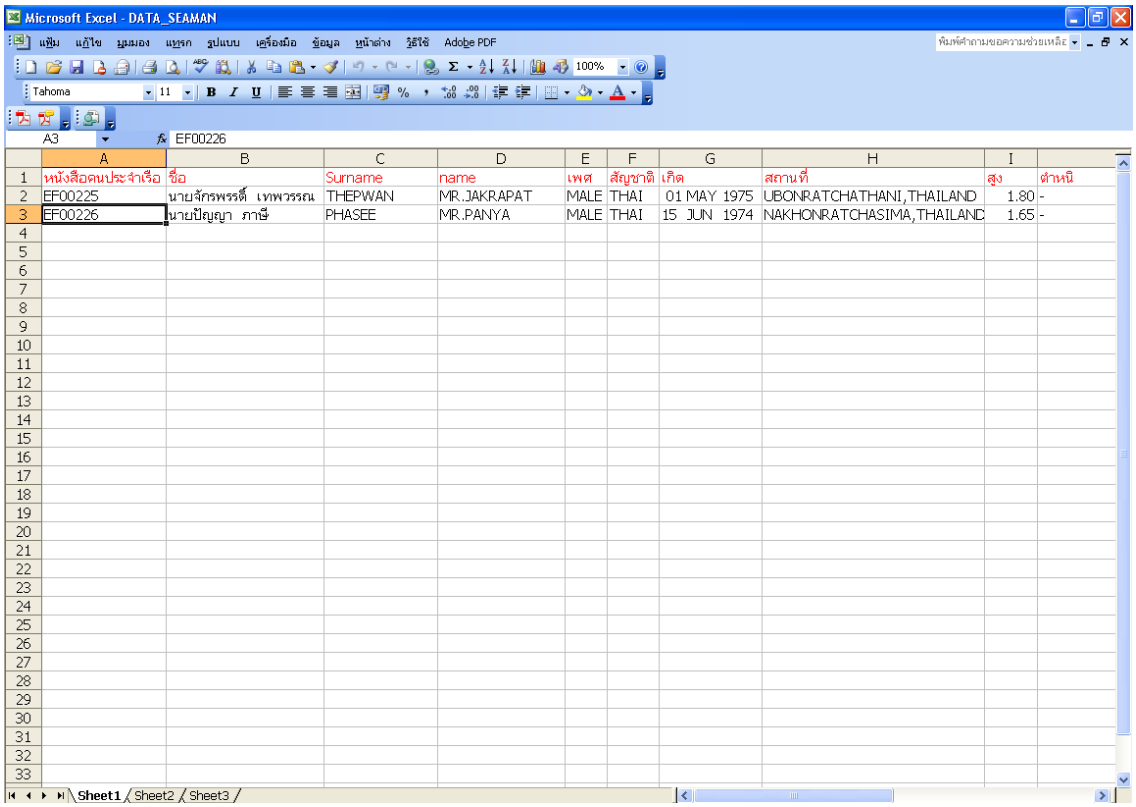
## I. ขั้นตอนดาวน์โหลดไฟล์

ให้ทำการ ดาวน์โหลดไฟล์จาก www.md.go.th/it

- DATA_SEAMAN.xls (ไฟล์ข้อมูล)
- PRINT_SEAMAN.doc (เอกสารสำหรับพิมพ์)

## II. ขั้นตอนการบันทึกข้อมูลใน Excel

๑. เปิดโปรแกรม Excel และ เปิดไฟล์ชื่อ DATA_SEAMAN.xls ดังรูปที่ ๑ เพื่อบันทึกข้อมูล โดยมีตัวอย่างการพิมพ์ให้ใน Sheet เรียบร้อยแล้ว

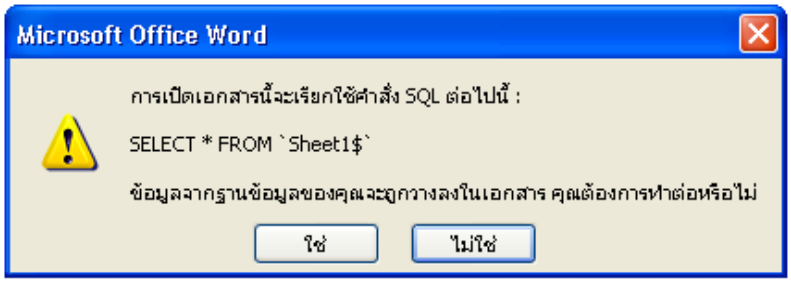



| | A | B | C | D | E | F | G | H | I | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | หนังสือคนประจำเรือ | ชื่อ | Surname | name | เพศ | สัญชาติ | เกิด | สถานที่ | สูง | ตำหนิ |
| 2 | EF00225 | นายจักรพรรดิ์ เทพวรรณ | THEPWAN | MR.JAKRAPAT | MALE | THAI | 01 MAY 1975 | UBONRATCHATHANI,THAILAND | 1.80 | - |
| 3 | EF00226 | นายปัญญา ภาษี | PHASEE | MR.PANYA | MALE | THAI | 15 JUN 1974 | NAKHONRATCHASIMA,THAILAND | 1.65 | - |

๒. เพิ่มข้อมูลจนเสร็จเรียบร้อยแล้วทำการบันทึก และปิดโปรแกรม Excel ๒๐๐๗ ได้เลย

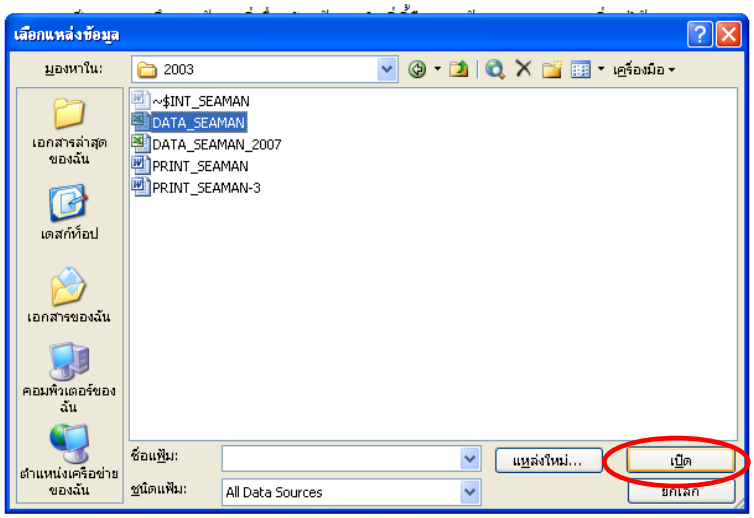
## III. ขั้นตอนพิมพ์เอกสารจาก Word

๓. เปิดโปรแกรม Word ๒๐๐๗ เปิดเอกสาร ชื่อ PRINT_SEAMAN.doc จะปรากฏหน้าจอดังรูปที่ ๒ เป็นการถามถึงฐานข้อมูลที่เชื่อมโยงข้อมูล ในที่นี้คือ ฐานข้อมูล Excel ๒๐๐๗ ที่เราได้ทำการบันทึกไปเรียบร้อย กด ใช่




รูปที่ ๒ แสดงเมื่อเลือกไฟล์ ชื่อ ชื่อ PRINT_SEAMAN.doc

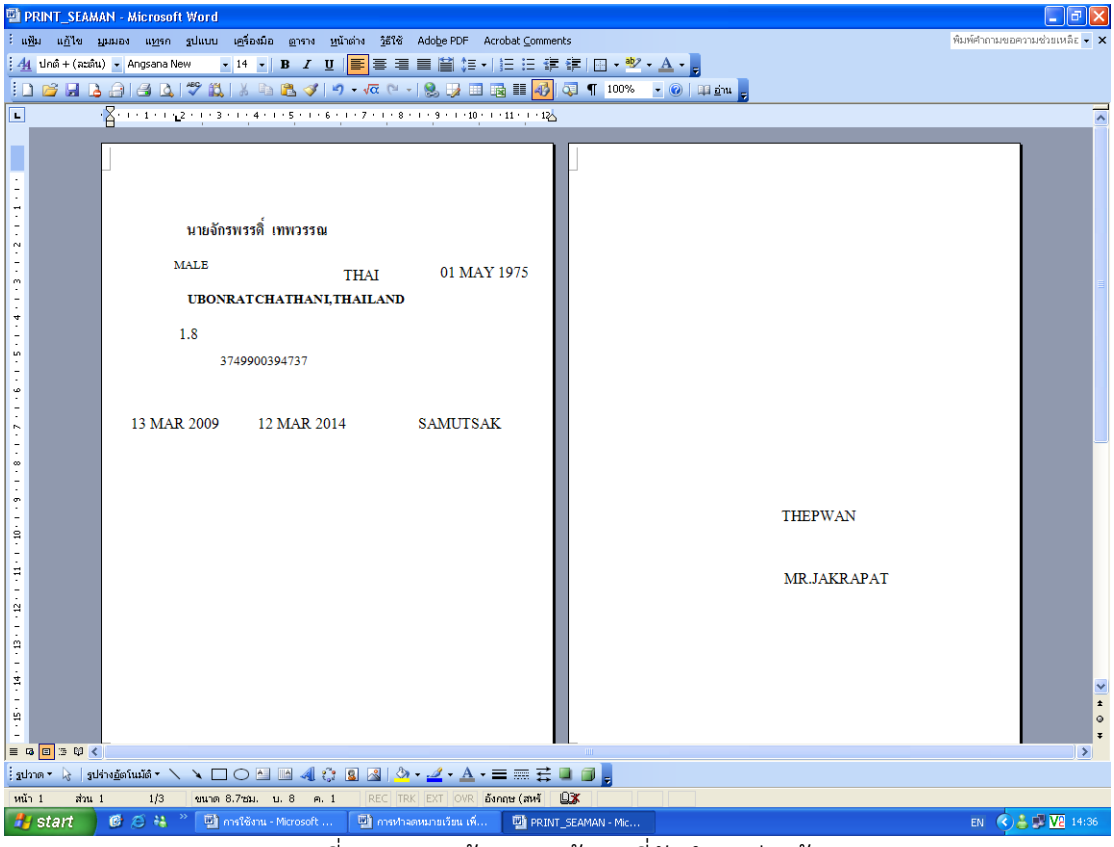
๔. จากรูปที่ ๒ เมื่อกดใช่ ปรากฏหน้าจอดังรูปที่ ๓ จะต้องไปหาไฟล์ Excel ชื่อ DATA_SEAMAN.xls ที่ใช้เป็นฐานข้อมูล ที่ได้บันทึกไปแล้วในขั้นตอนการบันทึกข้อมูล ใน Excel แล้ว กด เปิด




รูปที่ ๓ แสดงการเลือกแหล่งข้อมูล

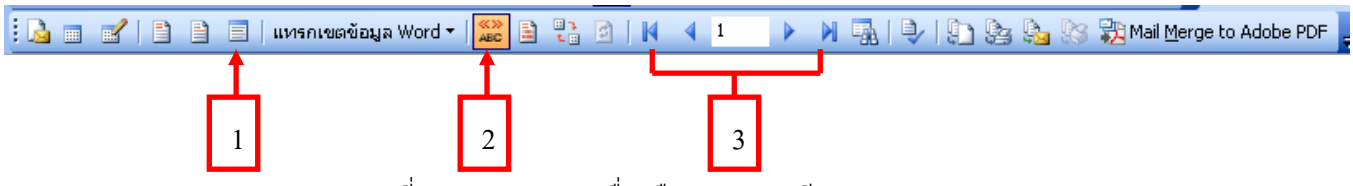
๕. ปรากฏหน้าดังรูปที่ ๔ เป็นข้อมูลที่อยู่ในฐานข้อมูลที่ทำการบันทึกไว้ใน Excel ซึ่งจะแสดงข้อมูลเพียงคนเดียว และเป็นข้อมูลคนแรกของแถว จากไฟล์ DATA_SEAMAN.xls

ส่วน Word ได้จัดทำหน้าที่พิมพ์ลงใน Seaman passbook ไว้ทั้งหมด ๒ หน้า คือ หน้าที่ ๑ และหน้าที่ ๒




รูปที่ ๔ แสดงหน้าตาของข้อมูลที่จัดตำแหน่งแล้ว

๖. ปรากฏแถบเครื่องมือจดหมายเวียน ดังรูปที่ ๖



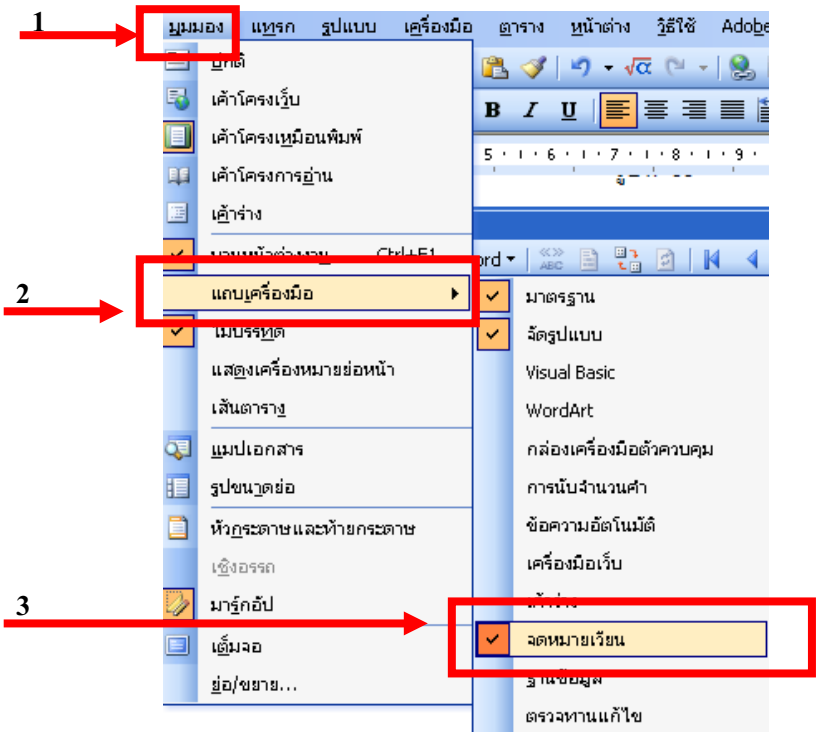

รูปที่ ๖ แสดงแถบเครื่องมือ จดหมายเวียน

แทรกเขตข้อมูลผสาน ใช้เลือกข้อมูลที่ต้องการแสดงจะเป็นชื่อ ของ คอลัมน์ที่อยู่ บรรทัดบนสุด ของ ไฟล์ Excel

แสดงข้อมูลผสาน ใช้แสดงข้อมูล

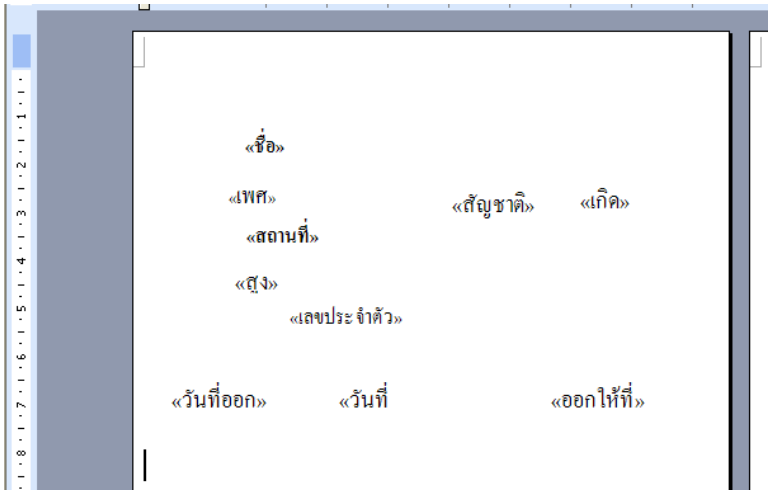
การเลือกระเบียน เป็นการเลื่อนเพื่อดูข้อมูลทีละคน ก่อนหน้า ถัดไป หรือคนแรกสุด หรือ คนสุดท้าย

๗. กรณีไม่มี ให้แทรกเครื่องมือของจดหมายเวียนขึ้นมาก่อนจึงจะสามารถเลือกข้อมูลของคนอื่น ๆ ดังรูปที่ ๕



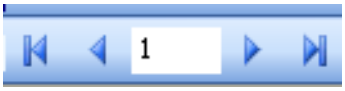

รูปที่ ๕ แสดงการแทรกเครื่องมือ จดหมายเวียน

๘. กรณีที่ข้อมูลแสดงดังรูปที่ ๗ ให้ กดที่เครื่องในข้อ ๗.๒ 


รูปที่ ๗ แสดงหน้าจอที่เป็นชื่อคอลัมน์

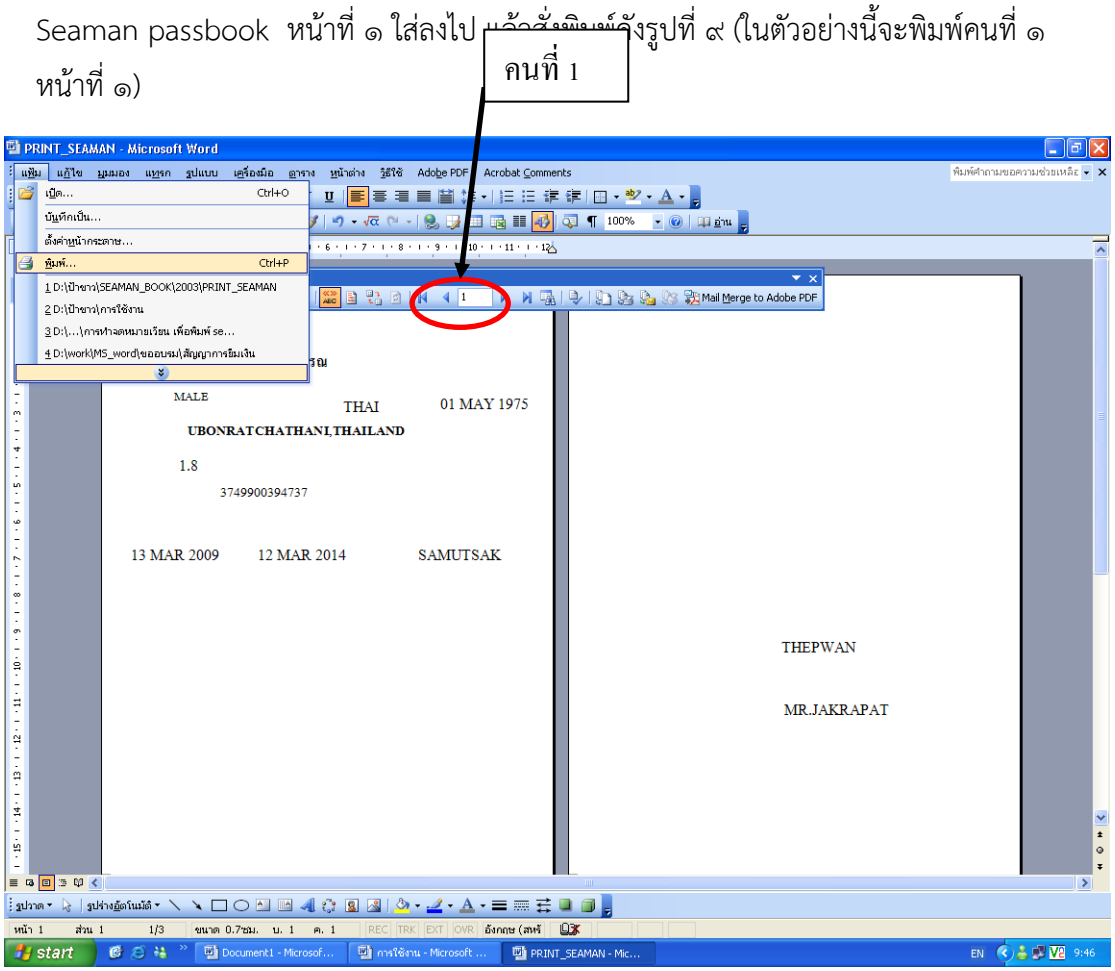
๙. หากต้องการดูข้อมูลคนถัดไปให้ใช้ เครื่องมือดังรูปที่ ๘ ได้ และทำการพิมพ์ข้อมูล ซึ่งเมื่อเลื่อนไปแล้ว จะเปลี่ยนข้อมูลทั้ง ๒ หน้าของ Seaman passbook




รูปที่ ๘ แสดงเครื่องมือที่ใช้ในการเลื่อนข้อมูล

๑๐. ก่อนทำการพิมพ์จริงให้ถ่ายเอกสารและตัดกระดาษให้พอดีกับ Seaman passbook ตัวจริงเพื่อทำการทดลองพิมพ์ให้ ตรงกับตำแหน่งที่ต้องการ หรือทำการปรับแต่งตำแหน่งตามความเหมาะสม

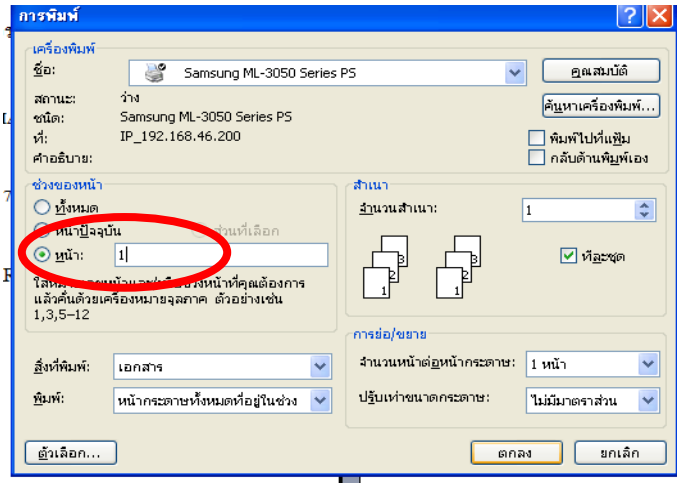
๑๑. เมื่อทำการเลือกข้อมูลของบุคคลที่ต้องการพิมพ์ลง Seaman passbook ได้แล้วให้นำสมุด Seaman passbook หน้าที่ ๑ ใส่ลงไป แล้วสั่งพิมพ์ดังรูปที่ ๙ (ในตัวอย่างนี้จะพิมพ์คนที่ ๑ หน้าที่ ๑)




รูปที่ ๙ แสดงการพิมพ์ข้อมูล หน้าที่ ๑

๑๒. ให้ระบุหน้าที่พิมพ์ เฉพาะหน้าที่ ๑ ดังรูปที่ ๑๐ แล้วจึงสั่งพิมพ์

๑๓. เมื่อต้องการพิมพ์หน้าที่ ๒ ให้นำ Seaman passbook หน้าที่ ๒ใส่เครื่องพิมพ์ และสั่งพิมพ์ตาม ข้อ ๑๑ – ๑๒ และใส่เลขหน้าเป็นหน้าที่ ๒ แล้วสั่งพิมพ์




รูปที่ ๑๐ แสดงการพิมพ์ข้อมูล

๑๔. เมื่อต้องการพิมพ์คนที่สองให้กดลูกศรเลื่อนจากเครื่องดังรูปที่ ๑๑


รูปที่ ๑๑ แสดงการเลือกข้อมูลคนต่อไป

๑๕. แล้วจึงทำตามขั้นตอนที่ ๑๑ -๑๓ ใหม่อีกครั้งหนึ่ง

# ภาคผนวก ช.

นโยบายการใช้เครื่องคอมพิวเตอร์และเครือข่าย

# บันทึกข้อความ

**ส่วนราชการ** ฝ่ายเทคโนโลยีสารสนเทศ สำนักแผนงาน

**ที่** คค 0307.ทส/00910 **วันที่** 11 สิงหาคม 2552

**เรื่อง** นโยบายใช้งานเครื่องคอมพิวเตอร์และเครือข่าย

① เรียน ททส.

ด้วยฝ่ายเทคโนโลยีสารสนเทศ กรมการขนส่งทางน้ำและพาณิชยนาวี ได้จัดทำร่างนโยบายการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย เพื่อให้การใช้งานเครื่องคอมพิวเตอร์และเครือข่ายของกรมเป็นไปด้วยความเรียบร้อย และสอดคล้องกับแนวทางในการบริหารจัดการ การบริหารความเสี่ยง และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรม

ในการนี้ ฝ่ายเทคโนโลยีสารสนเทศ จึงขอความร่วมมือจากเจ้าหน้าที่ทุกหน่วยงาน ให้ความร่วมมือและถือปฏิบัติตามนโยบาย ดังกล่าว (รายละเอียดตามเอกสารแนบ) อย่างเคร่งครัด ต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาก่อนนำ เสนอ CIO. เพื่อโปรดพิจารณาให้ความเห็นชอบ และแจ้งเวียนให้หน่วยงานภายใต้สังกัดกรม เพื่อทราบและถือปฏิบัติ ต่อไป

(นายอนุรักษ์ จอมแปงทา)
เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน

② เรียน รขน.ปภ. (CIO)

ทส. ได้จัดทำ "นโยบายการใช้เครื่องคอมพิวเตอร์และเครือข่าย" เพื่อให้การใช้งานไอทีของกรมดำเนินได้ด้วยความเรียบร้อย และมีประสิทธิภาพ นอกจากนี้ ยังเป็นกิจกรรมหนึ่งที่ฝ่ายจะต้องดำเนินการตามมาตรการจัดการความเสี่ยงด้านไอทีของกรมในปี 2552 ด้วย

จึงเรียนมาเพื่อโปรดพิจารณา ให้ความเห็นชอบในนโยบายดังกล่าว ก่อน ทส. จะได้แจ้งหน่วยงานภายในสังกัดทราบ รวมทั้งเผยแพร่ทางเว็บไซต์ต่อไป

ททส.
11 สิงหาคม 2552

③
- เห็นชอบ
- ดำเนินการต่อไป

เรือตรี
(ปรีชา เพ็ชรวงศ์)
รขน.(ปภ.)
20 ส.ค. 52

สำเนาเรียน
เพื่อโปรดทราบ และถือปฏิบัติต่อไป

ททส.
27 ส.ค. 52

3202

# นโยบายการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย
# กรมการขนส่งทางน้ำและพาณิชยนาวี

เพื่อให้การใช้งานเครื่องคอมพิวเตอร์และเครือข่ายของกรมการขนส่งทางน้ำและพาณิชยนาวี เป็นไปอย่างมีระเบียบเรียบร้อย และเกิดประโยชน์สูงสุด ฝ่ายเทคโนโลยีสารสนเทศ จึงเห็นควรกำหนดนโยบายการใช้เครื่องคอมพิวเตอร์และเครือข่าย ดังรายละเอียดต่อไปนี้

## นโยบายการใช้งานคอมพิวเตอร์ทั่วไป

1. เครื่องคอมพิวเตอร์และเครือข่ายของกรมเป็นสมบัติของทางราชการ ผู้ใช้งานควรใช้เพื่อประโยชน์ของทางราชการเท่านั้น
2. ผู้ใช้งานต้องยอมรับทราบกฎระเบียบหรือนโยบายต่าง ๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้
3. บัญชีผู้ใช้งาน (User Account) ให้เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้
4. บัญชีผู้ใช้งาน (User Account) ที่ให้กับผู้ใช้งานไว้นั้น ผู้ ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้นรวมถึงผลเสียหายต่าง ๆ ที่เกิดจาก บัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
5. ห้ามผู้ใช้งานปฏิบัติการใด ๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน หรือกระทำการที่ก่อให้เกิดความเสียหายแก่บุคคลอื่น โดยการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรม
6. ห้ามผู้ใช้งานทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร
7. การติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรม หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม หากก่อให้เกิดความเสียหาย หรือ การละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว
8. ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล
9. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่นกล่าวคือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต เช่น การบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น ๆ การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว

10. ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/นโยบาย/กฎ/ระเบียบ/คำแนะนำที่กรมกำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม

11. หากผู้ใช้งานกระทำการล่วงละเมิด หรือพยายามจะล่วงละเมิด ฝ่ายเทคโนโลยีสารสนเทศในฐานะผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายของกรม ขอสงวนสิทธิที่จะยกเลิกการใช้งาน หรือระงับการเชื่อมต่อ และ/หรือ การใช้งานใด ๆ ตามความเหมาะสม

**นโยบายการเชื่อมต่อเครื่องคอมพิวเตอร์และเครือข่าย**

1. ผู้ที่ต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด เพื่อให้การเชื่อมต่ออุปกรณ์ต่าง ๆ เป็นไปตามมาตรฐาน และไม่เกิดผลกระทบกับระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของกรม

2. การขออนุญาตนำเครื่องคอมพิวเตอร์เชื่อมต่อระบบเครือข่ายและขอหมายเลขไอพี (IP Address) และชื่อโดเมน (Domain Name) ของหน่วยงานใด ๆ หน่วยงานนั้นจะต้องทำหนังสือขออนุญาตส่งผ่านหน่วยงานต้นสังกัดมายังฝ่ายเทคโนโลยีสารสนเทศเพื่อพิจารณาดำเนินการ

3. ห้ามบุคคลใดกระทำการเคลื่อนย้าย หรือทำการใด ๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความเสียหายแก่ระบบเครือข่ายหลักของกรม ได้

4. ในกรณีที่ ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติของระบบเครือข่ายหลักของกรม ฝ่ายเทคโนโลยีสารสนเทศ อาจจะหยุดให้บริการจากระบบเครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไข ให้ทำงานได้เป็นปกติก่อน

5. ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบไร้สายด้วย (Wireless Network)

.....

# ภาคผนวก ซ.

การดำเนินการตามแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ (IT Contingency Plan) และการวิเคราะห์ ทบทวนสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ

# บันทึกข้อความ

**ส่วนราชการ** สำนักแผนงาน กลุ่มเทคโนโลยีสารสนเทศ โทร ๓๓๓ ๓๓๔

**ที่** คค ๐๓๑๙.๔/ทส. ๓๐๕ **วันที่** ๕ กันยายน ๒๕๖๑

**เรื่อง** รายงานปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ การวิเคราะห์ทบทวนสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ ประจำปีงบประมาณ ๒๕๖๑

(๑) เรียน ผสผ. (ผ่าน หทส.)

ตามที่กรมฯ ได้นำระบบฐานข้อมูลและระบบสารสนเทศมาใช้ในการปฏิบัติงานและให้บริการประชาชน ซึ่งหากระบบเกิดความเสียหายจะส่งผลต่อการปฏิบัติงานต่างๆ ภายในกรมฯ ดังนั้นจึงจำเป็นต้องให้ความสำคัญในการบริหารความเสี่ยงด้านระบบฐานข้อมูลและระบบสารสนเทศ ทส. จึงได้ดำเนินการจัดทำแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ และแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) ตั้งแต่ปี ๒๕๕๑ โดยปฏิบัติตามแผนฯ และมีการทบทวนในทุกปีอย่างต่อเนื่อง ดังนั้นเพื่อให้แผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ และแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) สอดคล้องกับสภาพเทคโนโลยีที่เปลี่ยนแปลงไป ทส. จึงได้มีการทบทวนและปรับปรุงแผนฯ ในปี ๒๕๖๒ และดำเนินการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๒๕๖๒ รายละเอียดปรากฏตามเอกสารแนบ

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบโปรดนำเสนอ ท่าน รจท.มฐ.(CIO) ให้ความเห็นชอบก่อนนำเสนอ ท่าน อจท. ให้ความเห็นชอบต่อไปด้วย จักขอบคุณยิ่ง

(ว่าที่ ร.ต.สมพิศ แกว่นธัญกิจ)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

(นายศุทธ์ธี คงพารา)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

(นายสมโภช วัฒนไวฑูรย์ชัย )
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

(นายอนุรักษ์ จอมแปงทา)
เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน

(๒) เรียน รจท. มฐ. (CIO)
เพื่อโปรดพิจารณาให้ความเห็นชอบก่อนนำเสนอ ท่าน อจท. เพื่อพิจารณาให้ความเห็นชอบต่อไป จักขอบคุณยิ่ง

(นางชนินทร วรวนาวงศ์)
นักวิชาการขนส่งชำนาญการพิเศษ
หกผ.รรก.ผสผ.
๖ ก.ย. ๖๑

(นางสาววิศัลยา ปานเจริญ)
หทส.
- ๕ ก.ย. ๒๕๖๑

**รายละเอียดการดำเนินการตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับงานสารสนเทศ (IT Contingency Plan) และแนวทางในการดำเนินการในปีงบประมาณ ๒๕๖๒**

| ลำดับที่ | ประเด็น | มาตรการ | การดำเนินการตามแผนปี ๒๕๖๑ | แนวทางในการดำเนินการในปี ๒๕๖๒ |
|---|---|---|---|---|
| ๑ | การป้องกันทางกายภาพ | (๑) ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย | - สผง.(ทส.) ได้ดำเนินการตรวจสอบ บำรุงรักษาระบบกล้องโทรทัศน์วงจรปิด และระบบรักษาความปลอดภัย (Access Control System) และอุปกรณ์ที่เกี่ยวข้องให้ใช้งานดีอยู่ตลอดเวลา | – ดำเนินการตามแผนที่ได้ปฏิบัติในปี ๒๕๖๑ และตรวจสอบ บำรุงรักษาอุปกรณ์ที่เกี่ยวข้องให้ใช้งานดีอยู่ตลอดเวลา เช่นระบบกล้องโทรทัศน์วงจรปิด และระบบรักษาความปลอดภัย (Access Control System) เพื่อควบคุมการเข้า - ออก ของบุคคลภายนอกห้องคอมพิวเตอร์โดยใช้การสแกนลายนิ้วมือ (Proximity Access Control) ติดตั้งที่ทางเข้าห้องคอมพิวเตอร์แม่ข่าย ห้องควบคุมระบบไฟฟ้า ระบบเครื่องปรับอากาศ และประตูทางเข้าห้องหลัก |
| | | (๒) การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้องเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ | - สผง.(ทส.) ได้ดำเนินการติดตั้งระบบไฟฟ้าหลักของกับอุปกรณ์ต่างๆ ภายในศูนย์คอมพิวเตอร์ (Data Center) และระบบไฟฟ้าสำรองให้กับอุปกรณ์ต่างๆ ภายในศูนย์คอมพิวเตอร์ (Data Center) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) | - ติดตาม ตรวจสอบ บำรุงรักษา อุปกรณ์ให้สามารถใช้งานได้ดีอยู่สม่ำเสมอ<br>- เปิดเครื่องสำรองไฟฟ้า ตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์<br>- ตรวจสอบ บำรุงรักษา เครื่องสำรองไฟฟ้าอยู่ในสภาพพร้อมใช้งานเสมอ<br>- ตรวจสอบปริมาณการใช้งานไม่ให้เกินโหลด |
| | | (๓) มีระบบป้องกันไฟไหม้ | - สผง.(ทส.) มีระบบป้องกันอัคคีภัยในห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Data Center) (อาคาร ๖) ชั้น ๔ ประกอบด้วย | - ติดตาม ตรวจสอบ บำรุงรักษา อุปกรณ์ระบบระบบดับเพลิงอัตโนมัติ (FIRE SUPPRESSION SYSTEM) และ ระบบ |

| ลำดับที่ | ประเด็น | มาตรการ | การดำเนินการตามแผนปี ๒๕๖๑ | แนวทางในการดำเนินการในปี ๒๕๖๒ |
|---|---|---|---|---|
| | | | - ระบบตรวจจับควันไฟความไวสูง (HIGH SENSITIVITY SMOKE DETECTION) บริเวณ Return air ของเครื่องปรับอากาศ<br>- ระบบระบบดับเพลิงอัตโนมัติ (FIRE SUPPRESSION SYSTEM) ทั้งเหนือพื้นยกและใต้บริเวณพื้นยก โดยใช้ระบบ Inert Gas System ชนิด FM-๒๐๐<br>- สผง.(ทส.) ดำเนินการติดตาม ตรวจสอบ บำรุงรักษา อุปกรณ์ระบบระบบดับเพลิงอัตโนมัติ (FIRE SUPPRESSION SYSTEM) และ ระบบแจ้งเตือนอัคคีภัยความไวสูง (HIGH SENSITIVITY SMOKE DETECTION) ให้สามารถใช้งานได้ดีอยู่สม่ำเสมอ<br>- ดำเนินการตามแผนการซักซ้อมกรณีเกิดเหตุเพลิงไหม้ | แจ้งเตือนอัคคีภัยความไวสูง (HIGH SENSITIVITY SMOKE DETECTION) ให้สามารถใช้งานได้ดีอยู่สม่ำเสมอ<br>- มีการซักซ้อมแผนกรณีเกิดไฟไหม้ ปีละ ๑ ครั้ง |
| | | (๔) ระบบแจ้งเตือนเหตุการณ์ผิดปกติต่างๆ | - ระบบแจ้งเตือนเหตุการณ์ต่างๆ ประกอบด้วย<br>๑. แจ้งเตือนเมื่อมีการเข้า-ออกห้อง Server<br>๒. แจ้งเตือนเมื่อมีกระแสไฟฟ้าขัดข้อง<br>๓. แจ้งเตือนระบบปรับอากาศ<br>๔. แจ้งเตือนน้ำรั่วซึมที่อาจเข้ามาในห้อง Server<br>๕. แจ้งเตือนเมื่อตรวจพบควันไฟ<br>ระบบจะแจ้งเตือนเหตุการณ์ผิดปกติที่ตรวจพบ โดยส่ง SMS ผ่านทางโทรศัพท์มือถือ | - ติดตาม ตรวจสอบ บำรุงรักษา อุปกรณ์ให้สามารถใช้งานได้ดีอยู่สม่ำเสมอ |

| ลำดับที่ | ประเด็น | มาตรการ | การดำเนินการตามแผนปี ๒๕๖๑ | แนวทางในการดำเนินการในปี ๒๕๖๒ |
|---|---|---|---|---|
| ๒ | มีระบบรักษาความมั่นคงปลอดภัย (Security) ของระบบคอมพิวเตอร์ | (๑) การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์ แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่ เชื่อมต่อกับระบบเครือข่าย ผู้ใช้งานต้องระมัดระวังในการใช้งานคอมพิวเตอร์ โดยเฉพาะเมื่อเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบ | - สผง.(ทส.) มีการติดตั้งระบบ Antivirus Gateway ป้องกันไวรัส/เวิร์ม และสแปมเมล์ ซึ่งสามารถกลั่นกรองไวรัส/เวิร์ม และ สแปมเมล์ที่มาจากเครือข่ายภายนอก ได้ส่วนหนึ่ง ซึ่งเป็นการแบ่งเบาภาระใน การบำรุงรักษาเครื่องคอมพิวเตอร์ ระบบ เครือข่ายภายใน ที่เกิดปัญหาต่าง ๆ ติดตั้ง โปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ<br>- ได้ดำเนินการ บำรุงรักษาเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงและการแก้ไขปัญหาระบบ ในส่วนกลาง เพื่อให้ผู้ปฏิบัติงานใน สามารถใช้ระบบสารสนเทศผ่านระบบเครือข่ายได้อย่างมีประสิทธิภาพ และเพื่อควบคุมดูแล บำรุงรักษาระบบคอมพิวเตอร์ในองค์กรสามารถใช้งานได้ตลอดเวลา โดยแผนการบำรุงรักษา ระบบเครื่องคอมพิวเตอร์มีการดำเนินการดังนี้<br>๑. การทำความสะอาด และบำรุงรักษาอุปกรณ์คอมพิวเตอร์<br>๒. ตรวจสอบการทำงานของระบบ ปฏิบัติการ เช่น ลบข้อมูลที่ไม่จำเป็น ( Disk Cleanup) และทำการจัดเรียงข้อมูล (Defragmenter) และทำการปรับปรุงช่องโหว่ของระบบปฏิบัติการ<br>๓. ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัส<br>๔. ถ่ายทอดความรู้และแนะนำการใช้งาน<br>๕. ให้คำปรึกษาวิธีการใช้ระบบงาน | - ดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมเจ้าท่า |

| ลำดับที่ | ประเด็น | มาตรการ | การดำเนินการตามแผนปี ๒๕๖๑ | แนวทางในการดำเนินการในปี ๒๕๖๒ |
|---|---|---|---|---|
| | | (๒) การป้องกันการบุกรุก | - สผง.(ทส.) ติดตั้ง Firewall ป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต เข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรม<br>- สผง.(ทส.) ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ต และกลั่นกรองข้อมูลที่มาทาง Website<br>- สผง.(ทส.) มีเจ้าหน้าที่ดูแล ระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตว่ามีปริมาณมากผิดปกติหรือไม่ หรือมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้หาสาเหตุและการป้องกันต่อไประบบเครือข่ายภายในมีการแบ่ง VLAN เพื่อป้องกัน Packet ที่จะเกิดการ Broadcast หรือเกิดการรบกวนกันภายในเครือข่าย<br>- ระบบ IPS (Intrusion Prevention System) : อุปกรณ์การตรวจจับและป้องกันผู้บุกรุกในระบบ เครือข่าย เพื่อนำมาใช้ในการตรวจสอบ และป้องกันผู้บุกรุกจากภายนอกในระดับที่ละเอียดมากขึ้น สามารถเฝ้าดู กลั่นกรองข้อมูล หรือPacketที่มีลักษณะพฤติกรรมผิดปกติที่ถูกส่งมาจากภายนอก ซึ่ง IPS จะปิดกั้น (drop packet) นั้น ๆ ไม่ให้ผ่านเข้ามาใน เครือข่ายภายในของหน่วยงาน และจะ ส่งข้อความแจ้งเตือนให้ผู้ดูแลระบบทราบ | - ดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมเจ้าท่า<br>- ปรับปรุงระบบ Network ในส่วนของ Core Switch |

| ลำดับที่ | ประเด็น | มาตรการ | การดำเนินการตามแผนปี ๒๕๖๑ | แนวทางในการดำเนินการในปี ๒๕๖๒ |
|---|---|---|---|---|
| | | | - ปรับปรุงระบบรักษาความปลอดภัยของระบบเครือข่ายโดยดำเนินการจัดหา Next-Generation IPS เพื่อทดแทนของเดิม<br><br>- สผง.(ทส.) ดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ของบุคลากรของกรมเจ้าท่าในส่วนภูมิภาคเพื่อให้เป็นไปตามพ.ร.บ.ว่า ด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ โดยในการเก็บข้อมูลจราจรนั้นจะสามารถระบุรายละเอียดผู้เข้าใช้บริการระบบเครือข่ายเป็นรายบุคคลได้ (Identification and Authentication) และการเข้าใช้ระบบงานต่างๆของกรม โดยมีการตรวจสอบเป็นประจำและสม่ำเสมอ<br>- สผง.(ทส.) ได้มีการจัดทำโครงการจัดหาระบบสำรองข้อมูลนอกสำนักงาน และเพิ่มประสิทธิภาพของระบบเครือข่ายและระบบรักษาความปลอดภัย | - จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของบุคลากรของกรมเจ้าท่า โดยในการเก็บ ข้อมูลจราจรนั้นจะสามารถระบุรายละเอียดผู้เข้าใช้บริการระบบเครือข่ายเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server , Network Address และการเข้าใช้ระบบงานต่างๆของกรม โดยมีการตรวจสอบเป็นประจำและสม่ำเสมอ |

| ลำดับที่ | ประเด็น | มาตรการ | การดำเนินการตามแผนปี ๒๕๖๑ | แนวทางในการดำเนินการในปี ๒๕๖๒ |
|---|---|---|---|---|
| ๓ | มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access rights) | มาตรการพื้นฐานในการสร้างความปลอดภัยให้กับระบบ สารสนเทศ ในการกำหนดรหัสผ่าน มีหลักการดังนี้<br>(๑) กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้แก่ผู้ใช้งานอย่าง เหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีการกำหนดสิทธิให้บุคคลสามารถ เข้าถึงแต่ละระดับฐานข้อมูล ดังนี้<br>- บุคคลที่สามารถเรียกดูข้อมูล ได้เพียงอย่างเดียว จะไม่สามารถแก้ไขปรับปรุงข้อมูลได้<br>- บุคคลที่สามารถเรียกดูข้อมูลและสามารถแก้ไขปรับปรุงข้อมูลได้เฉพาะในส่วนที่ตนรับผิดชอบ<br>- บุคคลที่สามารถเรียกดู และสามารถแก้ไขปรับปรุงข้อมูล ในระดับ ฐานข้อมูลกำหนด ให้เจ้าหน้าที่ของฝ่าย เทคโนโลยีสารสนเทศเป็นผู้ดาเนินการ หรือผู้รับผิดชอบของหน่วยงานเจ้าของระบบงานมอบหมายในการเข้าใช้ฐานข้อมูล แต่ละระบบจะมีการกำหนดสิทธิการเข้าถึงฐานข้อมูลตามหน้าที่ความรับผิด ชอบ ของ | - สผง.(ทส.) ดำเนินการกำหนดสิทธิในการเข้าใช้เครื่องคอมพิวเตอร์แม่ข่าย , กำหนดสิทธิในการเข้าใช้ระบบงานต่างๆ โดยหากมีการเพิ่ม แก้ไข สิทธิการเข้าใช้ระบบงานต้องมีการจัดทำหนังสือขอเพิ่มหรือแก้ไขเป็นลายลักษณ์อักษร และปฏิบัติตามมาตรการพื้นฐานในการสร้างความปลอดภัยให้กับระบบ สารสนเทศในการกำหนดรหัสผ่าน<br>- สผง.(ทส.) มีระบบบริหารจัดการ ผู้ใช้งานเครือข่ายและอินเตอร์เน็ต (Active Directory) ตามโครงการจัดทำระบบคอมพิวเตอร์เพื่อรองรับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และได้ทำการกำหนด username/ password ให้กับผู้ใช้งานระบบ Internet เพื่อให้เป็นไปตามพ.ร.บ.ว่า ด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่ใช้ในการ Log in เข้าใช้งานระบบงานต่างๆ นั้น ทาง ทส. ได้ทำการจำกัดสิทธิ์การเข้าใช้ ระบบงานตามสถานะของผู้ใช้งานแต่ละฝ่าย โดยจะสามารถเข้าใช้งานได้ตามหน้าที่หรือหน่วยงานรับผิดชอบเท่านั้น ไม่สามารถเข้าใช้งานในส่วนอื่นๆที่ไม่เกี่ยวข้อง<br>- สผง.(ทส.) พัฒนาระบบระบบการตรวจสอบรหัสผ่านเดียว ในการควบคุมสิทธ์ผู้ใช้ในการเข้าถึงสารสนเทศ (Access Control) โดยทำหน้าที่ตรวจสอบสิทธิ์การเข้าใช้ระบบงานของผู้ใช้ (User) และการจัดการสิทธิ์การเข้าใช้งานของผู้ใช้ (User) | - สผง.(ทส.) มีการกำหนด username/ password ให้กับผู้ใช้งานระบบ Internet และระบบงานต่างๆ ซึ่ง ในส่วนของ username/ password ที่ใช้ในการ Log in เข้าใช้งานระบบงานต่างๆ นั้น ทาง ทส. ได้ทำการจำกัดสิทธิ์การเข้าใช้ ระบบงานตามสถานะของผู้ใช้งานแต่ละฝ่าย โดยจะสามารถเข้าใช้งานได้ตามหน้าที่หรือหน่วยงานรับผิดชอบเท่านั้น ไม่สามารถเข้าใช้งานในส่วนอื่นๆที่ไม่เกี่ยวข้อง โดยมีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ไว้ด้วย สามารถทำการตรวจสอบได้<br>- มีการให้ความรู้แก่ผู้ใช้ ระบบงาน ถึงข้อพึงระวังในการเก็บรักษา Username/ password เพื่อ ป้องกันผู้อื่นนำไปใช้<br>- ดำเนินการแจ้งหน่วยงานต่างๆ ทบทวนการใช้งาน Username/ password ของบุคลากร (โอน/ย้าย/ลาออก/เกษียณอายุ) ในการเข้าใช้ระบบงาน |

| ลำดับที่ | ประเด็น | มาตรการ | การดำเนินการตามแผนปี ๒๕๖๑ | แนวทางในการดำเนินการในปี ๒๕๖๒ |
|---|---|---|---|---|
| | | ผู้ใช้ฐานข้อมูลเพื่อรักษาความปลอดภัยของฐานข้อมูลด้วยมีการกำหนดชื่อผู้ใช้ Log in และรหัสผ่าน Password<br>(๒) กำหนดระยะเวลาการใช้งานระบบ สารสนเทศ ของผู้ใช้ระบบ (User) โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้ เมื่อพ้นระยะเวลาที่ กำหนดไว้<br>(๓) การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า ๖ ตัวอักษร และควรใช้ตัวเลข อักขระพิเศษประกอบ ผู้ใช้งานระบบสารสนเทศควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน การเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรซ้ำกับรหัสเดิม ผู้ใช้จะต้องเก็บรหัสผ่านไว้เป็นความลับ หากผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนใหม่ทันที | ทุกคนในแต่ละระบบงานได้ในคราวเดียวกัน | |

| ลำดับที่ | ประเด็น | มาตรการ | การดำเนินการตามแผนปี ๒๕๖๑ | แนวทางในการดำเนินการในปี ๒๕๖๒ |
|---|---|---|---|---|
| ๔ | การฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Back up and Recovery ) | (๑) การสำรองข้อมูล (Back up) | ๑. สผง.(ทส.) มีการสำรองข้อมูลในฐานข้อมูลเป็นประจำทุกวัน เก็บไว้ในหน่วยเก็บสำรองข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายของระบบนั้นๆ<br>๒. สผง.(ทส.) ทำการสำรองข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด เป็นประจำทุกวัน โดยจะมีการสำรองข้อมูลที่เพิ่มเติมในแต่ละวัน โดยจัดเก็บไว้ที่หน่วยเก็บสำรองข้อมูล ที่ติดตั้ง ณ อาคาร ๖ ชั้น ๔ และศูนย์สำรองข้อมูลนอกสำนักงาน ณ ศูนย์ฝึกพาณิชย์นาวี จ.สมุทรปราการ<br>๓. สผง.(ทส.) ทำการสำรองข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด เป็นประจำทุกสัปดาห์ โดยในแต่ละสัปดาห์ระบบจะดำเนินการสำรองข้อมูลทั้งหมดใหม่ทุกครั้ง โดยจัดเก็บไว้ที่หน่วยเก็บสำรองข้อมูล ที่ติดตั้ง ณ อาคาร ๖ ชั้น ๔ และและศูนย์สำรองข้อมูลนอกสำนักงาน ณ ศูนย์ฝึกพาณิชย์นาวี จ.สมุทรปราการ | - ดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมเจ้าท่า<br>- ดำเนินการตามแผนที่ได้ปฏิบัติในปี ๒๕๖๑ มีการสำรองข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด เป็นประจำทุกวัน ,ทำการสำรองข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด เป็นประจำทุกสัปดาห์ โดยในแต่ละสัปดาห์ระบบจะดำเนินการสำรองข้อมูลทั้งหมดใหม่ทุกครั้ง และในส่วนของข้อมูลในระบบงานต่างๆ จะมีการสำรองข้อมูลในฐานข้อมูลเป็นประจำทุกวัน เก็บไว้ในหน่วยเก็บสำรองข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายของระบบนั้นๆ |
| | | (๒) การกู้คืนข้อมูลจากความเสียหาย(Recovery ) | - สผง.(ทส.) ได้มีการจัดทำโครงการจัดหาระบบสำรองข้อมูลนอกสำนักงาน โดยการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แม่ข่ายไปยังศูนย์สำรองข้อมูลฯ แบบ Real Time ซึ่งหากระบบที่กรมเจ้าท่าส่วนกลางเสียหายแบบสิ้นเชิงจะสามารถนำระบบที่ศูนย์สำรองข้อมูลฯ เปิดใช้งานต่อไปได้ | |

# ภาคผนวก ณ.

แผนการบำรุงรักษาเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง และการแก้ไขปัญหาระบบงาน ในส่วนกลางและส่วนภูมิภาค

กลุ่มเทคโนโลยีสารสนเทศ

ทส ๒๙ มค ๒๕๖๒
14.59 น

สำนักแผนงาน
รับที่ 0442
วันที่ ๒๙ ม.ค. ๒๕๖๒
เวลา 10.24 น.

# บันทึกข้อความ

**ส่วนราชการ** สำนักแผนงาน กลุ่มเทคโนโลยีสารสนเทศ โทร. ๓๓๓, ๓๓๔, ๓๓๕

**ที่** คค ๐๓๑๙.๔/ทส.๒๕ **วันที่** ๒๙ มกราคม ๒๕๖๒

**เรื่อง** การจัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์ส่วนกลาง ประจำปีงบประมาณ ๒๕๖๒

(๑) เรียน ผสผ. (ผ่าน หทส.)

ตามตัวชี้วัดของ กลุ่มเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ ๒๕๖๒ "ตัวชี้วัดที่ ๑.๑๐ ระดับความสำเร็จเฉลี่ยถ่วงน้ำหนักของการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงในส่วนกลาง ให้เป็นไปตามแผน" นั้น

ในการนี้ กระผมในฐานะเป็นผู้รับผิดชอบในการดำเนินการตามตัวชี้วัดดังกล่าว ได้จัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงส่วนกลางประจำปีงบประมาณ ๒๕๖๒ เสร็จเรียบร้อยแล้ว (รายละเอียดตามแนบ)

จึงเรียนมาเพื่อโปรดทราบแผนการดำเนินงาน ก่อนดำเนินการตามแผนต่อไป

(นายอนุรักษ์ จอมแปงทา)
เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน

(นางสาววิศัลยา ปานเจริญ)
หทส.
๒๘ ม.ค. ๒๕๖๒

(๒) เรียน หทส.
ทราบ/ดำเนินการต่อไป
ผสผ.
(นางชนินทร วรวนาวงศ์)
ผสผ.
๒๙ ม.ค. ๒๕๖๒

เรียน คุณอนุรักษ์
เพื่อโปรดดำเนินการต่อไป
(นางสาววิศัลยา ปานเจริญ)
หทส.
๒๙ มค ๒๕๖๒

# แผนงานบำรุงรักษาเครื่องคอมพิวเตอร์ กรมเจ้าท่า ส่วนกลาง ประจำปีงบประมาณ ๒๕๖๒

| กิจกรรม | อาคาร ชั้น | ระยะเวลาดำเนินงาน | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ก.พ. | | | | มี.ค. | | | | เม.ย. | | | | พ.ค. | | | | มิ.ย. | | | | ก.ค. | | | |
| | | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ |
| ๑. การทำความสะอาด และบำรุงรักษาอุปกรณ์คอมพิวเตอร์ต่างๆ<br>เช่น เมาส์ คีย์บอร์ด จอภาพ และตัวเครื่องคอมพิวเตอร์<br>๒. ตรวจสอบการทำงานของระบบปฏิบัติการ<br>๒.๑ ทำการลบข้อมูลที่ไม่จำเป็น ซึ่งอาจทำให้มีเกิดผลเสียตามมา<br>ต่อระบบปฏิบัติการได้ (Disk Cleanup)<br>๒.๒ ทำการจัดเรียงข้อมูลของฮาร์ดิสเพื่อให้การเรียกใช้หรือค้นหาข้อมูลได้ รวดเร็วไม่ติดขัด (Defragmenter)<br>๒.๓ ปรับปรุง ปิดช่องโหว่ของระบบปฏิบัติการ (Patch Windows)<br>๓. ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัส<br>๔. ถ่ายถอดความรู้และแนะนำการใช้งาน<br>๔.๑ แนะนำการดูแลรักษาอุปกรณ์คอมพิวเตอร์เบื้องต้น<br>๔.๒ แนะนำการใช้งาน และแก้ไขปัญหาเบื้องต้น<br>๔.๓ แนะนำการใช้งานให้เป็นไปตามนโยบายการใช้เครื่องคอมพิวเตอร์และเครือข่าย และตาม พ.ร.บ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ | อ.๑ ช.๑ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๑ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๑ ช.๓ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๑ ช.๔ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๑ ช.๕ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๓ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๔ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๕ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๖ | | | | | | | | | | | | | | | | | | | | | | | | |
| | เอี่ยมละออ | | | | | | | | | | | | | | | | | | | | | | | | |
| | กสท. | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๖ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๖ ช.๓ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๖ ช.๔ | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๖ ช.๕ | | | | | | | | | | | | | | | | | | | | | | | | |

**หมายเหตุ** : รายงานภายใน ๗ วันทำการ หลังการบำรุงรักษาของแต่ละอาคารเสร็จเรียบร้อย

**ผู้รับผิดชอบ :**

นายอนุรักษ์ จอมแปงทา : เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน

นายบดีณัฐ นันทวัน ณ อยุธยา : เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน

นายศิริศักดิ์ นพศรี : เจ้าหน้าที่เครื่องคอมพิวเตอร์

นายมนตรพล ลาชะเกตุ : เจ้าหน้าที่เครื่องคอมพิวเตอร์

นายสุกฤษณ์ ช่อนกลิ่น เจ้าหน้าที่เครื่องคอมพิวเตอร์

# แผนการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงส่วนกลาง
# ประจำปีงบประมาณ ๒๕๖๒

## ที่มาและความสำคัญ

ปัจจุบันกรมเจ้าท่าได้ดำเนินการพัฒนาระบบสารสนเทศและระบบเครือข่ายเพื่อใช้ภายในหน่วยงานส่วนกลางและส่วนภูมิภาคในการปฏิบัติงานประจำ และให้บริการประชาชนส่งผลให้บุคลากรของกรมเจ้าท่าจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์ในการปฏิบัติงานมากขึ้น หากอุปกรณ์ดังกล่าวเกิดขัดข้อง ไม่สามารถใช้งานได้ จะส่งผลต่อการปฏิบัติงานการให้บริการประชาชน กลุ่มเทคโนโลยีสารสนเทศเทศ เป็นหน่วยงานที่รับผิดชอบโดยตรงในการให้คำปรึกษาเกี่ยวกับระบบงานคอมพิวเตอร์ การตรวจสอบและการแก้ไขปัญหาระบบงานที่เกี่ยวกับเทคโนโลยีสารสนเทศต่างๆ การซ่อมแซมเครื่องคอมพิวเตอร์ให้สามารถใช้งานได้ตามปกติ การที่จะทำให้ระบบเทคโนโลยีสารสนเทศกรมเจ้าท่าที่ได้ลงทุนพัฒนาให้สามารถตอบสนองต่อความต้องการของผู้ใช้งาน และผู้บริหารขององค์กรได้นั้น จำเป็นอย่างยิ่งที่อุปกรณ์คอมพิวเตอร์ต้องอยู่ในสภาพที่พร้อมใช้งานตลอดเวลา

จากความสำคัญและปัญหาข้างต้น กลุ่มเทคโนโลยีสารสนเทศ ในฐานะผู้รับผิดชอบในการ จัดหา พัฒนา ดูแลบำรุงรักษาระบบคอมพิวเตอร์ของกรมเจ้าท่า ซึ่งที่ผ่านมาได้จัดหาเครื่องคอมพิวเตอร์จัดสรรให้หน่วยงานในกรมเจ้าท่าเพื่อใช้ในการปฏิบัติงาน และดำเนินการพัฒนาในด้านโครงสร้างพื้นฐานการติดตั้งระบบเครือข่ายภายในหน่วยงานเพื่อรองรับการใช้งานครอบคลุมทุกอาคาร รวมทั้งการเชื่อมโยงกับสำนักงานส่วนภูมิภาคทุกแห่งโดยผ่านระบบเครือข่าย (MOTNET) ของกระทรวงคมนาคม และจัดหาพัฒนาระบบสารสนเทศต่างๆ เพื่อใช้ในการสนับสนุนการปฏิบัติงานราชการของกรมตลอดหลายปีที่ผ่านมา

ดังนั้นการบำรุงรักษาและซ่อมเครื่องคอมพิวเตอร์จึงมีบทบาทสำคัญอย่างยิ่ง กลุ่มเทคโนโลยีสารสนเทศ โดยเจ้าพนักงานเครื่องคอมพิวเตอร์ และเจ้าหน้าที่เครื่องคอมพิวเตอร์จึงได้ดำเนินการจัดทำแผนการบำรุงรักษาเครื่องคอมพิวเตอร์ ประจำปี ๒๕๖๒ ขึ้นมา

## วัตถุประสงค์

๑. เพื่อให้ผู้ปฏิบัติงานสามารถใช้ระบบสารสนเทศผ่านระบบเครือข่ายได้อย่างรวดเร็ว มีประสิทธิภาพ

๒. เพื่อควบคุมดูแล บำรุงรักษา ให้ระบบคอมพิวเตอร์ในองค์กรพร้อมใช้งานอยู่ตลอดเวลา รวมถึงการแก้ไขปัญหา ปรับปรุง เพื่อให้การใช้งานระบบคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๓. เพื่อตรวจสอบ บันทึก รวบรวมข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงให้มีความถูกต้อง และเป็นปัจจุบัน

๔. เพื่อเป็นการป้องกันปัญหาภัยคุกคามทางคอมพิวเตอร์และทางอินเตอร์เน็ต และป้องกันปัญหาไวรัสแพร่กระจายภายในระบบเครือข่าย

## ขอบเขตของงาน

เพื่อให้การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง เป็นไปตามวัตถุประสงค์ที่ตั้งไว้ ในการสนับสนุนการปฏิบัติงานให้ลักษณะการดำเนินงานเป็นไปด้วยความเรียบร้อยอย่างมีประสิทธิภาพ และสนองตามภารกิจของกรมเจ้าท่า ในการบริการประชาชน ได้อย่าง สะดวก รวดเร็ว ถูกต้อง และทันต่อเวลา จึงได้จัดทำแผนการบริการบำรุงรักษา ระบบคอมพิวเตอร์ อุปกรณ์ต่อพ่วง โดยดำเนินการดังนี้

๑. การทำความสะอาด และบำรุงรักษาอุปกรณ์คอมพิวเตอร์ต่างๆ เช่น เมาส์ คีย์บอร์ด จอภาพ และตัวเครื่องคอมพิวเตอร์

๒. ตรวจสอบการทำงานของระบบปฏิบัติการ

๒.๑ ทำการลบข้อมูลที่ไม่จำเป็น ซึ่งอาจทำให้มีเกิดผลเสียตามมาต่อระบบปฏิบัติการได้ (Disk Cleanup)

๒.๒ ทำการจัดเรียงข้อมูลเพื่อทำให้การเรียกใช้หรือค้นหาข้อมูลได้รวดเร็วยิ่งขึ้นอย่างไม่ติดขัด (Defragmenter)

๒.๓ ปรับปรุงปรับช่องโหว่ของระบบปฏิบัติการ (Patch Windows)

๓. ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัส

๔. ถ่ายถอดความรู้และแนะนำการใช้งาน

๔.๑ แนะนำการดูแลรักษาอุปกรณ์คอมพิวเตอร์เบื้องต้น

๔.๒ แนะนำการใช้งาน และแก้ไขปัญหาเบื้องต้น

๔.๓ แนะนำการใช้งานให้เป็นไปตามนโยบายการใช้เครื่องคอมพิวเตอร์และเครือข่าย และตาม พ.ร.บ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๕. บันทึก รวบรวมข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงให้มีความถูกต้อง และเป็นปัจจุบัน เช่น IP address, Hard disk, Ram, CPU, Operator System

ทั้งนี้ จะประสานหน่วยงานเพื่อให้เกิดความสะดวกในการปฏิบัติงาน ไม่ดำเนินการพร้อมกันทุกเครื่องในหน่วยงานนั้นๆ ซึ่งจะทำให้หน่วยงานไม่สามารถปฏิบัติงานได้

**ประโยชน์ที่คาดว่าจะได้รับ**

๑. ลดปัญหาข้อขัดข้องความเสียหายที่จะเกิดขึ้นกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายจนเกินกว่าที่จะแก้ไข

๒. เจ้าหน้าที่ของกรมฯ สามารถใช้เครื่องคอมพิวเตอร์ได้อย่างดีมีประสิทธิภาพ

๓. มีข้อมูลจำนวนการใช้งานเครื่องคอมพิวเตอร์ที่มีความถูกต้อง เป็นปัจจุบัน เพื่อนำมาเป็นข้อมูลในการตัดสินใจ จัดหาเครื่องคอมพิวเตอร์ทดแทน และเพิ่มเติมในปีงบประมาณต่อไป

**แผนงานบำรุงรักษาเครื่องคอมพิวเตอร์ กรมเจ้าท่า ส่วนกลาง ประจำปีงบประมาณ ๒๕๖๐**

| กิจกรรม | อาคาร ชั้น | ระยะเวลาดำเนินงาน | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ก.พ. | | | | มี.ค. | | | | เม.ย. | | | | พ.ค. | | | | มิ.ย. | | | | ก.ค. | | | | | |
| | | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ | ๑ | ๒ | ๓ | ๔ | | |
| ๑. การทำความสะอาด และบำรุงรักษาอุปกรณ์คอมพิวเตอร์ต่างๆ<br>เช่น เมาส์ คีย์บอร์ด จอภาพ และตัวเครื่องคอมพิวเตอร์<br>๒. ตรวจสอบการทำงานของระบบปฏิบัติการ<br>๒.๑ ทำการลบข้อมูลที่ไม่จำเป็น ซึ่งอาจทำให้มีเกิดผลเสียตามมา<br>ต่อระบบปฏิบัติการได้ (Disk Cleanup)<br>๒.๒ ทำการจัดเรียงข้อมูลของฮาร์ดิสเพื่อให้การเรียกใช้หรือค้นหาข้อมูลได้ รวดเร็วไม่ติดขัด (Defragmenter)<br>๒.๓ ปรับปรุง ปิดช่องโหว่ของระบบปฏิบัติการ<br>(Patch Windows)<br>๓. ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัส<br>๔. ถ่ายถอดความรู้และแนะนำการใช้งาน<br>๔.๑ แนะนำการดูแลรักษาอุปกรณ์คอมพิวเตอร์เบื้องต้น<br>๔.๒ แนะนำการใช้งาน และแก้ไขปัญหาเบื้องต้น<br>๔.๓ แนะนำการใช้งานให้เป็นไปตามนโยบายการใช้เครื่องคอมพิวเตอร์และเครือข่าย และตาม พ.ร.บ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ | อ.๑ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๑ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๑ ช.๓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๑ ช.๔ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๔ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๕ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๒ ช.๖ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๓ ช.๑ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๓ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๓ ช.๓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๓ ช.๔ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๔ ช.๑ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๔ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๔ ช.๓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๔ ช.๔ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๔ ช.๕ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๕ ช.๑ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๕ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๕ ช.๓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๕ ช.๔ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๕ ช.๕ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๖ ช.๒ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๖ ช.๓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๖ ช.๔ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | อ.๖ ช.๕ | | | | | | | | | | | | | | | | | | | | | | | | | | |

**หมายเหตุ** : รายงานภายใน ๗ วันทำการ หลังการบำรุงรักษาของแต่ละอาคารเสร็จเรียบร้อย

: กำหนดเวลาการบำรุงรักษาแล้วเสร็จในแต่ละอาคาร

**ผู้รับผิดชอบ :**

นายอนุรักษ์ จอมแปงทา : เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน

นายบดีณัฐ นันทวัน ณ อยุธยา : เจ้าพนักงานเครื่องคอมพิวเตอร์ปฏิบัติงาน

นายศิริศักดิ์ นพศรี : เจ้าหน้าที่เครื่องคอมพิวเตอร์

นายมนตรพล ลาชะเกตุ : เจ้าหน้าที่เครื่องคอมพิวเตอร์

**แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ**
**กรมเจ้าท่า**

## ๑. บทนำ

### ๑.๑ หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่าหรือต่อไปนี้เรียกว่า “กรม” เป็นไปอย่างเหมาะสมมีประสิทธิภาพมีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ กรมจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ โดยมีวัตถุประสงค์ดังต่อไปนี้

๑.๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของกรมทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒. เป็นบรรทัดฐานด้านความมั่นคงปลอดภัยในการดำเนินกิจการอันเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๓. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๑.๔. นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๕. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหารเจ้าหน้าที่ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมตระหนักถึงความสำคัญของการรักษาความมั่นคง ปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๖. เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงคุณภาพด้านความมั่นคงปลอดภัยสารสนเทศ

๑.๗. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

**๒. องค์ประกอบของนโยบาย**

**คำนิยาม**

**ส่วนที่ ๑** การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

**ส่วนที่ ๒** การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์

**ส่วนที่ ๓** การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

**ส่วนที่ ๔** การบริหารจัดการการเข้าถึงของผู้ใช้งาน

**ส่วนที่ ๕** การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

**ส่วนที่ ๖** การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

**ส่วนที่ ๗** การควบคุมการเข้าถึงระบบปฏิบัติการ

**ส่วนที่ ๘** การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

**ส่วนที่ ๙** การจัดทำระบบสำรองข้อมูล

**ส่วนที่ ๑๐** การตรวจสอบและประเมินความเสี่ยง

**ส่วนที่ ๑๑** นโยบายความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต

**ส่วนที่ ๑๒** แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์

**ส่วนที่ ๑๓** ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์

**ส่วนที่ ๑๔** การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

**ส่วนที่ ๑๕** นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

**การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ**

องค์ประกอบของนโยบายการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมเพื่อที่จะทำให้กรมมีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงานทรัพย์สินบุคลากรของกรม ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของกรมนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของกรม ซึ่งเจ้าหน้าที่ของกรม และหน่วยงานภายนอกต้องปฏิบัติตามอย่างเคร่งครัด

## คำนิยาม

**คำนิยามที่ใช้ในนโยบายนี้**

๑. **<u>กรม</u>** หมายถึง กรมเจ้าท่า

๒. **<u>การรักษาความมั่นคงปลอดภัย</u>** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมเจ้าท่า

๓. **<u>ผู้ใช้งาน</u>** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่าโดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role)

- ผู้บริหารระดับสูงสุด (Chief Executive Office : CEO) หมายความว่า อธิบดีกรมเจ้าท่า
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Office :CIO) หมายความว่า รองอธิบดีกรมเจ้าท่าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ
- เจ้าหน้าที่ หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ
- บุคคลภายนอก หมายความว่า บุคคลที่กรมเจ้าท่าอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่า ได้ชั่วคราวเพื่อประโยชน์ในการดำเนินงานของกรมเจ้าท่า ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดต่อหรือดูแลรักษาระบบให้กับกรมเจ้าท่าหรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง

๔. **<u>สิทธิของผู้ใช้งาน</u>** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๕. **<u>สินทรัพย์</u>** หมายถึง ข้อมูลระบบข้อมูลและทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือสิ่งใดก็ตามที่มีคุณค่าของหน่วยงาน เช่นอุปกรณ์ระบบเครือข่ายซอฟต์แวร์ที่มีลิขสิทธิเป็นต้น

๖. **<u>การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ</u>** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๗. **<u>ความมั่นคงปลอดภัยด้านสารสนเทศ</u>** หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๘. **<u>ความมั่นคงปลอดภัยด้านการบริหารจัดการ</u>** หมายถึง การกระทำในระดับบริหารโดยการจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในกระบวนการคัดเลือก การพัฒนา การนำไปใช้งาน หรือการบำรุงรักษาทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย

๙. **<u>ความมั่นคงปลอดภัยทางด้านกายภาพ</u>** หมายถึง การจัดให้มีนโยบาย มาตรการหลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

๑๐. **<u>เหตุการณ์ด้านความมั่นคงปลอดภัย</u>** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิด การฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๑๑. **<u>สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด</u>** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยคุกคาม

๑๒. **<u>หน่วยงานภายนอก</u>** หมายถึง องค์กรหรือหน่วยงานที่กรมเจ้าท่าอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงานโดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๓. **<u>รหัสผ่าน</u>** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๔. **<u>ข้อมูลคอมพิวเตอร์</u>** หมายถึง ข้อมูลข้อความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๕. **<u>ระบบเครือข่าย</u>** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของกรมได้ เช่นระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต (Internet)

- ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบคอมพิวเตอร์ต่างๆภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
- ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

๑๖. **<u>ระบบเทคโนโลยีสารสนเทศ</u>** (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหารการสนับสนุนการให้บริการการพัฒนา และควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบเช่นระบบคอมพิวเตอร์ระบบเครือข่ายโปรแกรมข้อมูลและสารสนเทศเป็นต้น

๑๗. **<u>พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร</u>** (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล
- พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
- พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

๑๘. **<u>เจ้าของข้อมูล</u>** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆหรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๑๙. **<u>จดหมายอิเล็กทรอนิกส์</u>** (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกันข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

๒๐. **<u>ชุดคำสั่งไม่พึงประสงค์</u>** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหายถูกทำลายถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงาน ไม่ตรงตามคำสั่งที่กำหนดไว้

## ส่วนที่ ๑
## การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
## (Information Security Management)

**๑. วัตถุประสงค์**

เพื่อกำหนดผู้รับผิดชอบที่ชัดเจน ในการดูแลกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดการเสียหาย หรืออันตรายใดๆ แก่กรมเจ้าท่า ในการหาแนวทาง ทบทวนแนวนโยบายและแนวปฏิบัติไปใช้ในการแก้ปัญหาที่เกิดขึ้น และนำไปสู่การปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้มีคุณภาพต่อไป

**๒. แนวทางในการบริหารจัดการ**

๒.๑. ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นจากการละเลยการควบคุม ความมั่นคงปลอดภัยสารสนเทศกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่กรมฯ หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยจัดให้มีการประชุมคณะกรรมการพัฒนาบริหารจัดการระบบสารสนเทศ โดยผู้บริหารสารสนเทศระดับสูง และผู้อำนวยการสำนัก/ศูนย์/กลุ่ม เพื่อทำการทบทวนและทราบถึงแนวนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ๑ ครั้ง ส่วนผู้บริหารสารสนเทศระดับสูง (CIO) เป็นผู้กำกับดูแลรับผิดชอบด้านสารสนเทศของกรมเจ้าท่า

๒.๒. ทำความเข้าใจ และให้การสนับสนุนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยจัดให้มีการทำรายงานการประชุมผู้บริหารสารสนเทศและแจ้งเป็นแนวปฏิบัติให้เจ้าหน้าที่ผู้เกี่ยวข้องรับทราบและปฏิบัติตามอย่างเคร่งครัด

๒.๓. จัดให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศของกรมเจ้าท่า

๒.๔. จัดให้มีการประเมินแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ เพื่อนำไปปรับปรุงให้มีประสิทธิภาพในปีถัดไป

๒.๕. กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศต้องจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์ของขอบเขตงานที่ได้รับการอนุมัติจากผู้บริหารระดับสูงสุด (CEO) หรือผู้บริหารสารสนเทศระดับสูง (CIO) เพื่อประกาศใช้และถือปฏิบัติในกรมเจ้าท่า โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นของกรมเจ้าท่า ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของกรมเจ้าท่า

๒.๖. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยในแต่ละปีงบประมาณซึ่งรวมถึงแผนความมั่นคงปลอดภัยสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย

๒.๗. จัดให้มีการอบรมให้ความรู้ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้กับข้าราชการ พนักงานราชการ และเจ้าหน้าที่ เพื่อสร้างความตระหนักและความเข้าใจภัยและ

ผลกระทบที่จะเกิดขึ้น จากการใช้ระบบงานสารสนเทศโดยไม่ระมัดระวังหรือไม่เท่าถึงการณ์ อย่างน้อยปีละ ๑ ครั้ง

๒.๘. จัดให้มีการตรวจสอบและประเมินความเสี่ยงในการปฏิบัติ ปีละ ๑ ครั้งและจัดให้มีการทำแผนการปรับปรุง เพื่อทบทวนหรือแก้ไขปัญหาที่พบ

๒.๙. จัดให้มีการอบรมให้ความรู้และซักซ้อมแผนฉุกเฉินภัยพิบัติของประเทศของระบบเทคโนโลยีสารสนเทศ (IT Contingence plan) อย่างน้อยปีละ ๑ ครั้ง

๒.๑๐. กำหนดหน้าที่ที่ต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ และกำหนดหน้าที่รับผิดชอบของบุคลากรที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ และแผนฉุกเฉินภัยพิบัติของระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่า

๒.๑๑. ผู้บริหาร ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และ พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

## ส่วนที่ ๒
## การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์
## (Computing System Control Room)

**๑. วัตถุประสงค์**

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้ จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของกรม

**๒. การควบคุมการเข้าออก**

๒.๑. ภายในกรมมีการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) เพื่อควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย โดยจำแนกและกำหนดพื้นที่การติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) เป็น ๓ ส่วน โดยส่วนที่ ๑ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) บริเวณทางเข้าศูนย์คอมพิวเตอร์ ส่วนที่ ๒ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และส่วนที่ ๓ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) ห้อง Facility เพื่อจุดประสงค์ในการควบคุมการเข้าออกของบุคคลภายนอก โดยใช้เทคโนโลยีระบบ Biometric Finger Scan และ Proximity Card

๒.๒. ภายในกรมมีการติดตั้งระบบกล้องวงจรปิด เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้

๒.๓. ต้องกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถมีมีสิทธิในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายประกอบด้วย

๒.๓.๑. จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

๒.๓.๒. กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออก ดังกล่าวโดยจัดทำเป็นเอกสาร“บันทึกการเข้าออกพื้นที่”

๒.๓.๓. จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร ปีละ ๑ ครั้ง เป็นอย่างน้อย

๒.๔. บุคคลภายนอกเข้ามาติดต่อจะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้า-ออกให้ถูกต้องและจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๒.๕. บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

## ส่วนที่ ๓
## การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
## (Access Control)

**๑. วัตถุประสงค์**

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม ได้อย่างถูกต้อง

**๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบ**

๒.๑. สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศ ที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๒.๒. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๒.๔. ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของกรมและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๒.๕. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และ การผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

**๓. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ**

๓.๑. ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้นจะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

๓.๒. เจ้าของข้อมูลและ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้นเนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๓. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

**๔. การบริหารจัดการการเข้าถึงของผู้ใช้**

๔.๑. การลงทะเบียนเจ้าหน้าที่ใหม่ของกรมควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่างๆในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่นเมื่อลาออกไปต้องทำภายใน ๒๔ ชั่วโมงหรือ เมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน

๔.๒. กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๔.๓. ผู้ใช้ต้องลงนามรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๔.๔. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

๔.๔.๑.ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสาร“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๔.๔.๒.การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตาม“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๔.๔.๓.กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๔.๔.๓.๑. ควรได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้นๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ

๔.๔.๓.๒. ควรควบคุมการใช้งานอย่างเข้มงวดเช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

๔.๔.๓.๓. ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

๔.๔.๓.๔. ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือนเป็นต้น

๔.๕. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๔.๕.๑. ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูลวีธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๕.๒. เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔.๕.๓. วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๔.๕.๔. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๔.๕.๕. ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๔.๕.๖. ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรม เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อ บันทึกก่อน เป็นต้น

**๕. การบริหารจัดการการเข้าถึงระบบเครือข่าย**

๕.๑. ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งานกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่าง เป็นระบบ

๕.๒. ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๓. ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๕.๔. ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆได้ กำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต่างๆของระบบ

๕.๕. ป้องกันเครือข่ายและอุปกรณ์ต่างๆที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและควรทบทวนการกำหนดค่า Parameter ต่างๆอย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลง ค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๖. ระบบเครือข่ายทั้งหมดของกรมที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกกรม ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๕.๗. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรม ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๕.๘. การเข้าสู่ระบบงานเครือข่ายภายในกรมโดยผ่านทางอินเทอร์เน็ต จำเป็นต้องมีการล๊อกอิน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๕.๙. IP address ภายในของระบบงานเครือข่ายภายในของกรม จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๕.๑๐. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๑๑. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๑๒. การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ สำนักแผนงานเท่านั้น

**๖. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย**

๖.๑. ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือ เปลี่ยนแปลงค่าต่างๆของโปรแกรมระบบ (System Software) อย่างชัดเจน

๖.๒. ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งาน หรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

๖.๓. ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้นเช่น Telnet ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

๖.๔. ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่างๆของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น web server เป็นต้น

๖.๕. ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพ การใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๖.๖. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศเท่านั้น

**๗. การบริหารจัดการการบันทึกและตรวจสอบ**

๗.๑. ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๗.๒. ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๗.๓. ต้องมีมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆและจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

**๘. การควบคุมการเข้าใช้งานระบบจากภายนอก**

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กรเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติดังนี้

๘.๑. การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายของกรม ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของกรม จากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๘.๒. วิธีการใดๆก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ หรือผู้อำนวยการ สำนักแผนงาน ก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของกรมในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๘.๓. การทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกลผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๘.๔. ต้องมีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๘.๕. การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้ เมื่อมีการร้องขอที่จำเป็นเท่านั้น

**๙. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก**

๙.๑. ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กรดังนี้

๙.๑.๑. แสดงชื่อผู้ใช้งาน (Username)

๙.๑.๒. ใส่รหัสผ่าน (Password)

## ส่วนที่ ๔
## การบริหารจัดการการเข้าถึงของผู้ใช้งาน
## (User Access Management)

**๑. วัตถุประสงค์**

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม

**๒. การลงทะเบียนผู้ใช้งาน (User Registration)**

๒.๑. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศของกรม

๒.๒. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยเฉพาะผู้ที่ไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๒.๓. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๒.๔. ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๒.๕. ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๒.๖. การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

**๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)**

๓.๑. ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๒. ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ

๓.๓. ผู้ดูแลระบบต้องมอบหมายสิทธิควรมีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

๓.๔. ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๓.๕. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

**๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)**

๔.๑. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศของกรม

๔.๒. ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๔.๓. ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

๔.๔. ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น และควรกำหนดรหัสผ่านที่แตกต่างกัน

๔.๕. ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง และควรกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

**๕. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)**

๕.๑. ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ๑ ครั้ง / ปี เป็นอย่างน้อย

๕.๒. ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๕.๓. ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

๕.๔. ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

## ส่วนที่ ๕
## การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
## (User Responsibilities)

**๑. วัตถุประสงค์**

เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรม เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

**๒. การใช้งานรหัสผ่าน (Password Use)**

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

๒.๑. ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

๒.๒. ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

๒.๓. ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๒.๔. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๒.๕. ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำกำหนดไว้

๒.๖. ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

๒.๗. ผู้ใช้งานไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

๒.๘. ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓ , abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑ , aaa เป็นต้น

๒.๙. ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

๒.๑๐. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๒.๑๑. ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุกๆ ๓ เดือน สำหรับผู้ดูแล และ ๖ เดือน สำหรับผู้ใช้งานระบบ

๒.๑๒. ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล๊อคอินเข้าสู่ระบบงาน

๒.๑๓. ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล๊อคอินในภายหลัง

๒.๑๔. ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

๒.๑๕. ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ใช้งาน

**๓. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์**

๓.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องโน๊ตบุ๊ก

๓.๒ ผู้ใช้งานควรล๊อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๓.๓ ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

## ส่วนที่ ๖
## การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
## (Network Access Control)

**๑. วัตถุประสงค์**

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้ แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมโดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่างๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

**๒. กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย**

๒.๑ การใช้งานบริการเครือข่าย

๒.๑. ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรม

๒.๒. กรม ไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และ เครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อ แสวงหากำไร

๒.๓. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรมฯ ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๒.๔. ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้าม ของทางราชการ

๒.๕. กรม ให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๒.๖. บัญชีผู้ใช้งาน (User Account) ที่กรมฯ ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๒. ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่กรมมีแนวทางปฏิบัติดังนี้

๒.๒.๑. ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุม ระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก

“ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๒.๒.๒. สิทธิในการเข้าออกห้องต่างๆภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ เป็นลายลักษณ์อักษรโดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายห้องควบคุมระบบเครือข่าย

๒.๒.๓. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย จัดเก็บลายนิ้วมือเจ้าหน้าที่ผ่านเครื่องจัดเก็บลายนิ้วมือ และบันทึกข้อมูลลงคีย์การ์ด เพื่อบันทึกประวัติการเข้า-ออก ห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่

๒.๒.๔.กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายต้องทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย

๒.๒.๕. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องหลังจากดำเนินการเสร็จ ให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง

๒.๓. ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติดังนี้

๒.๓.๑. ผู้ติดต่อจากหน่วยงานภายนอกต้องทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย

๒.๓.๒. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งผู้ติดต่อจากหน่วยงานภายนอกหลังจากดำเนินการเสร็จ ให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง

## ส่วนที่ ๗
## การควบคุมการเข้าถึงระบบปฏิบัติการ
## (Operating System Access Control)

**๑. วัตถุประสงค์**

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

**๒. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย**

๒.๑. ผู้ใช้งานควรกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๒.๒. ผู้ใช้งานควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๓. ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

๒.๔. ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๕. ผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

**๓. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)**

๓.๑ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓.๒ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๓ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๓.๔ ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

## ส่วนที่ ๘
## การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
## (Application Information Access Control)

**๑. วัตถุประสงค์**

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของกรม และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม ได้อย่างถูกต้อง

**๒. การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)**

๒.๑. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของกรม ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๓. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๒.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๓.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๒.๓.๓ กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๒.๓.๔ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหนง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๔. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๔.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๔.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๒.๔.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๔.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

## ส่วนที่ ๙

## การจัดทำระบบสำรองข้อมูล

**๑.วัตถุประสงค์**

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและกู้คืนระบบ โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูล ได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

**๒.แนวปฏิบัติงานการสำรองข้อมูลและระบบคอมพิวเตอร์**

๒.๑. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของกรม

๒.๒ การจัดทำบันทึกการสำรองข้อมูล ( Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

๒.๓ การรายงานข้อผิดพลาด ( Fault logging ) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๒.๔ ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

๒.๕ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ

๒.๖ ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๒.๗ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล ( Encrypted backup ) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สาคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๒.๘ นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล ( Backup Policy ) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

**การปฏิบัติเกี่ยวกับการสำรองข้อมูล**

๑.๑ ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการ ตามความถี่ดังนี้

| | รายการ | ข้อมูลที่ต้องสำรอง | ความถี่ในการสำรองข้อมูล |
|---|---|---|---|
| | Web servers | ค่า configure | ก่อนและหลังการเปลี่ยนแปลง |
| | | ข้อมูลเผยแพร่บนเว็บไซต์ | ๑ ครั้งต่อสัปดาห์ |
| | Database servers | ค่า configure | ก่อนและหลังการเปลี่ยนแปลง |

| | รายการ | ข้อมูลที่ต้องสำรอง | ความถี่ในการสำรองข้อมูล |
|---|---|---|---|
| | | ข้อมูลในฐานข้อมูลของระบบที่สาคัญ | ๑ ครั้งต่อสัปดาห์ |
| | Firewall , Proxy , IPS , DNS , CoreSwitch | ค่า configure | ก่อนและหลังการเปลี่ยนแปลง |
| | | ข้อมูล Rule ของอุปกรณ์ | ๑ ครั้งต่อเดือน |
| | Server อื่น ๆ เช่น ระบบงานต่างๆ | ค่า configure | ก่อนและหลังการเปลี่ยนแปลง |
| | | ข้อมูลบนเซิร์ฟเวอร์อื่น ๆ | ๑ ครั้งต่อเดือน |
| **หมายเหตุ** ทุกรายการที่ปรากฏในตารางจะใช้วิธีแบคอัพแบบ Full Backup | | | |

๑.๒ ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบคอัพ ตามรายละเอียด ในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

**๓. การกู้คืนระบบ**

๓.๑ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบ เครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/ หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้ รายงานสรุปผลการปฏิบัติงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบ

๓.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๓.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

**๔. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)**

นโยบายเกี่ยวกับการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ต้องมอบหมายให้บุคลากรที่เกี่ยวข้องดำเนินการดังต่อไปนี้

๔.๑ กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสาหรับระบบที่มีความสำคัญสูง

๔.๒ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสาคัญสูงและจำเป็นต้องวางแผนรับมือ

๔.๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๔.๔ จัดทำแผนรับมือกับเหตุภัยพิบัติสาหรับระบบที่มีความสำคัญสูง

๔.๕ ทดสอบ/ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสาหรับระบบที่มีความสาคัญสูง อย่างน้อยปีละ ๑ ครั้ง

## ส่วนที่ ๑๐
## การตรวจสอบและประเมินความเสี่ยง

**๑.วัตถุประสงค์**

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

**๒.แนวปฏิบัติการประเมินความเสี่ยง**

๒.๑. ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของกรม เพื่อการประเมินความเสี่ยงนั้น

๒.๒.๑ ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย เนื่องจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error), ไวรัสคอมพิวเตอร์ (Computer Virus), ระบบไฟฟ้าขัดข้อง, ความเสียหายจากเพลิงไหม้ , โจรกรรม และการขโมยอุปกรณ์คอมพิวเตอร์

๒.๒.๒ ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย เนื่องจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)

๒.๒ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๒.๓ การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๒.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๒.๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๒.๓.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๒.๔ กำหนดมาตรการจัดการความเสี่ยง

๒.๔.๑ ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)

๒.๔.๒ จัดทำหลักเกณฑ์นโยบายกฎระเบียบในการใช้เครื่องคอมพิวเตอร์และเครือข่ายของกรม

## ส่วนที่ ๑๑
## นโยบายความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต
## (Internet Security Policy)

**๑. วัตถุประสงค์**

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุขทำให้ระบบคอมพิวเตอร์ของกรมถูกระงับชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

**๒. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต**

๒.๑. ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่กรมจัดสรรไว้เท่านั้นเช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากกลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน เป็นลายลักษณ์อักษร

๒.๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

๒.๓. ผู้ใช้ หมั่น Update Patch และ HotFix อย่างสม่ำเสมอ โดยสามารถ Download patch และ HotFix ต่างๆ จาก Microsoft web site เพื่อแก้ปัญหาช่องโหว่

๒.๔. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๒.๕. ผู้ใช้ ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของกรม เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมเช่นเว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๒.๖. ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกรม

๒.๗. ผู้ใช้ ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับกรม

๒.๘. ห้ามผู้ใช้ เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมที่ยังไม่ได้ประกาศอย่างเป็นทางการ ผ่านอินเทอร์เน็ต

๒.๙. ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย

๒.๑๐. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

## ส่วนที่ ๑๒
## แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์
## (Use of Electronic Mail)

**๑. วัตถุประสงค์**

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรม สามารถสนับสนุนการปฏิบัติงานของกรมเจ้าท่า และการบริหารงานของกรมเจ้าท่า เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ และประสิทธิผล

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สำหรับบุคลากรของกรม และหน่วยงาน เป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ ของกรมเจ้าท่า

**๒. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์**

๒.๑. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอเช่น การลาออกเป็นต้น

๒.๒. ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม

๒.๓. สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (default password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๒.๔. รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษร

๒.๕. ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๒.๖. ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ควรมีการล็อกเอ้าท์ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

๒.๗. ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

๒.๘. ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดเช่นควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๒.๙. ผู้ใช้ ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อกรม หรือ ละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมายหรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรม

๒.๑๐. ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านรับส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆในจดหมายอิเล็กทรอนิกส์ของตน

๒.๑๑. ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของกรมเพื่อการทำงานของกรมเท่านั้น

๒.๑๒. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรทำการล็อกเอ้าท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๒.๑๓. ผู้ใช้ ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

๒.๑๔. ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๒.๑๕. ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมข้อมูลอันอาจทำให้เสียชื่อเสียงของกรมทำให้เกิดความแตกแยกระหว่างกรมผ่านทางจดหมายอิเล็กทรอนิกส์

๒.๑๖. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๑๗. ผู้ใช้ ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒.๑๘. ผู้ใช้ ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

**ส่วนที่ ๑๓**

**ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์**

**(Terms of Use and Disclaimer)**

**๑. วัตถุประสงค์**

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรม สามารถสนับสนุนการปฏิบัติงานของกรม เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์ สำหรับบุคลากรของ กรม และหน่วยงาน เป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของกรมเจ้าท่า

**๒. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม**

๒.๑ ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของกรม จะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ อย่างน้อยดังต่อไปนี้

๒.๑.๑ พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๒.๑.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔

๒.๑.๓ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐

๒.๑.๔ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๒.๑.๕ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗

๒.๑.๖ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติเกี่ยวกับการสื่อสาร พ.ศ.๒๕๒๕

๒.๑.๙ ข้อตกลง เงื่อนไขการใช้บริการที่กรม กำหนด

**๓. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม**

๓.๑ หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม จะต้องใช้จดหมายอิเล็กทรอนิกส์ของกรม เพื่อผลประโยชน์ของทางราชการ

๓.๒ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม เพื่อการประกอบธุรกิจ หรือแสวงหาผลประโยชน์ส่วนตน

๓.๓ ห้ามใช้บริการนี้ ไปในการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใดๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และ พระมหากษัตริย์

๓.๔ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม ในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำการใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูล ข่าวสารลับของทางราชการ

๓.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม เพื่อการเผยแพร่ข้อมูลข่าวสาร หรือภาพ เสียง ข้อความ ที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น

๓.๖ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบ หรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือองค์กร

๓.๗ ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)

๓.๘ ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น

(๑) การสร้างจดหมายลูกโซ่ (Chain mail)

(๒) การส่งจดหมายจำนวนมาก (Spam mail)

(๓) การส่งจดหมายต่อเนื่อง (Letter bomb)

(๔) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

๓.๙ ห้ามผู้ใช้บริการกระทำการใดๆ ที่อาจจะนำมาซึ่งความเสื่อมเสีย หรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของ กรม

๓.๑๐ ผู้ใช้ต้องรักษารหัสผ่าน(Password) ส่วนบุคคล หรือหน่วยงานของจดหมายอิเล็กทรอนิกส์เป็นไว้เป็นความลับ

๓.๑๑ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของกรม

๓.๑๒ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานนอกกรมจะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่กรม กำหนด

๓.๑๓ ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail address) และรหัสผ่าน(Password) ของหน่วยหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับหากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)

๓.๑๔ ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ กรมหรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ และ ขอตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของกรม ได้อย่างถูกต้อง

๓.๑๕ กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับบริการแก่สมาชิกนั้นๆ เป็นการชั่วคราวเพื่อทำการสอบสวน และตรวจสอบหาสาเหตุของมูลเหตุนั้นๆ

๓.๑๖ การกระทำใดๆ ที่เกี่ยวกับการเผยแพร่ ทั้งในรูปแบบของอีเมล์ และ/หรือโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการ กลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน ไม่มีส่วนเกี่ยวข้องใดๆ

## ส่วนที่ ๑๔
## การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
## (Third party access control)

**๑. วัตถุประสงค์**

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่นความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้องและการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้นเพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการคัดเลือกควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่นการพัฒนาระบบการใช้บริการของที่ปรึกษาการใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกเป็นต้น

**๒. แนวทางปฏิบัติ**

๒.๑. หัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยี สารสนเทศและการสื่อสารหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

๒.๒. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๒.๒.๑. บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากหัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน

๒.๒.๒. จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อยดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
- การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๒.๒.๓. หน่วยงานภายนอกที่ทำงานให้กับกรม ทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในกรม หรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของกรม โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๒.๒.๔. กรมควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอกทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่เข้าไปปฏิบัติงาน

๒.๒.๕. เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๒.๒.๖. สำหรับโครงการขนาดใหญ่หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของกรม ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้านคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความ พร้อมที่จะให้บริการ (Availability)

๒.๒.๗. กรมมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจได้ว่ากรมสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๒.๒.๘. ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงานคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวดเพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขต ที่ได้กำหนดไว้

## ส่วนที่ ๑๕
## นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย
## (Wireless Policy)

**๑. วัตถุประสงค์**

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการ กำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

**๒. แนวทางปฏิบัติ**

๑. ผู้ดูแลระบบเครือข่ายไร้สายมีหน้าที่ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๑.๑. เครือข่ายของกรมเจ้าท่าเป็นสมบัติของกรมเจ้าท่า ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้าม ต้องได้รับโทษจากทางกรมเจ้าท่าและรับโทษตามกฎหมาย

๑.๒. ผู้ดูแลระบบต้องวางตัวกระจายสัญญาณไร้สาย Access Point ในตำแหน่งที่เหมาะสม โดยไม่ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายของกรมเจ้าท่า

๑.๓. การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องติดตั้งโดยการแยกเครือข่ายไร้สายออกจากระบบเครือข่ายภายใน LAN เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก

๑.๔. การกำหนดการเข้าถึงระบบเครือข่ายไร้สาย ต้องแบ่งแยกการใช้งานให้แตกต่างกันตามความจำเป็นของผู้ใช้งาน และกำหนดรหัสการเข้าใช้งานตามวัตถุประสงค์ของการใช้งาน

๑.๕. ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และ รหัสผ่าน (Password) ที่กำหนดไว้เท่านั้น

๑.๖. ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่ามาจากโรงงานผู้ผลิต และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

๑.๗. ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับ อนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๑.๘. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของ ระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้น ในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และ ในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแล ระบบรายงานให้ผู้อำนวยการสำนักแผนงานทราบทันที

๒. ผู้ใช้งานระบบเครือข่ายไร้สายกรมเจ้าท่ามีหน้าที่ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๒.๑. ห้ามผู้ใช้งาน นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

๒.๒. กรมเจ้าท่าให้บัญชีผู้ใช้งานเป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน จำหน่าย หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๒.๓. บัญชีผู้ใช้งานที่กรมเจ้าท่าให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งานนั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๔. ห้ามผู้ใช้งานปฏิบัติการใดๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรมเจ้าท่า

๒.๕. กรมเจ้าท่าไม่อนุญาตให้ผู้ใช้งานทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไร ผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๒.๖. ผู้ใช้งานจะต้องไม่อ่าน, เขียน, ลบ, เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของผู้อื่น หรือพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัย รวมไปถึงเข้าสู่เครื่องคอมพิวเตอร์ของหน่วยงานในกรมเจ้าท่าหรือหน่วยงานอื่นๆ การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรมเจ้าท่าไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๒.๗. ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไข ในการรับทราบกฎระเบียบ หรือนโยบายต่างๆ ที่กรมเจ้าท่ากำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบ หรือนโยบายของกรมเจ้าท่ามิได้

๒.๘. กรมเจ้าท่าทรงไว้ซึ่งสิทธิที่จะปฏิเสธการเชื่อมต่อและ/หรือการใช้งาน และทรงไว้ซึ่งสิทธิที่จะยกเลิกหรือระงับการเชื่อมต่อและ/หรือการใช้งานใดๆ ของผู้ใช้งานที่ล่วงละเมิดหรือพยายามจะล่วงละเมิดกฎระเบียบนี้ของกรมเจ้าท่าโดยไม่มีการแจ้งให้ทราบก่อนล่วงหน้า

## การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

**๑. ระบบป้องกันผู้บุกรุก**

**แผนดำเนินการรายวัน**

๑. **ดำเนินการตรวจสอบไฟล์ล็อกหรือรายงานของระบบป้องกันการบุกรุก** สิ่งที่ทำการตรวจสอดังต่อไปนี้

๑.๑ การโจมตีเกิดขึ้นมากน้อยเพียงใด การโจมตีประเภทใดเกิดขึ้นเป็นจำนวนมาก

๑.๒ ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่

๑.๓ ระดับความรุนแรงมากน้อยเพียงใด

๑.๔ หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

**๒. ระบบไฟร์วอลล์**

๑. ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

๒. ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟล์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๒.๑ Packet ที่ไฟล์วอลล์ได้ทำการ Block

๒.๒ ลักษณะของ Packet ที่ถูก Block

๒.๓ Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๓. กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

**๓. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต**

ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์

แผนดำเนินการรายวัน/รายสัปดาห์/รายเดือน

๑. ดำเนินการตรวจสอบไฟล์ล็อกและรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต สิ่งที่ควรตรวจสอบมีดังนี้

๑.๑ มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก

๑.๒ มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด

๑.๓ มีการส่งมัลแวร์จากเครือข่ายภายในกรม ไปยังภายนอกหรือไม่

๒. ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของกรม

๓. ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ควรระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที