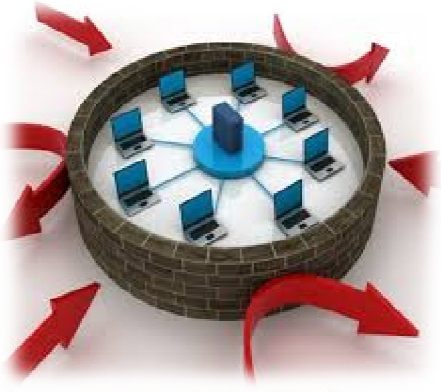
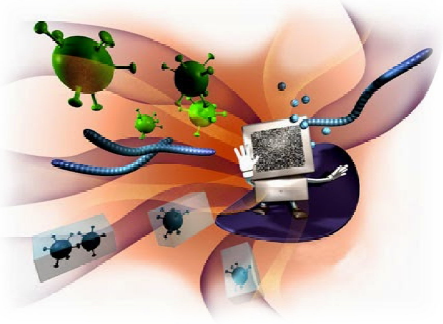
แผนเผชิญเหตุระบบสารสนเทศ กบ.ทร.





แผนเผชิญเหตุระบบสารสนเทศ กบ.ทร.

๑. หลักการและเหตุผล

๒. วัตถุประสงค์

๓. การประเมินความเสี่ยง

๔. แผนจัดการความเสี่ยง (Risk management action plan)

๓. แผนเผชิญเหตุภัยพิบัติต่าง ๆ

๖. การสำรอง (Backup) ระบบสารสนเทศและฐานข้อมูล

๑. หลักการและเหตุผล

ระบบการบริหารความเสี่ยงของระบบสารสนเทศ กบ.ทร. ปีงบประมาณ ๒๕๕๘

นิยาม ความเสี่ยง คือ เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหายหรือความล้มเหลวหรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมาย

นิยาม ระบบสารสนเทศ คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลข้อมูลทั้งภายในและภายนอกองค์กร และการนำเสนอสารสนเทศ สำหรับปีงบประมาณ ๒๕๕๘ จะพิจารณาระบบข้อมูล ทั้งหมดของ กบ.ทร. ได้แก่

๑. ข้อมูลและระบบฐานข้อมูลจากปีงบประมาณ ๒๕๕๘

ลำดับ	Software/Hardware	ระบบสารสนเทศ	ลักษณะการใช้งาน
๑.	Notebook/PC	การใช้ห้องประชุม กบ.ทร.	Font Office
๒.	i.navy.mi.th	ปฏิทินรวม กบ.ทร.	Font Office
๓.	i.navy.mi.th	ปฏิทินรวมการปฏิบัติของผู้บังคับบัญชา	Font Office
๔.	i.navy.mi.th	การปฏิบัติราชการของผู้บังคับบัญชา	Font Office
๕.	i.navy.mi.th	การปฏิบัติราชการของ นขต.กบ.ทร.	Font Office
๖.	i.navy.mi.th/SMS/Facebook/Line	ประกาศภายใน กบ.ทร.	Data Base
๗.	Shared PC	สร้างโฟลเดอร์สำหรับเก็บงานที่สำคัญ	Data Base
๘.	i.navy.mi.th	การนัดหมายการประชุม	Font Office
๙.	Web Server - Database Server	ระบบผ่านทางเครือข่ายภายนอก ทร.	Gateway
๑๐.	Web Server - Database Server	Web กบ.ทร. (Intranet)	Web
๑๑.	Web Server - Database Server	Web กบ.ทร. (Internet)	Web
๑๒.	External HD/PC หน่วย	ข้อมูลภายใน นขต.กบ.ทร.	File Management

องค์ประกอบของระบบคอมพิวเตอร์

๑. Hardware หมายถึง อุปกรณ์ต่างที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช่คอมพิวเตอร์

๒. Software หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน

๓. บุคลากร หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้นำ จักการข้อมูล และนำผลลัพธ์ออกจากระบบคอมพิวเตอร์

๔. ข้อมูลและแฟ้มข้อมูล หมายถึงข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง

๕. หน้าที่การปฏิบัติงาน หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

- องค์กร โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานขององค์กรโดยรวม ไม่ว่าจะเป็นฝ่ายต่างๆขององค์กร
- บุคลากร บุคลาการที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากรที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์

- เทคโนโลยี อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

หมายเหตุ องค์ประกอบของระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์ในการบริหาร จึงประกอบด้วยองค์ประกอบของทั้งสองระบบรวมกัน

นิยาม ความเสี่ยงของระบบสารสนเทศ คือ เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหายหรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จ ต่อการบริหารงานของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการบริหาร

๒. วัตถุประสงค์

<u>ข้อปฏิบัติการใช้งานระบบสารสนเทศของ กบ.ทร.</u>

ปัจจุบันการใช้ระบบสารสนเทศเป็นไปอย่างแพร่หลาย และมีการเชื่อมโยงระบบคอมพิวเตอร์และ การสื่อสารร่วมกันเป็นเครือข่ายเพิ่มมากขึ้น ซึ่งก่อให้เกิดความสะดวกในการเชื่อมโยงข้อมูลเพื่อการสืบค้น การแลกเปลี่ยนข้อมูล การติดต่อสื่อสารและการใช้ทรัพยากรร่วมกัน ขณะเดียวกันปัญหาการบุกรุกระบบคอมพิวเตอร์และเครือข่าย การเข้าถึงข้อมูลสำคัญจากผู้ไม่ประสงค์ดีหรือไมมีหน้าที่เกี่ยวข้อง การติดไวรัสคอมพิวเตอร์ หรือการได้รับจดหมายอิเล็กทรอนิกส์ที่ไม่พึงประสงค์รวมทั้งภัยคุกคามทางคอมพิวเตอร์และอาชญากรรมทางคอมพิวเตอร์ได้ทวีความรุนแรงเพิ่มมากขึ้นและแนวโน้มที่จะเพิ่มขึ้นอีกในรูปแบบที่หลากหลาย เพื่อเป็นการริเริ่มสร้างมาตรฐานการรักษาความปลอดภัยระบบสารสนเทศ ในระดับของผู้ใช้งานให้ตระหนักถึงความสำคัญและความจำเป็นของการรักษาความปลอดภัย และการใช้ประโยชน์ร่วมกันในระบบสารสนเทศของกบ.ทร. และนำไปสู่การพัฒนาและจัดทำเป็นแนวนโยบายและ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ กบ.ทร.ตามที่กฎหมายกำหนดต่อไปรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง จึงกำหนดข้อปฏิบัติการใช้งานระบบเทคโนโลยีสารสนเทศ ดังนี้

๑. คำนิยาม

๑.๑ “หน่วย”หมายความว่า

๑.๒ “หน่วยงานในสังกัด” หมายความว่า ส่วนราชการและหน่วยงานในสังกัดกบ.ทร. ระดับกองและแผนก

๑.๓ “ระบบเทคโนโลยีสารสนเทศ”หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบสารสนเทศ ชุดคำสั่งงานคอมพิวเตอร์สำหรับการบันทึกประมวลผล เรียกดู พิมพ์ออกรายงานในระบบของหน่วย และโปรแกรมการใช้งานที่เจ้าหน้าที่ทำการติดตั้งประจำเครื่องคอมพิวเตอร์

๑.๔ “ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใดๆ ไม่ว่า การสื่อสารความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยการผ่านวิธีการใด ๆ และได้จัดทำไว้ในรูปแบบเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม ภาพเคลื่อนไหว เสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่ทำการบันทึกไว้ปรากฏได้

๑.๕ “เครื่องคอมพิวเตอร์” หมายความว่า เครื่องคอมพิวเตอร์แม่ข่าย (Server) และรวมถึง เครื่องคอมพิวเตอร์ลูกข่าย (Client) ชนิดตั้งโต๊ะ (Personal Computer) และชนิดพกพา (Notebook, Palm, PDA)

๑.๖ “เครือข่ายคอมพิวเตอร์” หมายความว่า เครือข่ายคอมพิวเตอร์และการสื่อสารของกบ.ทร. รวมทั้งของกองทัพเรือที่อยู่ในพื้นที่ กบ.ทร.

๑.๗ “เจ้าหน้าที่” หมายความว่า ผู้ซึ่งได้รับมอบหมายให้ดูแลการใช้งานระบบเทคโนโลยีสารสนเทศของ กบ.ทร.

๑.๘ “ผู้ใช้งาน” หมายความว่า ข้าราชการ ทหาร ลูกจ้าง และพนักงานราชการของกองทัพเรือ

๒. การใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๑ ผู้ใช้งานมีสิทธิใช้ระบบเทคโนโลยีสารสนเทศของหน่วยได้ภายใต้ข้อปฏิบัติการใช้งานนี้รวมทั้งต้องปฏิบัติตามแนวทางหรือหลักเกณฑ์อื่นใดจะออกต่อไป

๒.๒ การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของหน่วยให้ปฏิบัติดังนี้

๒.๒.๑ ให้ใช้งานเพื่อภารกิจของหน่วยหรือกองทัพเรือ เท่านั้น

๒.๒.๒ หน่วยงานในสังกัดต้องจัดให้มีเจ้าหน้าที่ผู้ดูแลรับผิดชอบเป็นผู้ประสานการปฏิบัติด้านระบบเทคโนโลยีสารสนเทศ การจัดทำระเบียนครุภัณฑ์เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงรวมถึงการติดตามปรับปรุงและแก้ไขทะเบียนครุภัณฑ์อย่างต่อเนื่อง

๒.๒.๓ ห้ามนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงของหน่วยไปใช้งานนอกสถานที่เว้นแต่จะนำไปใช้งานภารกิจของหน่วย โดยจะต้องได้รับอนุญาตเป็นหนังสือจากหัวหน้าหน่วยงานในสังกัดที่ผู้ใช้งานสังกัด

๒.๒.๔ ห้ามผู้ใช้งานและบุคคลภายนอกนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงจากภายนอกหน่วยเข้ามาเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ของหน่วย เว้นแต่จะได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย

๒.๒.๕ ห้ามผู้ใช้งานทำการติดต่อเพิ่ม ลบ แก้ไข หรือเปลี่ยนแปลงโปรแกรมใดๆ บนเครื่องคอมพิวเตอร์ของหน่วยนอกเหนือจากที่เจ้าหน้าที่ได้ทำการติดตั้งและใช้งานไว้แล้ว

๒.๒.๖ ต้องจัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ไว้ในสถานที่ที่ปลอดภัย ห้ามเปิดฝา ถอด เพิ่ม หรือเปลี่ยนชิ้นส่วน เครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วง เว้นแต่เป็นการดำเนินการเพื่อซ่อมแซมบำรุงรักษาโดยเจ้าหน้าที่

๒.๒.๗ ห้ามผู้ใช้งานแก้ไข เปลี่ยนแปลง หรือปรับค่าต่างๆ ที่กำหนดไว้ในเครื่องคอมพิวเตอร์เพื่อให้ทำงานได้ในระบบเครือข่าย (Network Configuration / IP Address) เว้นแต่เป็นการดำเนินการโดยเจ้าหน้าที่

๒.๒.๘ กรณีมีการย้ายจุดติดตั้งเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วง ผู้ใช้งานต้องได้รับความเห็นชอบจากผู้บังคับบัญชาระดับหัวหน้าหน่วยงานในสังกัด และแจ้งให้แผนกกรรมวิธีข้อมูล กองพัฒนากำลังรบทราบเป็นหนังสือ

๒.๒.๙ ห้ามผู้ใช้งานติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อใช้งานในระบบเครือข่ายคอมพิวเตอร์ของหน่วย หรือเปิดการใช้แฟ้มข้อมูลร่วมกัน (Share File / Directory) ให้ผู้อื่นสามารถเข้าถึง (Access) ข้อมูลที่ไม่ใช้เพื่อประโยชน์ หรือภารกิจในการปฏิบัติงาน

๒.๒.๑๐ ให้ปิดเครื่องคอมพิวเตอร์และอุปกรณ์ทุกครั้งที่เลิกใช้งาน หรือเมื่อไม่ได้ใช้งาน เครื่องคอมพิวเตอร์เกินกว่า ๑ ชั่วโมง ๔๐

๒.๓ ผู้ใช้งานพึงใช้ทรัพยากรเครือข่ายคอมพิวเตอร์ให้เกิดประสิทธิภาพและประโยชน์ในการปฏิบัติงานส่วนรวม โดยให้ปฏิบัติ ดังนี้

๒.๓.๑ ไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ต่อไปนี้

๒.๓.๑.๑ กระทำผิดกฎหมายหรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

๒.๓.๑.๒ กระทำขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี

๒.๓.๑.๓ เพื่อการพาณิชย์

๒.๓.๑.๔ เปิดเผยข้อมูลที่เป็นความลับซึ่งได้จากการปฏิบัติงาน

๒.๓.๑.๕ เป็นการละเมิดทรัพย์สินทางปัญญา

๒.๓.๑.๖ รับหรือส่งข้อมูลซึ่งก่อให้เกิดความเสียหายแก่หน่วย เช่น การรับหรือส่งจดหมายที่มีลักษณะเป็นจดหมายลูกโซ่

๒.๓.๑.๗ ขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของผู้ใช้งานอื่น หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของหน่วยไม่สามารถใช้งานได้ตามปกติ

๒.๓.๑.๘ รับรู้ รับทราบข้อมูล ส่งต่อ ประกาศ หรือแสดงความคิดเห็นในเรื่องที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วย ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

๒.๓.๒ ไม่ถ่ายโอนข้อมูลที่มีขนาดใหญ่ที่ไม่เกี่ยวข้องกับการปฏิบัติงานโดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงาน

๒.๓.๓ ไม่นำเครื่องคอมพิวเตอร์ของหน่วย ไปติดตั้งหรือเชื่อมโยงกับเครือข่ายคอมพิวเตอร์ภายนอกโดยผ่านทางช่องทางโทรศัพท์หรือช่องทางอื่นที่หน่วยไม่ได้กำหนดไว้

๒.๓.๔ ไม่ควรติดตั้งและใช้งานโปรแกรมการสนทนาผ่านเครือข่ายคอมพิวเตอร์ เช่น โปรแกรม IRC, ICQ, MSN เป็นต้น

๓. การรักษาความปลอดภัยของข้อมูล เพื่อความปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของหน่วย ให้ผู้ใช้ปฏิบัติงานดังนี้

๓.๑ สำรวจแฟ้มข้อมูลต่างๆ ที่ได้บันทึกไว้ในแผ่นบันทึกข้อมูลเครื่องคอมพิวเตอร์ (Hard Disk) อย่างสม่ำเสมอและลบแฟ้มข้อมูลหรือข้อมูลที่ไม่จำเป็นออกไปเพื่อให้มีเนื้อที่ในการบันทึกข้อมูลอื่น ๆ เพิ่มมากขึ้น และเป็นการเพิ่มสมรรถนะในการประมวลผลข้อมูลของเครื่องคอมพิวเตอร์ให้เร็วยิ่งขึ้นได้

๓.๒ ข้อมูลที่เป็นความลับ หรือข้อมูลที่ไม่พึงเปิดเผย ให้บันทึกข้อมูลลงในแผ่นบันทึกข้อมูลที่สามารถแยกเก็บไว้ต่างหากในที่ปลอดภัย กรณีมีข้อมูลที่มีความสำคัญให้สำรองของมูล (Back Up) และจัดเก็บแยกต่างหากในที่ ที่ปลอดภัย

๓.๓ กรณีมีความจำเป็นต้องนำข้อมูลจากแหล่งจัดเก็บข้อมูลภายนอกมาใช้งานกับเครื่องคอมพิวเตอร์ของหน่วย ให้ตรวจไวรัสคอมพิวเตอร์ก่อนทุกครั้งโดยใช้โปรแกรมตรวจสอบไวรัสคอมพิวเตอร์ที่เจ้าหน้าที่ได้ติดตั้งไว้กับเครื่องคอมพิวเตอร์นั้น และหากตรวจพบไวรัสคอมพิวเตอร์ฝังอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด

๓.๔ ลงทะเบียนการใช้งานระบบงานสารสนเทศของหน่วยโดยหัวหน้าหน่วยงานในสังกัดที่ผู้ใช้งานสังกัดอยู่เป็นผู้พิจารณา

๓.๕ กรณีผู้ใช้งานโอนย้าย เปลี่ยนแปลงหน้าที่ หรือไม่มีความจำเป็นในการใช้งานระบบงานสารสนเทศใด ให้แผนกธุรการ หรือเจ้าหน้าที่กำลังพลของหน่วย แจ้งให้แผนกกรรมวิธีข้อมูล กองพัฒนากำลังรบทราบ เพื่อปรับปรุงเปลี่ยนแปลงสิทธิหรือยกเลิกชื่อหรือรหัสของผู้ใช้งานนั้นต่อไป

๓.๖ ในการใช้งานระบบสารสนเทศของหน่วย ผู้ใช้จะต้องใส่ชื่อผู้ใช้งาน (Log in Name) และกำหนดรหัสผ่าน (Password) เพื่อเชื่อมต่อเข้าสู่ระบบงานสารสนเทศ และเมื่อเสร็จสิ้นการใช้งานให้ปิดระบบ (Exit) ทันที

๓.๗ ดูแล และใช้รหัสผ่านที่ได้รับ ความระมัดระวังและรักษาเป็นความลับ มิให้แจ้งรหัสผ่านของตนเองให้กับบุคคลภายนอกหรือบุคคลอื่นที่ไม่เกี่ยวข้องกับการปฏิบัติงานเพื่อป้องกันมิให้ผู้อื่นนำชื่อรหัสผ่านไปใช้งานในระบบงานสารสนเทศของหน่วย ซึ่งอาจก่อให้เกิดความเสียหายขึ้นได้

๓.๘ ไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลที่สำคัญไว้ในที่ที่สามารถพบเห็นได้ง่าย โดยให้มีการจัดเก็บไว้ในที่ปลอดภัย

๓.๙ ต้องป้องกันข้อมูลและอุปกรณ์ที่อยู่ในเครื่องคอมพิวเตอร์ ชนิดพกพาเมื่อปฏิบัติงานนอกสถานที่ เช่นการใส่รหัสผ่านป้องกันการเข้าถึงหน้าจอ การใช้กุญแจล็อกเครื่องคอมพิวเตอร์ชนิดพกพา หรือการเข้ารหัสแฟ้มข้อมูลที่สำคัญ

๓.๑๐ กรณีที่ตรวจสอบหรือพบเห็นเหตุการณ์หรือการกระทำอื่นใดที่เป็นผลเสียต่อการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยรวมถึงการตรวจพบจุดอ่อนหรือภัยที่พบในระบบงานสารสนเทศที่ใช้งานอยู่ ให้รายงานให้แผนกกรรมวิธีข้อมูล กองพัฒนากำลังรบ ทราบ เพื่อป้องกันแก้ไขต่อไปโดยเร็ว

๓.๑๑ กรณีพบปัญหา หรือข้อบกพร่องของระบบงานสารสนเทศของหน่วย ผู้ใช้งานรายงานปัญหาหรือข้อบกพร่องที่พบให้แผนกกรรมวิธีข้อมูล กองพัฒนากำลังรบ ทราบ เพื่อแก้ปัญหาโดยเร็วที่สุด

๔. การดูแล บำรุงรักษา และการปฏิบัติของเจ้าหน้าที่

เจ้าหน้าที่ต้องดูแล บำรุงรักษา ระบบเทคโนโลยีสารสนเทศ ให้สามารถใช้งานได้ดีอยู่เสมอ และจะต้องตรวจสอบดูแลการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปตามข้อปฏิบัติ ดังนี้

๔.๑ เจ้าหน้าที่ต้องดำเนินการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ตามที่กฎหมายกำหนดไว้

๔.๒ เจ้าหน้าที่ต้องไม่ใช้สิทธิหรืออำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น เว้นแต่กรณีที่ได้รับมอบหมายให้ดำเนินการเพื่อแก้ไขปัญหาที่เกี่ยวข้อง และจะต้องไม่เปิดเผยหรือเผยแพร่ข้อมูลที่ได้รับจากการปฏิบัติหน้าที่

๔.๓ เจ้าหน้าที่ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของผู้ใช้งาน เช่น ข้อมูลในระบบไปรษณีย์อิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานกำลังพล

๔.๔ เจ้าหน้าที่ต้องบันทึกเหตุการณ์ที่มีการละเมิดความมั่นคงปลอดภัย จุดอ่อน ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไขปัญหาที่เกิดขึ้น

๔.๕ เจ้าหน้าที่ต้องติดตั้งซอฟต์แวร์หรืออุปกรณ์ป้องกันไวรัสคอมพิวเตอร์ และตรวจสอบไวรัสคอมพิวเตอร์ที่อาจบุกรุกเข้ามาทางเครือข่ายคอมพิวเตอร์อย่างสม่ำเสมอหากตรวจพบต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์นั้นโดยเร็วที่สุด

๔.๖ เจ้าหน้าที่ต้องสำรองข้อมูลในระบบสารสนเทศ โดยต้องมีข้อมูลการสำรองข้อมูลและจัดทำบันทึกรายละเอียดการสำรองข้อมูล รวมถึงการรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นและวิธีการแก้ไขปัญหาที่เกิดขึ้น

๔.๗ เจ้าหน้าที่ต้องจัดการให้มีระบบการบริหารจัดการเกี่ยวกับการกำหนดสิทธิ์การใช้งานระบบงานสารสนเทศและทำการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบงานสารสนเทศแต่ละระบบ

๔.๘ เจ้าหน้าที่ต้องจัดให้มีการควบคุมการใช้งานของชุดคำสั่งงานคอมพิวเตอร์ (Program source library) ไม่เก็บซอร์สโค้ด (source code) ไว้ในเครื่องที่ใช้ปฏิบัติงานระบบงานสารสนเทศ ไม่เก็บซอร์สโค้ดที่อยู่ระหว่างทำการทดสอบรวมไว้กับไลบรารีที่ใช้งานได้จริงแล้ว และต้องเก็บซอร์สโค้ดไว้ในที่ที่ปลอดภัย

เจ้าหน้าที่หรือผู้ใช้งานฝ่าฝืนหรือไม่ปฏิบัติตามข้อปฏิบัตินี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่หน่วยหรือบุคคลหนึ่งบุคคลใด หน่วยจะพิจารณาระงับสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๓. การประเมินความเสี่ยง

องค์ประกอบการคุกคามหลัก

๑. บุคลากร

๒. เครื่องแม่ข่ายและอุปกรณ์ (Hardware & accessory)

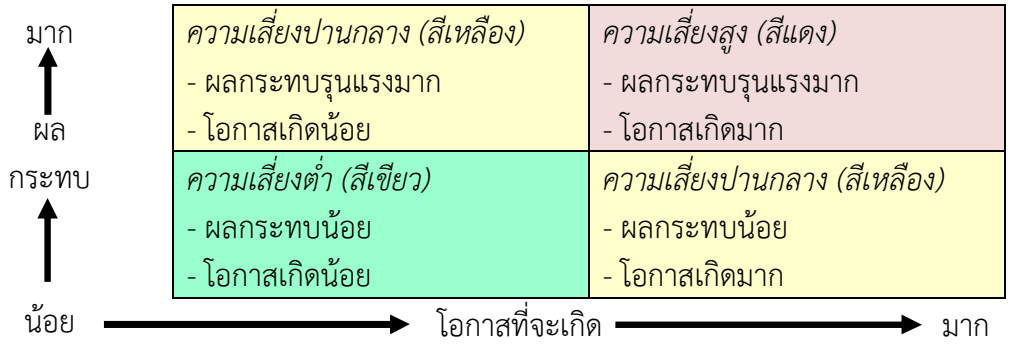
๓. โปรแกรม (Software)

๔. การเชื่อมโยงเครือข่าย (Network & Communicate)

๕. ระบบงานและข้อมูล (System & Information)

๖. องค์ประกอบอื่นๆ (Other Unexpected condition)

โดยพิจารณาองค์ประกอบการคุกคามหลัก จะใช้การวัดระดับความเสี่ยง ตามตารางนี้



โอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง

โอกาสที่จะเกิด	ความถี่ที่เกิดขึ้น (เฉลี่ย)	ระดับคะแนน
สูงมาก	มากกว่า ๑ ครั้งต่อเดือน	๕
สูง	ระหว่าง ๑-๖ เดือนต่อครั้ง	๔
ปานกลาง	ระหว่าง ๖-๑๒ เดือนต่อครั้ง	๓
น้อย	มากกว่า ๑ ปีต่อครั้ง	๒
น้อยมาก	มากกว่า ๕ ปีต่อครั้ง	๑

ผลกระทบต่อองค์กร

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	มากกว่า ๑๐ ล้านบาท	๕
สูง	๕ แสนบาท - ๑๐ ล้านบาท	๔
ปานกลาง	๑ - ๕ แสนบาท	๓
น้อย	๑ หมื่นบาท – ๑ แสนบาท	๒
น้อยมาก	น้อยกว่า ๑ หมื่นบาท	๑

การพิจารณาองค์ประกอบการคุกคามหลัก

๑. องค์ประกอบการคุกคามหลัก : บุคลากร

ความถี่ : ๐ = ไม่เกิด, ๑ = ทุกสิบปี, ๒ = ทุกปี, ๓ = ทุกเดือน, ๔ = ทุกสัปดาห์, ๕ = ทุกวัน

ผลกระทบ : ๐ = ไม่มี, ๑ = น้อยมาก, ๒ = น้อย, ๓ = ปานกลาง, ๔ = มาก, ๕ = มากที่สุด

องค์ประกอบ ความเสี่ยง	สถานการณ์	โอกาส/ ความถี่	ผล กระทบ	Plot Value
บุคลากรภายใน				
ไม่ปฏิบัติหน้าที่ Front	ป่วย/ขาดงานโดยไม่ได้แจ้ง	๒	๒	G
	อุบัติเหตุ	๑	๒	G
	ติดภารกิจด่วนมาก	๔	๒	Y
ไม่ปฏิบัติหน้าที่ Admin	ป่วย/ขาดงานโดยไม่ได้แจ้ง	๐	๓	Y
	อุบัติเหตุ	๑	๓	Y
	ติดภารกิจด่วนมาก	๔	๓	R
ไม่ปฏิบัติหน้าที่ Network	ป่วย/ขาดงานโดยไม่ได้แจ้ง	๓	๓	R
	อุบัติเหตุ	๑	๓	Y
	ติดภารกิจด่วนมาก	๔	๓	R
ทำหน้าที่งาน Front	ทำงานผิดขั้นตอน(ระบบเสียหาย)	๒	๑	G
	ทำงานผิดขั้นตอน (Hardware เสียหาย)	๑	๔	Y
	ย้าย/แก้ไข/เปลี่ยนแปลง/เพิ่มอุปกรณ์ผิดพลาด	๑	๔	Y
	ประมาทเลินเล่อในการรักษาความปลอดภัย	๒	๓	Y
	มอบสิทธิ์ให้ผู้ที่ไม่เกี่ยวข้องโดยพลการ	๑	๔	Y
ทำหน้าที่ Administrator ผิดพลาด	ไม่ตรวจสอบการ Backup	๒	๕	Y
	Start up ระบบผิดพลาด	๓	๔	R
	ประมาทเลินเล่อในการรักษาความปลอดภัย	๑	๕	Y
	มอบสิทธิ์ให้ผู้ที่ไม่เกี่ยวข้องโดยพลการ	๑	๕	Y
	ไม่ตรวจสอบผลหลังการ Backup	๒	๔	Y
	ไม่ดูแลรักษาอุปกรณ์ที่เกี่ยวข้อง	๒	๔	Y
	ไม่ดูแล Server อย่างสม่ำเสมอ	๑	๔	Y
	ไม่ตรวจสอบ Performance ของระบบ	๒	๔	Y
ทำหน้าที่ Input & maintenance ผิดพลาด	นำข้อมูลเข้าผิด	๔	๑	Y
	ไม่นำข้อมูลเข้า	๔	๑	Y
	ไม่ตรวจสอบความถูกต้อง	๔	๒	Y
บุคลากรภายนอก เข้ามาใช้งานระบบ	เข้ามาใช้งานโดยไม่มีสิทธิ์	๓	๑	Y
	เข้ามาโจมตีระบบ (Hacker)	๒	๕	Y
	เข้ามาทำลายข้อมูลใน PC	๓	๔	R
	ทำลายอุปกรณ์ Hardware	๓	๔	R
	ขโมยอุปกรณ์ Hardware	๒	๓	Y
	การแผ่กระจาย Virus	๔	๔	R
	ไม่ตรวจสอบข้อมูลก่อนการบันทึก	๔	๑	Y

๒. องค์ประกอบการคุกคามหลัก : เครื่องแม่ข่ายและอุปกรณ์ (Hardware & Accessory)

ความถี่ : ๐ = ไม่เกิด, ๑ = ทุกสิบปี, ๒ = ทุกปี, ๓ = ทุกเดือน, ๔ = ทุกสัปดาห์, ๕ = ทุกวัน

ผลกระทบ : ๐ = ไม่มี, ๑ = น้อยมาก, ๒ = น้อย, ๓ = ปานกลาง, ๔ = มาก, ๕ = มากที่สุด

องค์ประกอบความเสี่ยง	สถานการณ์	โอกาส/ความถี่	ผลกระทบ	Plot Value
PC	PC ไม่ทำงาน/ Start up	๓	๔	R
	PC หยุดทำงานโดยไม่ทราบสาเหตุ	๒	๔	Y
	ไม่สามารถ Mount External Device	๒	๔	Y
	ไม่สามารถติดต่อ PABX/ATM	๒	๔	Y
	Server ตั้งอยู่ในที่ที่สะเทือน	๑	๔	Y
	PC ตั้งอยู่ในที่ที่อุณหภูมิสูง	๑	๔	Y
	อุบัติเหตุที่เกิดจากภัยธรรมชาติ/ภัยพิบัติ	๑	๔	Y
	PC ตั้งอยู่ในที่ที่ มีฝุ่นเยอะ	๑	๔	Y
External Hard Disk	Hard Disk ตั้งอยู่ในที่ที่สะเทือน	๑	๔	Y
	Hard Disk ตั้งอยู่ในที่ที่อุณหภูมิสูง	๑	๔	Y
	Disk เกิด Bad (Physical Failure)	๑	๕	Y
	Connect กลับไปยัง PC ไม่ได้	๑	๔	Y
	อุปกรณ์ต่อพ่วง/เชื่อมใช้งานไม่ได้	๑	๔	Y
ATM/PABX	จุดต่อหลุดโดยอุบัติเหตุ	๑	๓	Y
	Switch เสีย	๑	๓	Y
	ช่อง Port เสีย	๑	๓	Y
Power Supply/UPS	Power Supply เกิดข้อผิดพลาดในการจ่ายไฟ	๑	๔	Y
	ไม่มีการสำรองไฟเมื่อเกิดเหตุฉุกเฉิน	๑	๔	Y
	Power Supply ไม่สามารถจ่ายไฟได้สม่ำเสมอ	๑	๔	Y
	Power Supply อยู่ในที่อุณหภูมิสูง	๑	๔	Y
	Power Supply ระเบิด	๑	๔	Y
Network Printer	Printer ไม่ทำงาน	๑	๓	Y
	Printer ไม่สามารถ Connect ได้	๑	๓	Y
	Printer Feed กระดาษไม่ได้	๑	๓	Y
	ผลลัพธ์ผิดพลาด	๑	๓	Y
Monitor Keyboard	Monitor ไม่แสดงผล	๑	๒	G
	Monitor แสดงผลไม่ถูกต้อง (Sync เสีย)	๑	๒	G
	Keyboard ไม่ตอบสนอง	๑	๒	G

๓. องค์ประกอบการคุกคามหลัก : โปรแกรม (Software)

ความถี่ : ๐ = ไม่เกิด, ๑ = ทุกสิบปี, ๒ = ทุกปี, ๓ = ทุกเดือน, ๔ = ทุกสัปดาห์, ๕ = ทุกวัน

ผลกระทบ : ๐ = ไม่มี, ๑ = น้อยมาก, ๒ = น้อย, ๓ = ปานกลาง, ๔ = มาก, ๕ = มากที่สุด

องค์ประกอบความเสี่ยง	สถานการณ์	โอกาส/ความถี่	ผลกระทบ	Plot Value
Software ทำงานไม่ได้	Software เสีย/อ่านไม่ได้	๑	๒	G
	Software License Expire	๒	๓	Y
	Software โดนความร้อน	๑	๒	G
	Software โดนความชื้น	๑	๒	G
	Software หัก/งอ/แตก	๑	๒	G
Software หาย	Software โดนขโมย	๑	๒	G
	นำ Software ไปใช้งานแล้วไม่นำมาเก็บเข้าที่	๒	๓	Y

๔. องค์ประกอบการคุกคามหลัก : การเชื่อมโยงเครือข่าย (Network & Communicate)

ความถี่ : ๐ = ไม่เกิด, ๑ = ทุกสิบปี, ๒ = ทุกปี, ๓ = ทุกเดือน, ๔ = ทุกสัปดาห์, ๕ = ทุกวัน

ผลกระทบ : ๐ = ไม่มี, ๑ = น้อยมาก, ๒ = น้อย, ๓ = ปานกลาง, ๔ = มาก, ๕ = มากที่สุด

องค์ประกอบความเสี่ยง	สถานการณ์	โอกาส/ความถี่	ผลกระทบ	Plot Value
อุปกรณ์ต่อเชื่อม				
- สาย NetWork/หัว Jumb	สายLANโดนความร้อน/ไฟ	๐	๒	G
	สาย LAN ขาดใน	๓	๒	Y
	สาย LAN ถูกแมลงกัดกิน	๑	๒	G
	หัว Jump ไม่สามารถใช้งานได้	๑	๒	G
	Hub ไม่สามารถใช้งานได้	๑	๒	G
- Wireless	Wireless ตัวส่งสัญญาณไม่สามารถส่งสัญญาณได้	๐	๐	G
	Wireless ตัวรับสัญญาณไม่สามารถรับสัญญาณได้	๐	๐	G
	USB เสีย	๐	๐	G
	Network	๐	๐	G

๕. องค์ประกอบการคุกคามหลัก : ระบบงานและข้อมูล (System &Information)

ความถี่ : ๐ = ไม่เกิด, ๑ = ทุกสิบปี, ๒ = ทุกปี, ๓ = ทุกเดือน, ๔ = ทุกสัปดาห์, ๕ = ทุกวัน

ผลกระทบ : ๐ = ไม่มี, ๑ = น้อยมาก, ๒ = น้อย, ๓ = ปานกลาง, ๔ = มาก, ๕ = มากที่สุด

องค์ประกอบความเสี่ยง	สถานการณ์	โอกาส/ความถี่	ผลกระทบ	Plot Value
OS Client	มี File โดนลบ/ทำลาย	๐	๓	Y
	โดน Virus โจมตี	๐	๒	G
	OS ไม่ทำงาน	๐	๒	G
	Client หยุดทำงานโดยไม่ทราบสาเหตุ	๐	๒	G
	Performance ตก	๐	๒	G
	Physical Disk Space ไม่ทำงาน	๐	๒	G
PC Application Software	PC Application ไม่ทำงานโดยไม่ทราบสาเหตุ	๑	๓	Y
	Performance ตกไม่ทำงานเพราะ ไม่ได้ Manipulate/tuning	๐	๒	G
Client Application	Performance ตกไม่ทำงานเพราะ ไม่ได้ Manipulate/tuning	๐	๒	G
System Data/ Information (Server Information)	Performance ตกไม่ทำงานเพราะ ไม่ได้ Manipulate/tuning	๑	๒	G
	ข้อมูลสูญหาย	๑	๔	Y
	ข้อมูลไม่สามารถสำรองได้	๑	๔	Y
	ข้อไม่สามารถกู้คืนได้(Data Recovery)	๑	๔	Y
	ข้อมูลได้สามารถย้อนกระบวนการได้ (Roll Back)	๑	๔	Y
	ข้อมูลไม่สามารถบันทึกเพิ่มได้(Quota Maximum)	๑	๔	Y
System Data/ Information (Client Information)	Performance ตกไม่ทำงานเพราะ ไม่ได้ Manipulate/tuning	๑	๒	G
	ข้อมูลสูญหาย	๑	๒	G
	ข้อมูลโดน Virus	๑	๒	G
	ข้อมูลสูญหายเนื่องจาก window ต่าง Version	๐	๑	G
	ข้อผิดพลาดของ Application Software (Software ไม่เสถียร)	๐	๑	G

๖.องค์ประกอบการคุกคามหลัก : องค์ประกอบอื่นๆ(Other Unexpected condition)

ความถี่ : ๐ = ไม่เกิด, ๑ = ทุกสิบปี, ๒ = ทุกปี, ๓ = ทุกเดือน, ๔ = ทุกสัปดาห์, ๕ = ทุกวัน

ผลกระทบ : ๐ = ไม่มี, ๑ = น้อยมาก, ๒ = น้อย, ๓ = ปานกลาง, ๔ = มาก, ๕ = มากที่สุด

องค์ประกอบความเสี่ยง	สถานการณ์	โอกาส/ความถี่	ผลกระทบ	Plot Value
ไฟฟ้า	ไฟดับ จาก Mea	๓	๓	R
	ไฟกระตุก	๓	๓	R
	ตัดไฟเอง	๓	๓	R
	ฟ้าผ่า	๐	๓	Y
เครื่องสำรองไฟ	เครื่องสำรองไฟไม่ทำงาน	๐	๓	Y
	เครื่องสำรองไฟเสีย	๑	๓	Y
	เครื่องสำรองไฟไม่สามารถควบคุมไฟได้	๒	๓	Y
ระบบปรับอากาศ	ระบบปรับอากาศไม่ทำงาน	๓	๔	R
	เกิดไฟฟ้าลัดวงจร	๑	๓	Y
	เกิดการเสียหายหรือชำรุด	๑	๔	Y
	เครื่องไม่ทำความเย็น	๓	๔	R
ภัยธรรมชาติ	น้ำท่วม	๐	๔	Y
	ไฟไหม้	๐	๕	Y
	พายุ	๐	๕	Y
	แผ่นดินไหว	๐	๕	Y
การก่อสร้างหรือต่อเติม	ทำให้เกิดฝุ่น	๑	๔	Y
	การสะเทือน	๑	๔	Y
	อุปกรณ์เสียหาย	๑	๔	Y
ภัยสงคราม	เกิดวินาศกรรม	๐	๔	Y
	เกิดการจลาจล	๐	๔	Y

๔. แผนจัดการความเสี่ยง (Risk management action plan)

หัวข้อ (Process Title) : การรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ PC

วัตถุประสงค์ : จัดการความเสี่ยงกรณีเครื่องคอมพิวเตอร์ PC ไม่สามารถให้บริการได้

วิธีกำหนดแนวทางจัดการความเสี่ยง ประกอบด้วย ๔ รูปแบบ

๑. Risk Acceptance การยอมรับความเสี่ยง เหตุผล คือ ค่าใช้จ่าย จะสูงกว่า ผลที่ได้รับ แต่จะมีมาตรการ หรือแผน ในการกำกับดูแล

๒. Risk Reduction / Control การลด/ควบคุม ความเสี่ยง ด้วยมาตรการต่างๆ

๓. Risk Avoidance การหลีกเลี่ยง ความเสี่ยง โดยการ ปรับ/เปลี่ยนแปลง รูปแบบการทำงาน

๔. Risk Sharing การกระจายความเสี่ยง ด้วยการโอนความเสี่ยงไปให้หน่วยงานอื่นรับผิดชอบ เช่น จ้างผู้อื่นมาดูแล

ลำดับความเร่งด่วนในการจัดการความเสี่ยง(กลั่นกรอง) โดยให้ความสำคัญและจัดการโดยเร่งด่วน กับ กลุ่มความเสี่ยง มาก (สีแดง,R) ส่วนกลุ่มความเสี่ยงต่ำ จะใช้วิธี ออกมาตรการ กำกับ ดูแล ให้อยู่ในระดับที่ยอมรับได้ผลกระทบต่อวัตถุประสงค์ของการควบคุม มี ๓ ด้าน คือ

ด้านการดำเนินงาน (O)

ด้านการเงิน (F)

ด้านการปฏิบัติ ด้านกฎหมาย กฎ ระเบียบ (C)

ความเสี่ยง	เหตุการณ์	กระทบ วัตถุประสงค์ของการควบคุมด้าน	ระดับ	วิธี	มาตรการ	ระดับการยอมรับได้	สถานะ	ติดตาม ปรับปรุง
ไฟฟ้า,เครื่องสำรองไฟ	ไฟดับ สาเหตุจากการไฟฟ้านครหลวงไฟกระตุก ตัดไฟเอง	O,C	R	๒,๔	๑.ติดตั้งเครื่องสำรองไฟฟ้า (UPS) ให้กับเครื่อง PC เพื่อป้องกันไฟกระชาก และ สำรองไฟกรณีไฟฟ้าดับ ๒. มีการกระตุ้น/ทบสอบการทำงานของเครื่องกำเนิดไฟฟ้า (DC Generator) ทุกสัปดาห์ สัปดาห์ละ ๑ ครั้งในทุกวันพฤหัสบดีเวลา ๑๕.๔๕ น.-๑๖.๐๐ น. ๓. มีการตรวจเช็คประสิทธิภาพของเครื่องสำรองไฟฟ้า (UPS) ทุก ๓ เดือน โดยจนท.บริษัท ๔. กำหนด จนท. ที่ดูแลรับผิดชอบ	ต้องสำรองไฟได้ ๑๕ นาที เป็นอย่างน้อย	ดำเนินการแล้ว	กำลังดำเนินการจัดหาเครื่องสำรองไฟฟ้า (UPS) ใหม่ มีความสามารถในการสำรองไฟได้ ๓๐ นาที
	เครื่องสำรองไฟไม่ทำงาน เครื่องสำรองไฟเสีย เครื่องสำรองไฟไม่สามารถควบคุมไฟได้	O,C	Y	๒,๔				
เหตุไม่คาดหมาย	ไฟไหม้	O,C,F	Y	๒,๔	๑. ติดตั้งอุปกรณ์จับควัน ซึ่งจะส่งสัญญาณเตือน เมื่อเกิดควันขึ้นภายในห้อง ๒ ตรวจสอบการทำงานโดยบริษัทขายเครื่องอย่างสม่ำเสมอ ๓. ติดตั้งระบบตัดวงจรไฟฟ้ากรณีไฟฟ้าลัดวงจร (Circuit Breaker) ๔. มีการติดตั้งอุปกรณ์ดับเพลิง ชนิดไพโรเจน (Pyrogen) ในห้องเครื่อง PC และห้องเครือข่าย	ต้องตรวจจับได้	ดำเนินการแล้ว	ต้องจัดหาอุปกรณ์ดับไฟที่สามารถใช้กับเครื่องคอมพิวเตอร์ได้

ความเสี่ยง	เหตุการณ์	กระทบวัตถุประสงค์ของการควบคุมด้าน	ระดับ	วิธี	มาตรการ	ระดับการยอมรับได้	สถานะ	ติดตามปรับปรุง
ระบบปรับอากาศ	ระบบปรับอากาศไม่ทำงาน/ ระดับความเย็นของห้องคอมพิวเตอร์สูง ทำให้การทำงานของเครื่องผิดปกติ	O,C	R	๓,๔	๑. กำหนดแผนการทำงานโดยให้เครื่องปรับอากาศภายในห้องคอมพิวเตอร์ ๕ ตัว ทำงานสลับกัน เวลา ๘.๓๐ – ๑๗.๓๐ น. เครื่อง ๑,๒,๓ จะทำงานเวลา ๑๗.๓๐ – ๐๘.๓๐ น. เครื่อง ๔,๕ จะทำงานติดตั้งไว้แบบอัตโนมัติ ๒. จัดเจ้าหน้าที่คอยดูแล ๓. มีจนท.บริษัทคอยดูแลบำรุงรักษาเครื่องปรับอากาศ ทุกเดือน ๆ ละ ๑ ครั้ง	อุณหภูมิภายในห้องเครื่อง PC จะต้องไม่สูงกว่า ๒๕ องศาเซนติเกรด	ดำเนินการแล้ว	
บุคลากร	จนท. ไม่ปฏิบัติหน้าที่	C	R	๒	มีมาตรการการมอบหมายผู้รับผิดชอบอย่างชัดเจน		ดำเนินการแล้ว	
	บุคคลภายนอกเข้าห้องเครื่อง PC โดยไม่ได้รับอนุญาต	O,C	Y	๒	มีการมอบหมายผู้รับผิดชอบ กุญแจเข้าห้องเครื่อง PC มีการลงชื่อเข้าใช้ห้อง		ดำเนินการแล้ว	
	บุคคลภายนอกมาใช้เครื่อง PC โดยไม่ได้รับอนุญาต	O,C	Y	๒	มีการกำหนดสิทธิในการเข้าใช้ระบบโดยมีการใช้ User/password ซึ่งมอบหมายให้เจ้าหน้าที่บางคนเท่านั้นที่ จะ Login เข้าเครื่องได้ และ มีการเปลี่ยนรหัสผ่านเป็น ระบบ ๆ และไม่อนุญาตให้มีการใช้ Remote Login เข้าเครื่อง PC มี Firewall ภายในเครือข่ายกั้น (มีผังเครือข่ายประกอบ)		ดำเนินการแล้ว	

ความเสี่ยง	เหตุการณ์	กระทบวัตถุประสงค์ของการควบคุมด้าน	ระดับ	วิธี	มาตรการ	ระดับการยอมรับได้	สถานะ	ติดตามปรับปรุง
	บุคคลภายนอกมาใช้เครื่อง PC โดยไม่ได้รับอนุญาต		Y	๒	๑. กำหนดมาตรการให้พัฒนาโปรแกรมบนเครื่องลูกข่ายเมื่อทดสอบว่าทำงานถูกต้องแล้วจึงนำไปติดตั้งบนเครื่อง PC ๒. มีการทำการสำรอง (backup) กรณีลบโปรแกรมผิด สามารถนำโปรแกรมที่ทำสำเนาไว้มาติดตั้งใหม่ได้		ดำเนินการแล้ว	จัดทำโครงการจัดหา เครื่อง PC ที่สามารถทำงานแบบ Mirror เมื่อเครื่อง PC down อีกเครื่องหนึ่งจะทำงานแทนได้ทันทีโดยอัตโนมัติ (ยังไม่ได้ดำเนินการ เพราะใช้งบประมาณในการดำเนินการมาก)
	บุคคลภายนอกมาใช้ระบบ เช่น ติดตั้งโปรแกรมอื่นบนเครื่อง PC โดยไม่ได้รับอนุญาต	O,C	Y	๒,๔	๑. มีการป้องกันการเข้ามาแก้ไขตัวระบบจากภายนอก ๒. มีระบบกำหนดสิทธิในการเข้าใช้เครื่อง PC ไว้แล้ว ๓. มีมาตรการกำชับผู้ดูแลเครื่อง PC ในการติดตั้งโปรแกรมบนเครื่องจะต้องแจ้งให้หัวหน้าผู้ควบคุมดูแลทราบก่อนการติดตั้ง			

ความเสี่ยง	เหตุการณ์	กระทบวัตถุประสงค์ของการควบคุมด้าน	ระดับ	วิธี	มาตรการ	ระดับการยอมรับได้	สถานะ	ติดตามปรับปรุง
ระบบ และ ข้อมูล System & Information	โดน Virus โจมตี	O,C	Y	๒,๔	๑. มีการติดตั้งโปรแกรมป้องกันไวรัสและมีการทำสำรองโปรแกรมเป็นประจำ เมื่อโปรแกรมมีปัญหาสามารถนำโปรแกรมที่สำเนาไว้มาติดตั้งใหม่ ๒. มีการ Update ตลอดเวลา ๓. มีการติดตั้งระบบป้องกันไวรัสแบบองค์กร มีเครื่อง PC ให้บริการ update ข้อมูล โดยเครื่องลูกข่ายในสำนักงานมีการ กำหนดให้ทุกเครื่องทำการ ตรวจสอบไวรัสแบบอัตโนมัติทุกวันเวลา ๑๒.๐๐ น. และเวลา ๑๗.๐๐ น.โปรแกรมป้องกันไวรัสที่เครื่องลูกข่ายจะตรวจสอบการ update ข้อมูลกับเครื่อง PC ให้ข้อมูลที่ทันสมัย โดยผู้ใช้เครื่องลูกข่ายไม่ต้องใช้คำสั่งให้เครื่องทำงาน	ยอมรับได้	ดำเนินการแล้ว	
	การอัพเกรดซอฟต์แวร์ทำให้ระบบไม่สามารถให้บริการได้	O	Y	๒	กำหนดแผนการทำงานโดยต้องมีการทดลองติดตั้งกับเครื่องสำรอง เพื่อทดสอบว่าระบบจะสามารถทำงานได้ก่อนใช้กับเครื่องจริง		ดำเนินการแล้ว	

ความเสี่ยง	เหตุการณ์	กระทบวัตถุประสงค์ของการควบคุมด้าน	ระดับ	วิธี	มาตรการ	ระดับการยอมรับได้	สถานะ	ติดตามปรับปรุง
	โปรแกรมเพื่อการบริหารจัดการ (Operating System) ไม่ทำงาน , เครื่อง PC หยุด/ไม่ทำงานโดยไม่ทราบสาเหตุ , โปรแกรมเพื่อการบริหารจัดการ (Operating System) เสียหาย	O,C	Y	๒	มีเครื่อง PC สำรองไว้ใช้บริการแทนขณะซ่อม		ดำเนินการแล้ว	
	การกู้คืนระบบเมื่อเครื่อง PC ชำรุดต้องติดตั้งระบบใหม่ทั้งหมด	O,C			๑. จัดทำคู่มือการติดตั้งระบบตั้งแต่การติดตั้งโปรแกรมเพื่อการบริหารจัดการ (Operating System) ซึ่งใช้ Windows ๒๐๐๓ การติดตั้ง Web Portal การติดตั้งฐานข้อมูล Oracle ๒. มีข้อมูลที่มีการทำสำรอง ไว้ใช้งาน ๓. มีการทำสำเนาข้อมูล (Backup) อย่างสม่ำเสมอ ๔. มี จนท. ที่ดูแลรับผิดชอบโดยตรง			

๕. แผนเผชิญเหตุภัยพิบัติต่าง ๆ

กรณีเครื่อง PC ไม่สามารถให้บริการได้เนื่องจากเกิดภัยพิบัติจากสาเหตุต่อไปนี้

๑. เครื่อง PC โดนไวรัสคอมพิวเตอร์โจมตี

๒. ตัวเครื่อง PC เกิดปัญหาไม่สามารถให้บริการได้ สาเหตุอาจมาจากจานบันทึกข้อมูล (Hard Disk) เสียหาย, อุปกรณ์จ่ายไฟเสีย ฯลฯ

๓. เกิดไฟไหม้ตัวเครื่อง PC หรือภายในห้องเครื่อง PC

๔. เครื่อง PC ถูกโจรกรรม

๕. ข้อมูลสูญหาย

๖. การเชื่อมโยงเครือข่ายล้มเหลว

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน ปี ๒๕๕๘	ผู้รับผิดชอบ	แผน/การแก้ไข	ผลการดำเนินงานปี ๒๕๕๘	ผู้รับผิดชอบ
๑. เครื่อง PC โดนไวรัสคอมพิวเตอร์โจมตี	ป้องกันไม่ให้ไวรัสคอมพิวเตอร์โจมตีเครื่อง PC ได้	๑. มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ชื่อ NOD 32 มีการตั้งเวลาให้เครื่อง PC ทำการ update โปรแกรมป้องกันไวรัสและตรวจสอบไวรัสภายในเครื่องโดยอัตโนมัติ	กวป.ฯ	๑. กำจัดไวรัสคอมพิวเตอร์ โดยค้นหาโปรแกรมกำจัดไวรัสจากอินเทอร์เน็ต	-	กวป.ฯ
		๒. มีการกำหนด กฎ (Rule) ของ Firewall ให้เครื่องลูกข่ายที่เข้ามาใช้บริการมีสิทธิใช้ได้เฉพาะ เว็บเพจ เท่านั้น	กวป.ฯ	๒. กรณีที่ไวรัสคอมพิวเตอร์ทำลายระบบจนไม่สามารถให้บริการต่อไปได้ จะทำการ format เครื่อง PC แล้วติดตั้งระบบใหม่จากคู่มือการติดตั้งระบบและนำข้อมูลที่สำเนาไว้มาติดตั้ง	- ได้ทำสำเนาข้อมูลทั้งหมดของระบบไว้ที่ กวป.ฯ - จัดทำคู่มือการติดตั้งระบบใหม่ และวิธีการนำเข้าข้อมูล	กวป.ฯ
		๓. มีการตรวจสอบการเข้าโจมตีเครื่อง PC	กวป.ฯ			

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน ปี ๒๕๕๘	ผู้รับผิดชอบ	แผน/การแก้ไข	ผลการดำเนินงานปี ๒๕๕๘	ผู้รับผิดชอบ
๒. ตัวเครื่อง PC เกิดปัญหาไม่สามารถให้บริการได้ สาเหตุอาจมาจากจานบันทึกข้อมูล (Hard Disk) เสียหาย, อุปกรณ์จ่ายไฟเสีย ฯลฯ	ติดตั้งเครื่อง PC ภายในห้องที่มีความเหมาะสม	๑. ติดตั้งเครื่อง PC ภายในห้องที่มีอุณหภูมิพอเหมาะ ควบคุมไม่ให้อุณหภูมิสูงเกินไป	กวป.ฯ	มีระบบเครื่อง PC สำรองเพื่อให้บริการแทน	มีการติดตั้งเครื่อง PC สำรองไว้แล้ว เมื่อเครื่อง PC หลักไม่สามารถให้บริการได้ สามารถนำข้อมูลที่ได้ทำสำเนาไว้มานำเข้าระบบก็จะสามารถให้บริการทดแทนได้ภายในเวลาไม่เกิน ๒๔ ชั่วโมง	สสท.ทร. / บริษัทผู้แทนจำหน่าย
		๒. ไม่มีฝุ่นละอองมากเกินไปจนทำให้เครื่องเสีย	กวป.ฯ			
		๓. ติดตั้งอุปกรณ์สำรองไฟฟ้า กันไฟฟ้ากระชากไฟฟ้าดับ	กวป.ฯ			
๓. เกิดไฟไหม้ตัวเครื่อง PC หรือภายในห้องเครื่อง PC	ป้องกันไม่ให้เกิดเพลิงไม้	๑. มีการติดตั้งแผงวงจรตัดไฟฟ้า กรณีไฟฟ้าลัดวงจร	กวป.ฯ	จัดหาเครื่อง PC สำรองมาทดแทน	-	สสท.ทร. / บริษัทผู้แทนจำหน่าย
		๒. ติดตั้งอุปกรณ์ตรวจจับควันทั้งอาคาร ส่งสัญญาณแจ้งเตือน, ติดตั้งอุปกรณ์ดับเพลิง	กวป.ฯ			
		๓. ป้องกันไม่ให้มีผู้ที่ไม่เกี่ยวข้องเข้าไปในห้องเครื่อง PC	กวป.ฯ			
		๔. มีการติดตั้งอุปกรณ์ดับเพลิง ชนิด CO๒ ในห้องเครื่อง PC และห้องเครือข่าย	กวป.ฯ			
๔. เครื่อง PC ถูกโจรกรรม	มีระบบการเข้าใช้ห้องเครื่อง PC	๑. ป้องกันไม่ให้มีผู้ที่ไม่เกี่ยวข้องเข้าไปในห้องเครื่อง PC	กวป.ฯ			
		๒. จัดทำทะเบียนผู้เข้าใช้ห้องเครื่อง PC	กวป.ฯ			
		๓. ให้เจ้าหน้าที่เข้าไปสังเกตการณ์การทำงานของ ผู้ที่ไม่ใช่เจ้าหน้าที่ของ กวป.ฯ	กวป.ฯ			

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน ปี ๒๕๕๘	ผู้รับผิดชอบ	แผน/การแก้ไข	ผลการดำเนินงานปี ๒๕๕๘	ผู้รับผิดชอบ
๕. ข้อมูลสูญหาย	ทำการสำเนาข้อมูล	- ได้ทำสำเนาข้อมูลทั้งหมดของระบบไว้ ๒ ชุด แยกเก็บต่างที่ (กวป.ฯ (ถ.อัษฎางค์) ๑ ชุด, ศสส. ถ.วิสุทธิกษัตริย์ ๑ ชุด) - จัดทำคู่มือการติดตั้งระบบใหม่ และวิธีการนำเข้าข้อมูล	กวป.ฯ	ทำการกู้คืนข้อมูล	๑. ได้ถ่ายข้อมูลออกจากฐานข้อมูล (SQL SERVER) มาไว้ภายในเครื่อง PC โดยตั้งเวลาในการถ่ายไว้ทุกวันโดยอัตโนมัติ หมุนเวียน ทุก ๗ วัน สามารถนำเข้าฐานข้อมูลได้ทันที	กวป.ฯ
					๒. ข้อมูลที่สำเนาไว้ในอุปกรณ์อื่น (เทป, แผ่นซีดี)	กวป.ฯ
๖. การเชื่อมโยงเครือข่ายล้มเหลว	ตรวจสอบ การเชื่อมโยงเครือข่ายเป็นประจำทุกวัน	มอบหมายเจ้าหน้าที่ผู้ดูแลเครื่อง PC ให้ตรวจสอบการเรียกใช้ระบบทุกวัน	กวป.ฯ	แผนตรวจสอบการเชื่อมโยงเครือข่าย	จัดทำคู่มือการตรวจสอบการเชื่อมโยงเครือข่าย	กวป.ฯ

มาตรการรักษาความปลอดภัยในบริเวณสถานที่รับผิดชอบ

๑. เจ้าหน้าที่ควบคุมเครื่องคอมพิวเตอร์ และเจ้าหน้าที่ซ่อมแซมและบำรุงรักษาอุปกรณ์

- ดูแลประตูเข้า – ออกให้อยู่ในสภาพที่ Lock ตลอดเวลา (แม้ว่าจะมีการติดตั้งอุปกรณ์ควบคุมการปิด – เปิดประตูอัตโนมัติแล้วก็ตาม)
- ห้ามนำบุคคลภายนอกเข้าไปในบริเวณห้องเครื่อง PC
- ห้ามนำอาหารเข้าไปรับประทานในบริเวณห้องเครื่อง PC
- เข้มงวดให้บุคคลภายนอกที่จำเป็นต้องเข้าไปปฏิบัติงานในบริเวณห้องเครื่อง PC ลงบันทึกในสมุด

๒. สำหรับบุคคลภายนอกที่จำเป็นต้องเข้าไปปฏิบัติงานในบริเวณห้องเครื่อง PC

- ติดต่อเจ้าหน้าที่ที่รับผิดชอบเพื่อแจ้งความจำนงเข้าปฏิบัติงาน
- ลงบันทึกเวลาเข้า และงานที่จะปฏิบัติ
- ลงบันทึกเวลาออก และแจ้งให้เจ้าหน้าที่ทราบ

๖. การสำรอง (Backup) ระบบสารสนเทศและฐานข้อมูล

มาตรการปฏิบัติในการสำรองระบบงาน (Backup) และการนำข้อมูลกลับมาใช้ (Recovery)

๖.๑ ขั้นตอนในการสำรองระบบงาน (Backup)

ระบบงาน Office

การ Backup Operating System ทั้งระบบ และการเก็บ File Backup

การ Backup ข้อมูล จะทำการ Backup ใน External HD ขนาด ๑ TB และบันทึกลงในแผ่น DVD Rom

ระบบงาน Document

การ Backup Operating System ทั้งระบบ และการเก็บ File Backup

การ Backup ข้อมูล จะทำการ Backup ใน External HD ขนาด ๑ TB และบันทึกลงในแผ่น DVD Rom

Database Server

การ Backup Operating System โดย สสท.ทร.

การ Backup ข้อมูล จะทำการ Backup ใน External HD ขนาด ๑ TB และบันทึกลงในแผ่น DVD Rom

๖.๒ แผนการสำรองข้อมูล

ระบบงาน Office

จะทำการสำรองข้อมูลไว้ในแผ่น DVD Rom

ระบบงาน Document

จะดำเนินการโดยผู้ใช้

Database Server

จะทำการสำรองข้อมูลไว้ในแผ่น DVD Rom