ผลงานเรื่องที่ ๒

ผลงานฉบับเต็ม

เรื่อง

การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กรมพัฒนาที่ดิน

ของ

นางจันทร์เพ็ญ ลาภจิตร
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ ตำแหน่งเลขที่ ๑๘๒
ศูนย์สารสนเทศ กรมพัฒนาที่ดิน

ขอประเมินเพื่อแต่งตั้งให้ดำรงตำแหน่งนักวิเคราะห์นโยบายและแผนเชี่ยวชาญ
ตำแหน่งเลขที่ ๑๘๒
ผู้เชี่ยวชาญด้านสารสนเทศ
ศูนย์สารสนเทศ กรมพัฒนาที่ดิน
กระทรวงเกษตรและสหกรณ์

สารบัญ

หน้า

สารบัญตาราง

สารบัญภาพ

ภาพที่ **หน้า**

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

ภายใต้สภาวะการดำเนินงานของทุก ๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการบริหารจัดการภาครัฐแนวใหม่ตามพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. ๒๕๔๖ มุ่งเน้นการพัฒนาระบบราชการไทยให้มีขีดสมรรถนะสูง สามารถรองรับการเปลี่ยนแปลงภายใต้สภาพแวดล้อมที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ไม่แน่นอน หน่วยงานภาครัฐต้องมีการบริหารจัดการความเสี่ยง เพื่อให้การบริหารงานและการตัดสินใจด้านเทคโนโลยีสารสนเทศ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงานตลอดจนการใช้ทรัพยากรต่าง ๆ ได้อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร

สำนักงาน ก.พ.ร. ได้ดำเนินการส่งเสริมให้ส่วนราชการยกระดับและการพัฒนาคุณภาพการบริหารจัดการภาครัฐ (Public Sector Management Quality Award: PMQA) ในปี พ.ศ. ๒๕๕๐ ได้กำหนดให้การพัฒนาคุณภาพการบริหารจัดการภาครัฐ เป็นตัวชี้วัดบังคับตามคำรับรองการปฏิบัติราชการของส่วนราชการ จากนั้นในปี พ.ศ. ๒๕๕๒ - ๒๕๕๔ สำนักงาน ก.พ.ร. ได้วางแนวทางให้ส่วนราชการพัฒนาองค์การตามเกณฑ์ PMQA ในแต่ละหมวด ซึ่งศูนย์สารสนเทศ กรมพัฒนาที่ดิน รับผิดชอบ หมวด ๔ การวัด การวิเคราะห์ และการจัดการความรู้ (IT๑-IT๖) ซึ่ง IT๖ คือ ส่วนราชการต้องมีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ เพื่อกำจัด ป้องกันหรือลดความเสียหายในรูปแบบต่างๆ โดยมีแนวทาง/มาตรการที่จะป้องกันความเสียหาย และมีการสำรองข้อมูลสารสนเทศ (Back up) ซึ่งเมื่อเกิดความเสียหายส่วนราชการสามารถฟื้นฟูระบบสารสนเทศและกู้คืนข้อมูลจากความเสียหายได้ (Recovery) เป็นต้น

นอกจากนี้ กรมพัฒนาที่ดิน ต้องดำเนินการตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ศูนย์สารสนเทศ กรมพัฒนาที่ดิน ได้กำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมพัฒนาที่ดิน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่องและป้องกันภัยคุกคามต่าง ๆ โดยดำเนินการจัดทำการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาะสม

๑.๒ วัตถุประสงค์

๑.๒.๑ วิเคราะห์ประเมินความเสี่ยงจากภัยคุกคามที่เกิดจากช่องโหว่ทางด้านเทคโนโลยีสารสนเทศกรมพัฒนาที่ดิน

๑.๒.๒ จัดทำแผนควบคุม และป้องกันหรือลดความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมพัฒนาที่ดิน ให้สามารถทำงานได้อย่างมีประสิทธิภาพ

๑.๒.๓ กำหนดแนวทางกิจกรรมในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และพร้อมสำหรับการใช้งาน

๑.๒.๔ จัดทำระบบบริหารความเสี่ยงที่มีผลกระทบต่อการดำเนินงาน ตามเป้าหมายและแนวทางของนโยบายรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อนำไปใช้ในการพิจารณาแนวทางการวิเคราะห์ประเมินความเสี่ยง และกำหนดแผนการป้องกัน และจัดการกับความเสี่ยง

๑.๒.๕ เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับแผนงานด้านเทคโนโลยีสารสนเทศ ให้ได้รับการยอมรับและมีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและมีความต่อเนื่อง

๑.๓ วิสัยทัศน์ พันธกิจ ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศกรมพัฒนาที่ดิน

๑.๓.๑ วิสัยทัศน์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

เป็นหน่วยงานที่มีการนำเทคโนโลยีสารสนเทศและการสื่อสาร มาใช้สนับสนุนงานพัฒนาที่ดิน เพื่อให้มีฐานข้อมูลและองค์ความรู้ ด้านทรัพยากรดินและด้านอื่น ๆ ที่เกี่ยวข้อง พร้อมให้บริการสารสนเทศ อย่างถูกต้อง สะดวก รวดเร็ว และทันสมัย

๑.๓.๒ พันธกิจด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

๑.๓.๒.๑ พัฒนา ระบบฐานข้อมูล ระบบเครือข่ายการสื่อสาร ระบบคอมพิวเตอร์ ที่เกี่ยวข้องกับการพัฒนาที่ดิน

๑.๓.๒.๒ พัฒนา ส่งเสริม การนำเทคโนโลยีสารสนเทศ มาใช้ในการบริหารจัดการภายในองค์กร

๑.๓.๒.๓ พัฒนาบุคลากรในองค์กรทุกระดับ ให้สามารถใช้เทคโนโลยีสารสนเทศ ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

๑.๓.๒.๔ เผยแพร่และบริการ ความรู้ ข้อมูลข่าวสาร ด้านการพัฒนาที่ดิน โดยใช้เทคโนโลยีสารสนเทศ เพื่อให้สาธารณชนเกิดความรู้ ความเข้าใจ และมีส่วนร่วม

๑.๓.๓ ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

ยุทธศาสตร์ที่ ๑ การพัฒนาศักยภาพบุคลากรด้านเทคโนโลยีสารสนเทศ

ยุทธศาสตร์ที่ ๒ การพัฒนาระบบสารสนเทศและฐานข้อมูล

ยุทธศาสตร์ที่ ๓ การพัฒนาระบบคอมพิวเตอร์

ยุทธศาสตร์ที่ ๔ การพัฒนาระบบเครือข่ายและการสื่อสารข้อมูล

๑.๓.๔ เป้าหมายโดยรวมและยุทธศาสตร์ในการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๓.๔.๑ เป้าหมายโดยรวมของการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมพัฒนาที่ดิน

จากยุทธศาสตร์กรมพัฒนาที่ดิน ในช่วงแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๑ (พ.ศ.๒๕๕๕ - ๒๕๕๙) ได้ให้ความสำคัญในเรื่องของเทคโนโลยี อุปกรณ์ การจัดเก็บข้อมูล การทำงานของผู้ปฏิบัติงาน และพัฒนาระบบงานสนับสนุนของกรมฯ โดยการจัดอบรมเพิ่มพูนความรู้ ความสามารถให้แก่บุคลากรในกรมฯ ให้มีความทันสมัยต่อการเปลี่ยนแปลงเทคโนโลยีและมีการสร้างความพร้อมเพื่อทันต่อโลกาภิวัตน์ แสดงให้เห็นคุณประโยชน์และโทษของเทคโนโลยี ที่มีต่อบุคลากร องค์กร สังคม และสิ่งแวดล้อม รวมทั้งสร้างเครือข่ายงานวิชาการกับหน่วยงานทั้งในและต่างประเทศ เพื่อส่งเสริมให้ทุกหน่วยงานพัฒนาศักยภาพให้ทันต่อการเปลี่ยนแปลง

นอกจากนี้ ได้กำหนดให้มีการปรับระบบงานกรมพัฒนาที่ดิน ให้มีประสิทธิภาพคล่องตัว การปรับกระบวนการทำงานและระบบบริหารงานด้านการเงิน การพัสดุ การคลัง ให้เอื้อต่อการปฏิบัติงาน โดยปรับการทำงานและลดขั้นตอนให้น้อยลง พร้อมทั้งส่งเสริมและพัฒนาบุคลากรโดยยึดหลักสมรรถนะให้มีการเรียนรู้อย่างต่อเนื่อง โดยมีการจัดการความรู้ สร้างคลังข้อมูล และเชื่อมโยงเครือข่ายแห่งการเรียนรู้อย่างเป็นระบบ

ตารางที่ ๑ ยุทธศาสตร์ในการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาที่ดิน

ยุทธศาสตร์แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน พ.ศ. ๒๕๕๒-๒๒๕๖	**ยุทธศาสตร์แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ประเทศไทย พ.ศ. ๒๕๕๒-๒๕๕๖**
ยุทธศาสตร์ที่ ๑ การพัฒนาศักยภาพบุคลากร ด้านเทคโนโลยีสารสนเทศ **แผนงานที่ ๑** การพัฒนาศักยภาพของบุคลากรด้าน ICT	**ยุทธศาสตร์ที่ ๑** การพัฒนากำลังคนด้าน ICT และบุคคลทั่วไปให้มีความสามารถในการสร้างสรรค์ ผลิต และใช้สารสนเทศอย่างมีวิจารณญาณและรู้เท่าทัน **๑. การพัฒนาบุคลากร ICT** ๑.๒ เพิ่มปริมาณและคุณภาพของบุคลากรที่มีทักษะสูง (High skilled professionals) (๒) สนับสนุนและส่งเสริมให้บุคลากรที่จบการศึกษาในสาขาอื่นๆ ที่มีความสนใจได้เข้าศึกษาในมหาวิทยาลัยหรือสถาบันเฉพาะทางด้าน ICT หรือสถาบันการศึกษาระดับ อุดมศึกษาอื่นๆ เพื่อปรับเปลี่ยนสายวิชาชีพเป็นบุคลากรด้าน ICT โดยอาจใช้กลไกสร้างแรงจูงใจแก่ผู้เรียนหรือผู้ว่าจ้างตามความเหมาะสม **๒. การพัฒนาบุคลากรในสาขาวิชาชีพ อื่น ๆ และบุคคลทั่วไป** ๑.๗ พัฒนาความรู้และทักษะด้าน ICT แก่บุคลากรภาครัฐ (๔) พัฒนาความรู้และทักษะที่จำเป็น ทั้งด้าน ICT และด้านการบริหารจัดการให้แก่ CIO ทั้งที่อยู่ในส่วนกลาง ส่วนภูมิภาค และส่วนท้องถิ่น (ที่จะตั้งขึ้นต่อไป) อย่างต่อเนื่อง เพื่อให้สามารถปฏิบัติหน้าที่ในการเป็นผู้นำและรับผิดชอบการบริหารจัดการ ICT ในหน่วยงาน (ระดับกระทรวงและกรม) ได้อย่างมีประสิทธิภาพ

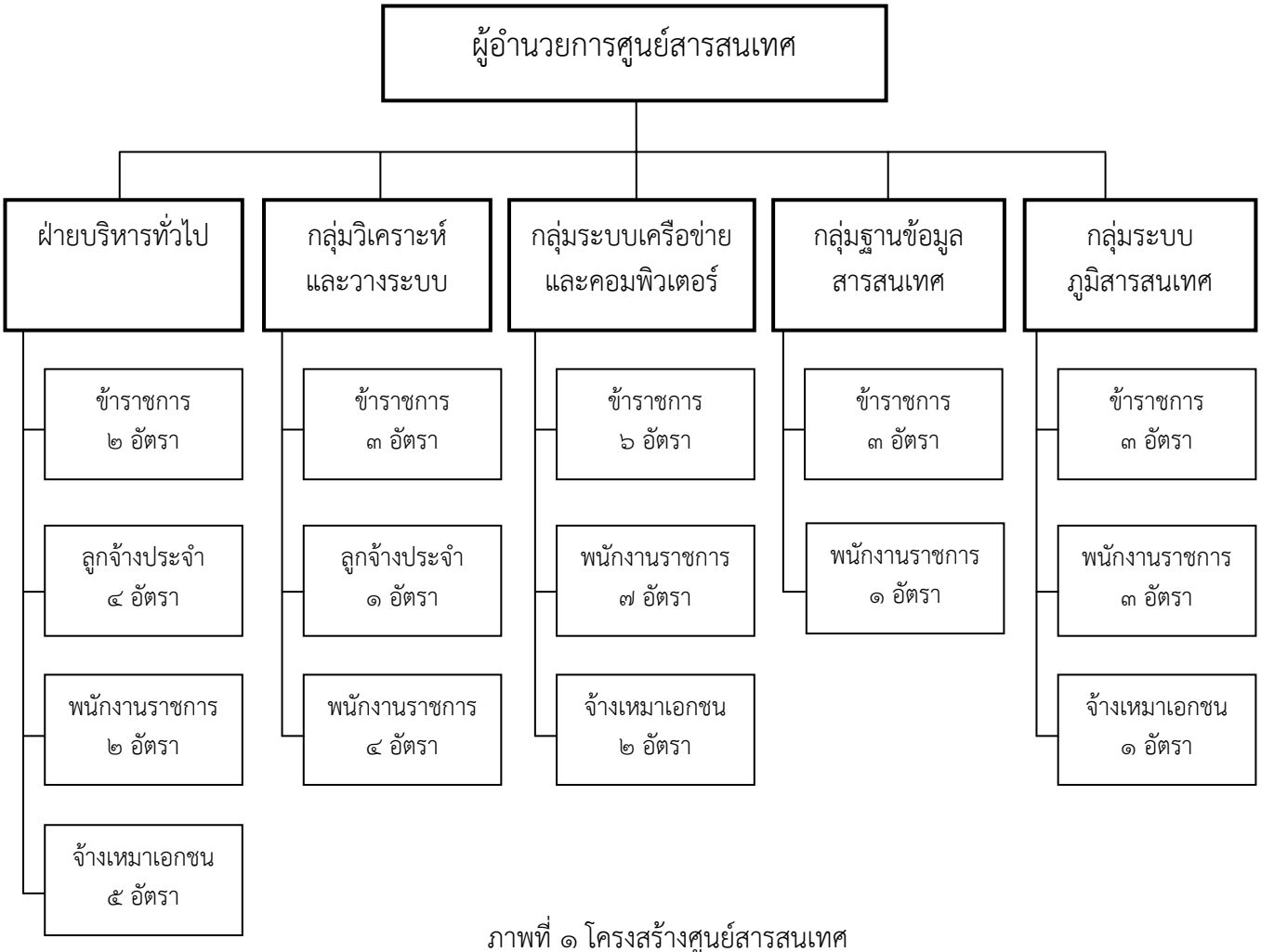
ยุทธศาสตร์แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน พ.ศ. ๒๕๕๒-๒๕๕๖	ยุทธศาสตร์แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ประเทศไทย พ.ศ. ๒๕๕๒-๒๕๕๖
	(๕)พัฒนาความรู้และทักษะเกี่ยวกับซอฟต์แวร์โอเพนซอร์สแก่ข้าราชการและบุคลากรของรัฐเพื่อให้มีการใช้ซอฟต์แวร์โอเพนซอร์สเพิ่มขึ้น **ยุทธศาสตร์ที่ ๔** การใช้เทคโนโลยีสาร สนเทศและการสื่อสารเพื่อสนับสนุนการสร้างธรรมาภิบาลในการบริหารและการบริการของภาครัฐ ๔.๓สร้างความเข้มแข็งด้าน ICT แก่หน่วยงานของรัฐทั้งในส่วนกลางและส่วนภูมิภาค (๑) สร้างความเข้มแข็งให้แก่ CIO ระดับกระทรวง กรม และ CIO ของจังหวัด รวมทั้งบุคลากรที่รับผิดชอบงานด้าน ICT ขององค์กรปกครองส่วนท้องถิ่นในทุกระดับ โดยการอบรมความรู้และทักษะตามความเหมาะสมและสอดคล้องกับภารกิจและหน้าที่ความรับผิดชอบ รวมทั้งส่งเสริมให้มีการฝึกปฏิบัติงานจริง ผ่านการทำโครงการร่วม เพื่อให้การพัฒนางาน ICT ในภาพรวมมีเอกภาพและสอดคล้องกับนโยบายและแผนแม่บท ICT
ยุทธศาสตร์ที่ ๒ การพัฒนาระบบสารสนเทศและฐานข้อมูล **แผนงานที่ ๑** การนำ ICT มาใช้ในการจัดเก็บข้อมูลงานหลักของหน่วยงาน **แผนงานที่ ๒** การนำ ICT มาใช้สำหรับการบริหารจัดการ และการตัดสินใจของผู้บริหาร **แผนงานที่ ๓** การพัฒนาระบบสารสนเทศภูมิศาสตร์ **แผนงานที่ ๔** การพัฒนาระบบสารสนเทศด้านวิชาการ **แผนงานที่ ๕** การพัฒนาระบบข้อมูลข่าวสารและสื่อความรู้อิเล็กทรอนิกส์	**ยุทธศาสตร์ที่ ๔** การใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อสนับสนุนการสร้างธรรมาภิบาลในการบริหารและการบริการของภาครัฐ ๔.๒ให้ทุกกระทรวงดำเนินการเพื่อพัฒนาบริการอิเล็กทรอนิกส์ของรัฐแบบบูรณาการ (๑) ให้ทุกหน่วยงานปรับปรุงระบบข้อมูลและระบบบริหารจัดการให้สามารถเชื่อมโยงกับ NSDI และ GIN (Government Information Network) ทั้งภายในและระหว่างหน่วยงาน ภายใต้กรอบมาตรฐาน THe-GIF (Government Interoperability Framework) (๒) ให้ทุกหน่วยงานใช้ ICT เป็นช่องทางหนึ่งในการส่งเสริมและสนับสนุนให้ภาคประชาสังคมเข้ามามีส่วนร่วมในการบริหารราชการแผ่นดิน โดยเฉพาะการพัฒนานโยบายหรือบริการสาธารณะ และการออกกฎหมาย การติดตามตรวจสอบ และให้สำนักงานคณะกรรมการพัฒนาระบบราชการ (กพร.) กำหนดเป็นตัวชี้วัดหนึ่งในมาตรการการพัฒนาระบบราชการ ในส่วนที่เกี่ยวกับการบริหารราชการแบบมีส่วนร่วม **ยุทธศาสตร์ที่ ๖** การใช้ ICT เพื่อสนับสนุนการเพิ่มขีดความสามารถในการแข่งขันอย่างยั่งยืน ๖.๔ส่งเสริมการนำ ICT มาใช้ในภาคการผลิตและบริการที่เป็นยุทธศาสตร์ของประเทศและไทยมีความได้เปรียบ โดยเฉพาะการเกษตร การบริการด้านสุขภาพ และการท่องเที่ยว

ยุทธศาสตร์แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน พ.ศ. ๒๕๕๒-๒๕๕๖	ยุทธศาสตร์แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ประเทศไทย พ.ศ. ๒๕๕๒-๒๕๕๖
	(๑) นำ ICT มาพัฒนาด้านการเกษตร โดยการพัฒนาและเชื่อมโยงข้อมูลที่สำคัญต่อการทำการเกษตร โดยเฉพาะข้อมูลที่เกี่ยวกับการจัดการทรัพยากรน้ำในระดับชุมชน ข้อมูลราคาพืชผล ข้อมูลการใช้พื้นที่เกษตรกรรม และสร้างความเข้มแข็งของกลุ่มสหกรณ์การเกษตร และเกษตรกรรายย่อยให้สามารถใช้ประโยชน์จากข้อมูลและความรู้เพื่อเพิ่มผลผลิต และผลิตภาพ รวมทั้งเพื่อการค้าผลผลิตทางการเกษตรอย่างครบวงจร (รวมระบบการบริหารจัดการโลจิสติกส์ ตั้งแต่กระบวนการผลิต การแปรรูป ไปจนถึงการค้าส่ง ค้าปลีกในประเทศ และการส่งออก) โดยเบื้องต้น ให้มีการศึกษาความต้องการใช้ข้อมูลของกลุ่มเกษตรกร และศึกษาห่วงโซ่อุปทานในรายละเอียด เพื่อให้เกิดความเข้าใจพฤติกรรมและความต้องการข้อมูลที่นำไปใช้ประโยชน์ได้จริงในทางปฏิบัติ (๒) พัฒนาความรู้และทักษะที่เกี่ยวข้องกับการใช้ประโยชน์จาก ICT และสารสนเทศ (รวมถึงข้อมูลทรัพยากรน้ำในชุมชน) ให้แก่เกษตรกร โดยสร้างเครือข่ายการเรียนรู้ด้าน ICT ให้กับเกษตรกรผ่านหน่วยงานที่มีอยู่แล้วในท้องถิ่น เช่น ศูนย์บริการชุมชน โรงเรียน วัด ไปรษณีย์ สหกรณ์ และองค์กรท้องถิ่นอื่นๆ และสร้างผู้สอนในท้องถิ่นเพื่อให้คำปรึกษาเกี่ยวกับการใช้ ICT แก่เกษตรกร (๔) ส่งเสริมและสนับสนุนการจัดทำโครงการนำร่องระบบเกษตรความแม่นยำสูง (Precision agriculture) เพื่อพัฒนาการผลิตให้สามารถควบคุมการผลิตให้บรรลุตามเป้าหมายที่กำหนด เป็นการเพิ่มผลผลิตและผลิตภาพของการทำการเกษตร กับชุมชนเกษตรกรที่มีความพร้อม
<u>ยุทธศาสตร์ที่ ๓</u> การพัฒนาระบบคอมพิวเตอร์ **<u>แผนงานที่ ๑</u>** การจัดหาครุภัณฑ์คอมพิวเตอร์พร้อมอุปกรณ์ต่อพ่วง เพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน และการให้บริการ **<u>แผนงานที่ ๒</u>** การบำรุงรักษาระบบเครือข่ายและคอมพิวเตอร์	**<u>ยุทธศาสตร์ที่ ๓</u>** การพัฒนาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร ๓.๔พัฒนาโครงสร้างพื้นฐานสารสนเทศสำหรับบริการภาคสังคมที่สำคัญต่อความปลอดภัยสาธารณะและคุณภาพชีวิตของประชาชน (๕) ให้จัดสรรทรัพยากรด้าน ICT ให้กับหน่วยงานที่มีหน้าที่เกี่ยวกับการเตือนภัยและการบริหารจัดการภัยพิบัติอย่างเหมาะสม เพื่อจัดซื้ออุปกรณ์ที่ทันสมัยและมีประสิทธิภาพสามารถเฝ้าระวังภัยที่เกิดจากธรรมชาติ เช่น ดินถล่ม แผ่นดินไหว น้ำท่วม เป็นต้น และสามารถเตือนภัยได้ทันท่วงที สอดคล้องกับแนวปฏิบัติตามมาตรฐานสากล อันจะช่วยลดความสูญเสียต่อชีวิตและทรัพย์สินของประชาชน

ยุทธศาสตร์แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน พ.ศ. ๒๕๕๒-๒๕๕๖	ยุทธศาสตร์แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ประเทศไทย พ.ศ. ๒๕๕๒-๒๕๕๖
<u>ยุทธศาสตร์ที่ ๔</u> การพัฒนาระบบเครือข่ายและการสื่อสารข้อมูล **<u>แผนงานที่ ๑</u>** การพัฒนาระบบเครือข่ายและการสื่อสารข้อมูล กรมพัฒนาที่ดิน **<u>แผนงานที่ ๒</u>** การรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์และการสื่อสาร กรมพัฒนาที่ดิน	**<u>ยุทธศาสตร์ที่ ๓</u>** การพัฒนาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร ๓.๓พัฒนาโครงสร้างพื้นฐานสารสนเทศและการสื่อสารเพื่อยกระดับการศึกษา และการเรียนรู้ตลอดชีวิตของประชาชน (๖) ขยายขอบเขตของศูนย์สารสนเทศตำบล หรือที่ทำการไปรษณีย์ รวมทั้งศูนย์สารสนเทศชุมชนรูปแบบต่าง ๆ ที่มีอยู่ เป็นศูนย์บริการสารสนเทศสาธารณะ ที่ประชาชนสามารถเข้ามาใช้บริการได้ โดยรัฐสนับสนุนงบประมาณค่าดำเนินการบางส่วน และบางส่วนเก็บจากผู้ใช้บริการ มีรูปแบบวิธีการในการดำเนินงานให้เกิดความยั่งยืน ๓.๖สร้างความมั่นคงปลอดภัยให้กับโครงข่ายสารสนเทศของประเทศ (๓) ให้นำแผนแม่บทด้านความมั่นคงปลอดภัยของระบบสารสนเทศแห่งชาติ (National information security master plan) ซึ่งได้รับความเห็นชอบแล้ว มาใช้กับหน่วยงานของรัฐ และเอกชน ให้มีผลอย่างกว้างขวางและทั่วถึง โดยเริ่มจากหน่วยงานภาครัฐ และหน่วยงานที่เกี่ยวกับโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Critical infrastructure) เช่น การเงิน สาธารณูปโภค การขนส่ง ฯลฯ ทั้งหมดเป็นลำดับแรก (๔) ส่งเสริมและสนับสนุนให้เกิดความรู้ความเข้าใจถึงภัยอันตราย ซึ่งอาจเกิดขึ้นกับระบบสารสนเทศ อันจะส่งผลความเสียหายในวงกว้างของกิจกรรมต่างๆ ซึ่งใช้ระบบสารสนเทศของทุกภาคส่วนในสังคมไทย ทั้งนี้เพื่อจะได้กำหนดแนวทางในการป้องกันอย่างเหมาะสมต่อไป

ที่มา : ศูนย์สารสนเทศ กรมพัฒนาที่ดิน

๑.๔ โครงสร้างศูนย์สารสนเทศ



ภาพที่ ๑ โครงสร้างศูนย์สารสนเทศ

อัตรากำลังทั้งสิ้น ๔๘ อัตรา ประกอบด้วย ข้าราชการ ๑๘ อัตรา ลูกจ้างประจำ ๕ อัตรา พนักงานราชการ ๑๗ อัตรา และ จ้างเหมาเอกชน ๘ อัตรา

๑.๔.๑ ภารกิจของศูนย์สารสนเทศ

๑.๔.๑.๑ จัดทำแผนแม่บทระบบสารสนเทศด้านการพัฒนาที่ดิน

๑.๔.๑.๒ ศึกษาและพัฒนาระบบเทคโนโลยีสารสนเทศด้านการบริหารจัดการ จัดวางระบบฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ และระบบการสื่อสารข้อมูลของกรมฯ

๑.๔.๑.๓ เป็นศูนย์กลางข้อมูลภูมิสารสนเทศด้านดินของกระทรวงฯ และเป็นศูนย์ฝึกอบรมระบบเทคโนโลยีสารสนเทศและภูมิสารสนเทศทางการเกษตร

๑.๔.๑.๔ ปฏิบัติงานร่วมกับ หรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ได้รับมอบหมาย

๑.๔.๒ อำนาจหน้าที่แต่ละกลุ่ม/ฝ่าย ของศูนย์สารสนเทศ

๑.๔.๒.๑ ฝ่ายบริหารทั่วไป

๑) ดำเนินการเกี่ยวกับงานบริหารทั่วไป

๒) จัดทำแผนงาน งบประมาณประจำปี ควบคุมการเบิกจ่ายงบประมาณ ติดตามผลการปฏิบัติงานของกลุ่มต่าง ๆ ภายในศูนย์

๓) งานบริหารงานบุคคลและงานประชาสัมพันธ์ของศูนย์

๔) ตรวจสอบและกลั่นกรองเรื่องต่าง ๆ ก่อนนำเสนอผู้อำนวยการศูนย์ รวมทั้งประสานงานระหว่างศูนย์กับหน่วยงานอื่น ๆ

๑.๔.๒.๒ กลุ่มวิเคราะห์และวางระบบข้อมูล

๑) ศึกษา วิเคราะห์ ออกแบบและวางระบบคอมพิวเตอร์ ทั้งด้าน Hardware/ Software การสื่อสาร ให้สามารถรองรับสอดคล้องเชื่อมโยงทั้งภายในและภายนอกหน่วยงานต่าง ๆ

๒) จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ แผนปฏิบัติการของกรมฯ ให้สอดคล้องกับของชาติ

๓) บริหารการดำเนินงานตามโครงการพัฒนาระบบสารสนเทศ

๔) ประสานงานด้านนโยบายสารสนเทศกับกระทรวงเกษตรและสหกรณ์ สำนักงบประมาณ และหน่วยงานที่เกี่ยวข้อง

๕) ประสานงานให้คำปรึกษาแนะนำการพัฒนาระบบสารสนเทศ

๑.๔.๒.๓ กลุ่มระบบเครือข่ายและคอมพิวเตอร์

๑) จัดหา พัฒนาระบบเครือข่ายคอมพิวเตอร์และการสื่อสารตามแผนและงบประมาณด้านสารสนเทศ

๒) เป็นแม่ข่ายของระบบและรับผิดชอบการซ่อมบำรุง ดูแลรักษาระบบเครื่องและควบคุมพัฒนาระบบ เชื่อมโยงข้อมูลต่าง ๆ ของกรมฯ และกระทรวงเกษตรและสหกรณ์ ในระบบอินเตอร์เน็ต (Internet) และ ระบบอินทราเน็ต (Intranet)

๓) พัฒนาระบบเครือข่ายและการสื่อสารรูปแบบ อินเตอร์เน็ต (Internet) และระบบอินทราเน็ต (Intranet) ให้เชื่อมต่อกันอย่างมีประสิทธิภาพสูง

๔) กำหนดระเบียบและมาตรฐานรหัสดัชนีแฟ้มข้อมูลด้านปฏิบัติงานระบบเครือข่ายในการกำหนด User/Password

๕) จัดฝึกอบรม ฝึกสอนเพื่อการใช้งานโปรแกรมคอมพิวเตอร์ และระบบเครือข่ายของกรมฯ โดยถ่ายทอดเทคโนโลยีสารสนเทศ และการเพิ่มพูนความรู้ ความสามารถ ด้านคอมพิวเตอร์ที่เกี่ยวข้องแก่บุคลากรกรมพัฒนาที่ดิน

๖) จัดระบบการสื่อสาร โทรคมนาคม และงานวิทยุกระจายเสียง เพื่อการประชาสัมพันธ์ด้านพัฒนาที่ดินและอื่น ๆ ที่เกี่ยวข้องด้านการเกษตร

๑.๔.๒.๔ กลุ่มฐานข้อมูลสารสนเทศ

๑) รวบรวม จัดเก็บข้อมูลและปรับปรุงข้อมูลด้านบริหารจัดการและวิชาการ ให้เป็นปัจจุบัน เพื่อเข้าสู่ระบบเครือข่ายทางระบบอินเตอร์เน็ต (Internet) และ ระบบอินทราเน็ต (Intranet)

๒) ศึกษา ออกแบบ วิเคราะห์ จัดหาและพัฒนาโปรแกรมและฐานข้อมูลด้านการบริหาร การจัดการ และด้านวิชาการ

๓) ศึกษา วิเคราะห์ ออกแบบ จัดหา พัฒนาและบริหารห้องสมุดอิเล็กทรอนิกส์ โดยการรวบรวมจัดหาเอกสารวิชาการ วารสารทั้งภาษาไทยและต่างประเทศ จัดหมวดหมู่ จัดระบบการให้ยืมเอกสาร และพัฒนาระบบงานห้องสมุดให้อยู่ในรูปอิเล็กทรอนิกส์ รวมทั้งบริการและให้คำปรึกษาแนะนำ

๔) ดำเนินการตามบทบัญญัติของพระราชบัญญัติข้อมูลข่าวสารของราชการ

๕) ให้บริการข้อมูลด้านการบริหารการจัดการและวิชาการ แก่ผู้บริหารและผู้เกี่ยวข้อง

๖) ติดต่อประสานงาน แลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานอื่นที่เกี่ยวข้อง

๑.๔.๒.๕ กลุ่มระบบภูมิสารสนเทศ

๑) เป็นศูนย์กลางระบบสารสนเทศภูมิศาสตร์ของกระทรวงเกษตรและสหกรณ์

๒) จัดทำรวบรวมข้อมูล (Meta Data) ด้านภาพถ่ายทางอากาศ ภาพถ่ายดาวเทียมและแฟ้มข้อมูลแผนที่ทุกประเภท เพื่อเป็นฐานข้อมูลสำหรับบริการหน่วยงานต่าง ๆ ของกรมฯ และกระทรวงเกษตรและสหกรณ์

๓) จัดทำมาตรฐานข้อมูล (Meta Data) ด้านภูมิสารสนเทศ เพื่อใช้แลกเปลี่ยนและบริการ

๔) จัดเก็บ รวบรวมและปรับปรุงข้อมูลสารสนเทศด้านภูมิศาสตร์ให้เป็นปัจจุบันเพื่อเข้าสู่ระบบเครือข่ายกลาง

๗) จัดหาและพัฒนาเทคโนโลยีและโปรแกรมการใช้งานทางด้านระบบภูมิสารสนเทศ และการให้บริการข้อมูลต่าง ๆ ในรูปของโปรแกรมบนระบบเครือข่ายระบบ Online ทั้งในระบบอินเตอร์เน็ต (Internet) และ ระบบอินทราเน็ต (Intranet)

๕) ประสาน ดำเนินการ วิเคราะห์จัดทำข้อมูล กรณีเร่งด่วนด้านการบริหารสินทรัพย์ ด้านการเตือนภัย การติดตามประเมินผลการใช้ประโยชน์ที่ดินให้ผู้บริหารทางด้านภูมิสารสนเทศแก่กระทรวงเกษตรและสหกรณ์

๖) บริการข้อมูลด้านระบบสารสนเทศภูมิศาสตร์แก่ผู้บริหาร ผู้เกี่ยวข้องและประชาชน

๗) จัดฝึกอบรมด้านการพัฒนาทางระบบสารสนเทศภูมิศาสตร์ เพื่อการพัฒนางานด้านการเกษตรให้แก่เจ้าหน้าที่ทุกกรมฯ ในกระทรวงเกษตรและสหกรณ์ รวมทั้งสถาบันการศึกษาและองค์กรเอกชนที่ปฏิบัติหรือมีส่วนเกี่ยวข้องด้านการเกษตร

จากวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ ภารกิจ และอำนาจหน้าที่ข้างต้น ศูนย์สารสนเทศ เป็นหน่วยงานกลางที่ทำหน้าที่ด้านการพัฒนาเทคโนโลยีสารสนเทศให้เกิดผลสัมฤทธิ์ มุ่งเน้นการปรับปรุงประสิทธิภาพเครือข่ายและเทคโนโลยี เพื่อตอบสนองความต้องการของผู้ใช้งานสารสนเทศ พัฒนาระบบงานบริการด้านสารสนเทศ เพื่ออำนวยความสะดวกในการปฏิบัติงานให้กับเจ้าหน้าที่ภายในกรมพัฒนาที่ดิน รวมถึงการให้บริการข้อมูลด้านต่างๆ แก่เกษตรกร นักศึกษา ประชาชนทั่วไป ผ่านเว็บไซต์กรมพัฒนาที่ดิน พัฒนาระบบฐานข้อมูลสนับสนุนผู้บริหารในการบริหารจัดการการตัดสินใจแก้ไขปัญหาที่เกิดขึ้นได้อย่างถูกต้อง แม่นยำ และรวดเร็ว ทันเวลากับสถานการณ์ต่างๆ ที่เกิดขึ้นอย่างเหมาะสม

๑.๕ ขอบเขตการให้บริการด้านสารสนเทศ

๑.๕.๑ ด้านระบบเครือข่ายและการสื่อสาร

ระบบเครือข่ายสื่อสารคอมพิวเตอร์ กรมพัฒนาที่ดิน : LDD Net ในปัจจุบันวางโครงสร้างระบบโดยศูนย์กลางของระบบ (Backbone) ตั้งอยู่ที่กรมพัฒนาที่ดิน ถนนพหลโยธิน แขวงลาดยาว เขตจตุจักร กรุงเทพฯ และมีเครือข่ายเชื่อมโยงไปยังหน่วยงานในส่วนภูมิภาคทั่วประเทศรวมทั้ง การต่อเชื่อมหน่วยงานระดับกอง/สำนักงานพัฒนาที่ดินเขต/ สถานีพัฒนาที่ดิน เพื่อการสื่อสารข้อมูลคอมพิวเตอร์หรือการสื่อสาร

รูปแบบอื่นในอนาคตสามารถใช้งานได้อย่างรวดเร็วและมีประสิทธิภาพ ตอบสนองความต้องการของผู้ใช้งานยิ่งขึ้น

โครงข่ายสื่อสารคอมพิวเตอร์ LDD-Net ระบบเครือข่ายคอมพิวเตอร์ของ กรมพัฒนาที่ดิน ประกอบด้วยระบบเครือข่ายหลัก ๒ ระบบ คือ ๑.ระบบเครือข่ายหลักส่วนกลาง (Central Local Area Network; CLN) ๒.ระบบเครือข่ายส่วนภูมิภาค (Regional Local Area Network: RLN) เครือข่ายในปัจจุบันของ กรมพัฒนาที่ดิน ระหว่างหน่วยงานส่วนกลางและส่วนภูมิภาคแบ่งเป็นระบบ LAN จำนวน ๑๑๐ วง ประกอบด้วย ส่วนกลาง ๑๖ วง สำนักงานพัฒนาที่ดินเขต ๑-๑๒ จำนวน ๑๒ วง ศูนย์ศึกษาฯ จำนวน ๓ วง โครงการในพระราชดำริ ๓ วง และสถานีพัฒนาที่ดิน จำนวน ๗๗ วง

๑.๕.๑.๑ ระบบเครือข่ายหลักส่วนกลาง (Central Local Area Network : CLN)

ระบบเครือข่าย LDD-Net ทำหน้าที่เชื่อมโยงระบบเครือข่ายระดับกอง/สำนักงาน เข้าด้วยกัน โดยมีระบบ CLN เป็นเครือข่ายหลัก ซึ่งมี ATM Switch เป็นศูนย์กลางการเชื่อมต่อ และมี Backbone LAN Switch จำนวน ๒ ชุด ตั้งอยู่ที่ศูนย์สารสนเทศ จำนวน ๑ ชุด และสำนักงานเลขานุการกรม จำนวน ๑ ชุด ATM Switch และ Backbone LAN Switch เชื่อมต่อด้วยสายใยแก้วนำแสงมีความเร็วในการจัดส่ง ๖๒๒ Mbps และ เชื่อมโยง Backbone LAN Switch ทั้ง ๒ ชุด ด้วยสายใยแก้วนำแสงที่มีความเร็วในการจัดส่ง ๑๐๐ Mbps เข้าด้วยกัน

จากระบบเครือข่ายแกนหลัก จะกระจายระบบการเชื่อมต่อเครือข่ายภายในส่วนกลาง (LAN) จาก Backbone CORE Switch ไปที่ DISTRIBUTE Switch และกระจายการเชื่อมต่อไปยัง ACCESS Switch ด้วยสื่อนำสัญญาณชนิดสายใยแก้วนำแสง (Fiber Optics) หรือสายคู่เกลียวบิดไม่หุ้มเกราะ (Unshielded Twisted Pairs : UTP) ที่มีความเร็วในการจัดส่งไม่ต่ำกว่า ๑๐๐ Mbps เพื่อทำหน้าที่เชื่อมโยงเครื่องคอมพิวเตอร์ของระบบเครือข่ายภายในของกอง และ สำนักต่างๆ เข้าด้วยกัน ระบบเครือข่ายกรมพัฒนาที่ดิน เป็นประเภทเครือข่ายแบบผู้ให้บริการ และผู้ใช้บริการ (Client/Server Network) ใช้เทคโนโลยี VLAN (Virtual Local Area Network) เป็นระบบของกลุ่มคอมพิวเตอร์ที่อยู่ในบรอดคาสต์โดเมน(Broadcast Domain) เดียวกัน

ระบบเครือข่าย LDD-Net ที่ CLN มีอุปกรณ์กำหนดเส้นทาง (Routers) ให้ระบบเชื่อมต่อเข้าด้วยกันทั้งหมดโดยผ่าน ATM Switch และสามารถติดต่อเชื่อมโยงไปยังระบบเครือข่ายของสำนักงานพัฒนาที่ดิน ๑๒ เขต ศูนย์ศึกษาฯและสถานีพัฒนาที่ดิน โดยผ่านระบบ MPLS (Multi Protocol Label Switching) ที่ความเร็ว ๑๐๐ Mbps

๑.๕.๑.๒ ระบบเครือข่ายส่วนภูมิภาค (Regional Local Area Network : RLN)

ในส่วนระบบเครือข่ายระดับสำนักงานพัฒนาที่ดินเขต (RLN) เป็นเครือข่ายแบบ LAN ประกอบด้วย เครื่อง Server ที่ทำหน้าที่เป็นแม่ข่ายของสำนักงานพัฒนาที่ดินเขต และเครื่อง Client ที่อยู่ในกลุ่ม/ฝ่าย ของสำนักงานพัฒนาที่ดินเขต มีความเร็วในการใช้งานในระบบอยู่ที่ ๑๐๐ Mbps โดยสามารถติดต่อเชื่อมโยงมายังระบบเครือข่าย (ส่วนกลาง) และเครือข่ายระบบอินเตอร์เน็ต (Internet) ของผู้ให้บริการผ่านระบบ MPLS (Multi Protocol Label Switching) ที่ความเร็ว ๘ Mbps

ในส่วนระบบเครือข่ายระดับสถานีพัฒนาที่ดิน เป็นเครือข่ายแบบ LAN ประกอบด้วยเครื่อง Server ที่ทำหน้าที่เป็นแม่ข่ายของ สพด. และเครื่อง Client ที่อยู่ในกลุ่ม/ฝ่าย ของสถานีพัฒนาที่ดิน มีความเร็วในการใช้งานในระบบอยู่ที่ ๑๐๐ Mbps โดยสามารถติดต่อเชื่อมโยงมายังระบบเครือข่าย (ส่วนกลาง) และเครือข่ายระบบอินเตอร์เน็ต (Internet) ของผู้ให้บริการ ผ่านระบบ MPLS (Multi Protocol Label Switching) ที่ความเร็ว ๒ Mbps

๑.๕.๒ ด้านระบบสารสนเทศและข้อมูล

การนำเทคโนโลยีสารสนเทศและเครือข่ายสื่อสารมาประยุกต์ใช้ในการปฏิบัติงานเพื่อเพิ่มประสิทธิภาพการดำเนินงานของ กรมพัฒนาที่ดิน สนับสนุนกระบวนการหลักของกรมฯ ให้มีคุณค่า ทันสมัย มีความต่อเนื่องทันต่อเหตุการณ์ และสามารถใช้สารสนเทศให้เกิดประโยชน์สูงสุด ซึ่งจะช่วยให้องค์การสามารถนำข้อมูลมาตัดสินใจแก้ไขปัญหาที่เกิดขึ้นได้อย่างถูกต้อง แม่นยำ และรวดเร็ว ทันเวลากับสถานการณ์ต่างๆ ปัจจุบันมีระบบบริการสารสนเทศที่ให้บริการ ๒ ช่องทาง ดังนี้

๑.๕.๒.๑ ระบบบริการสารสนเทศผ่านช่องทางระบบอินเตอร์เน็ต (Internet)

สำหรับให้บริการประชาชน เกษตรกร และผู้สนใจทั่วไป ประกอบด้วยระบบต่าง ๆ ดังนี้

๑) ระบบบริการประชาชน เพื่อเป็นการอำนวยความสะดวกให้แก่เกษตรกรและผู้สนใจในการขอรับบริการ สารเร่ง พด. ต่างๆ กล้าแฝก และเมล็ดพันธุ์พืชเพื่อการอนุรักษ์ดินและน้ำ จึงได้จัดทำระบบบริการประชานชนขึ้น เกษตรกรสามารถขอรับบริการได้ผ่านทางเครือข่ายระบบอินเตอร์เน็ต (Internet) และในกรณีที่เกษตรกรขอรับบริการสารเร่ง ทางกรมฯ มีบริการจัดส่งให้ทางไปรษณีย์ ช่วยประหยัดเวลาและค่าใช้จ่ายในการเดินทางมาติดต่อขอรับบริการที่หน่วยงานโดยตรง

๒) ฐานข้อมูลบันทึก Stock วัสดุการเกษตร เพื่อให้ ผู้ขอรับบริการตรวจสอบยอดคงเหลือวัสดุการเกษตรแต่ละชนิด ก่อนขอรับบริการที่หน่วยงาน หรือขอรับบริการผ่านระบบบริการประชาชน

๓) รายงานผลการวิเคราะห์ตัวอย่างดิน น้ำ ปุ๋ย เพื่อให้ ผู้ขอรับบริการตรวจสอบข้อมูลผลการวิเคราะห์ดิน น้ำ ปุ๋ย ผ่านระบบเครือข่ายอินเตอร์เน็ต (Internet) ได้ตลอดเวลา

๔) ระบบฐานข้อมูลแหล่งน้ำขนาดเล็ก เพื่อติดตามความก้าวหน้าการดำเนินการก่อสร้างแหล่งน้ำขนาดเล็กในพื้นที่ต่าง ๆ ผู้ใช้งานสามารถเรียกดูข้อมูลผ่านระบบอินเตอร์เน็ต (Internet) ได้ เช่น ข้อมูลโครงการ สถานที่ดำเนินการ ผู้ดำเนินการ

๕) ระบบฐานข้อมูลหมอดินอาสา เป็นระบบสำหรับรวบรวมข้อมูลประวัติหมอดินอาสาประจำหมู่บ้าน ประจำตำบล ประจำอำเภอ และประจำจังหวัด เพื่อเป็นการสร้างเครือข่ายของกรมฯ สนับสนุนการดำเนินงานโครงการตามนโยบายของกรมพัฒนาที่ดิน และ กระทรวงเกษตรและสหกรณ์

๖) ระบบฐานข้อมูลแหล่งน้ำในไร่นานอกเขตชลประทาน เป็นระบบสำหรับเกษตรกรที่สนใจเข้าร่วมโครงการแหล่งน้ำในไร่นานอกเขตชลประทาน โดยการขุดสระน้ำขนาด ๑,๒๖๐ ลูกบาศก์เมตร โดยเกษตรกรสามารถยื่นคำร้องขอขุดสระน้ำผ่านทางอินเตอร์เน็ต (Internet) ได้ ซึ่งกรมพัฒนาที่ดินจะได้นำข้อมูลไปพิจารณาและดำเนินการต่อไป

๗) ห้องสมุดอิเล็กทรอนิกส์ (E-Library) ผู้ใช้บริการห้องสมุดกรมพัฒนาที่ดินสามารถตรวจสอบหนังสือที่ต้องการในรูปแบบ Catalog และตรวจสอบสภาพหนังสือที่พร้อมให้ยืมได้ พร้อมทั้งสืบค้นข้อมูลจากห้องสมุดอื่น แบบ Broadcast Searching และเรียกอ่าน E-book หรือ บทคัดย่อ ข้อมูลของกรมพัฒนาที่ดินได้ทันที ทั้งนี้สามารถ ยืม – คืน ทรัพยากรในห้องสมุด ได้อย่างรวดเร็วโดยใช้ Barcode

๘) ระบบรับรองมาตรฐานสินค้าประเภทปัจจัยการผลิตทางการเกษตร สำหรับผู้ประกอบการ กลุ่มเกษตรกร หรือผู้สนใจสามารถยื่นคำขอรับรองมาตรฐานสินค้าประเภทปัจจัยการผลิตทางการเกษตร เช่น ปุ๋ยชีวภาพ ปุ๋ยอินทรีย์ สารปรับปรุงบำรุงดิน ฯลฯ ซึ่งกรมพัฒนาที่ดินมีการตรวจ

รับรองและออกใบอนุญาตการใช้เครื่องหมายรับรองมาตรฐาน ปัจจัยการผลิตทางการเกษตร “Q” ผ่านทางเว็บไซต์ของกรมพัฒนาที่ดิน (ระบบ Q Center)

๙) ห้องเรียนอิเล็กทรอนิกส์ (e-Learning) เพื่อรวบรวมองค์ความรู้ตามยุทธศาสตร์ ของกรมพัฒนาที่ดิน มาจัดทำเป็นรูปแบบการเรียนรู้ด้วยสื่ออิเล็กทรอนิกส์ สำหรับให้เกษตรกร นักเรียน นักศึกษา และประชาชนทั่วไป สามารถศึกษาค้นคว้าคว้าเรียนรู้ด้วยตนเอง ผ่านทางเว็บไซต์กรมพัฒนาที่ดิน ปัจจุบันมีทั้งสิ้น ๑๓ หลักสูตร

๑๐) ระบบการจัดซื้อจัดจ้าง กรมพัฒนาที่ดิน เพื่อช่วยสนับสนุนการปฏิบัติงานของเจ้าหน้าที่พัสดุของทุกหน่วยงาน ในการบันทึกข้อมูลการจัดซื้อจัดจ้างเข้าสู่ระบบและเผยแพร่ประชาสัมพันธ์ผ่านทางเว็บไซต์ได้ด้วยความคล่องตัวสะดวก และอำนวยความสะดวกให้กับภาคเอกชนในฐานะผู้ขายที่ต้องการเข้าร่วมในการจัดซื้อจัดจ้างของหน่วยงาน และ กรมพัฒนาที่ดิน ในฐานะผู้ซื้อ สามารถแสดงถึงความโปร่งใสและตรวจสอบได้ในทุกขั้นตอนกระบวนการจัดซื้อจัดจ้าง

๑๑) ระบบ e-Search LDD พัฒนาระบบค้นหาข้อมูลวิชาการ ผลงานวิจัย งานบริการและฐานข้อมูล กรมพัฒนาที่ดิน (e-Search LDD) ขึ้น เพื่อเป็นแหล่งรวบรวมรายการดังกล่าวในรูปแบบฐานข้อมูล เพื่อให้ประชาชนทั่วไปสามารถค้นหาข้อมูลที่จำเป็นหรือความรู้ที่เกี่ยวข้องของส่วนราชการได้อย่างสะดวก รวดเร็ว และทั่วถึงมากยิ่งขึ้น

๑๒) KM LDD Blog (Web Blog) เพื่อเป็นช่องทางในการเผยแพร่ข้อมูลองค์ความรู้ที่เป็นประโยชน์จากบุคลากรของกรมพัฒนาที่ดิน สนับสนุนการมีส่วนร่วมในการแลกเปลี่ยนและแบ่งปันความรู้ต่าง ๆ ผ่านเครือข่าย ระบบอินเตอร์เน็ต (Internet)

๑๓) บัญชีรายการข้อมูลกรมพัฒนาที่ดิน เพื่อเผยแพร่ข้อมูลในส่วนที่กรมพัฒนาที่ดินเป็นผู้ผลิต หรือรับผิดชอบ ให้ผู้สนใจสามารถศึกษารายละเอียดของข้อมูลเบื้องต้น ก่อนที่จะขอรับบริการข้อมูลหรือนำข้อมูลไปใช้ประโยชน์ โดยจัดทำเป็นรายละเอียดบนเว็บไซต์กรมพัฒนาที่ดิน

๑.๕.๒.๒ ระบบบริการสารสนเทศผ่านช่องทาง Intranet เป็นระบบเครือข่ายภายในกรมพัฒนาที่ดิน ที่ให้บริการระบบงานสารสนเทศที่เกี่ยวข้องกับข้าราชการและเจ้าหน้าที่ ซึ่งเป็นโครงสร้างพื้นฐานที่สำคัญขององค์การ ไม่ว่าจะเป็นด้านข้อมูลระบบ และเครือข่าย ที่จะสามารถส่งเสริมให้คนในองค์การมีศักยภาพเพิ่มขึ้น และสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ อำนวยความสะดวกในการปฏิบัติงานให้สะดวกรวดเร็วยิ่งขึ้น โดยมีระบบ ดังนี้

๑) ไปรษณีย์ พ.ด. (LDD Mail) เป็นโปรแกรมที่ใช้ในการรับ-ส่งเมล์ของกรมพัฒนาที่ดิน เฉพาะสมาชิกบนระบบเครือข่ายของกรมฯ

๒) ระบบสำนักงานอิเล็กทรอนิกส์ (e-Office) เป็นกระบวนการนำเทคโนโลยีสารสนเทศ (Information Technology) ทั้งระบบฐานข้อมูล และระบบเครือข่ายมาประยุกต์ใช้ในงานสำนักงาน ช่วยลดขั้นตอนการทำงาน สามารถดำเนินการได้แบบระบบเรียลไทม์ (Real-time system) เช่น การจัดทำใบลา การเบิกวัสดุสำนักงานสิ้นเปลือง โดยเจ้าหน้าที่ทำการล็อกอิน (Login) เข้าสู่ระบบ กรอกข้อมูลตามแบบฟอร์มเอกสารที่กำหนด พร้อมทั้งลงนามลายมือชื่ออิเล็กทรอนิกส์เพื่อขออนุมัติ ระบบสามารถสืบค้นข้อมูลเพื่อติดตามผลการอนุมัติได้ และสามารถใช้ระบบได้ทุกสถานที่ ทุกเวลาผ่านเครือข่ายอินเตอร์เน็ต (Internet)

๓) ระบบตรวจสอบเวลาการทำงานผ่าน Web ข้าราชการและลูกจ้างประจำ (ส่วนกลาง) สามารถตรวจสอบเวลาการทำงานของตนเองได้หลังจากทาบบัตรประจำตัวอิเล็กทรอนิกส์กับ

เครื่องบันทึกเวลาแล้ว และผู้บังคับบัญชาสามารถตรวจสอบได้ว่าเจ้าหน้าที่ภายในหน่วยงานของตนเองมาทำงานหรือไม่

๔) ระบบตรวจสอบ บริหารเวลาปฏิบัติงานของบุคลากร กรมพัฒนาที่ดิน เพื่อให้เจ้าหน้าที่ที่รับผิดชอบการลาของแต่ละหน่วยงาน บันทึกการลาป่วย ลากิจส่วนตัว ไปราชการต่างจังหวัด เป็นต้น ของเจ้าหน้าที่ในหน่วยงานตนเองได้

๕) คำสั่งต่างๆ เจ้าหน้าที่ของกรมพัฒนาที่ดินสามารถค้นหาคำสั่งต่างๆ หรือคำสั่งย้อนหลังเป็นรายปี

๖) ระบบสารบรรณอิเล็กทรอนิกส์ เป็นระบบลงรับหนังสือราชการผ่านระบบอิเล็กทรอนิกส์ โดยระบบจะออกเลขหนังสือให้อัตโนมัติ สามารถตรวจสอบการรับเอกสารต้นฉบับได้อย่างสะดวกและรวดเร็ว และสามารถติดตามงานได้เองจากระบบ สามารถค้นหาเอกสารรับ และเอกสารส่ง ได้อย่างรวดเร็ว โดยค้นหาจากเลขที่หนังสือ,วันที่ลงรับ เป็นต้น ช่วยลดขั้นตอนการทำงาน และลดปริมาณการใช้กระดาษได้

๗) ระบบการประชุมอิเล็กทรอนิกส์(e-Meeting) ระบบการประชุมแบบไร้กระดาษโดยนำวาระการประชุมและเอกสารประกอบการประชุมเข้าสู่ระบบอิเล็กทรอนิกส์ ซึ่งผู้เข้าร่วมประชุมสามารถเรียกดูวาระและเอกสารประกอบการประชุมผ่านทางระบบอินเตอร์เน็ต (Internet) และสามารถสืบค้นข้อมูลการประชุมย้อนหลังได้

๘) ฐานข้อมูลครุภัณฑ์กรมพัฒนาที่ดิน เพื่อใช้จัดเก็บฐานข้อมูลครุภัณฑ์ของกรมพัฒนาที่ดินทั้งหมด ประกอบด้วย ๒ ระบบคือ ระบบบริหารครุภัณฑ์ Online กรมพัฒนาที่ดิน และระบบบริหารครุภัณฑ์ต่ำกว่าเกณฑ์ เพื่อให้เป็นมาตรฐานเดียวกันทุกหน่วยงานตามระเบียบสำนักนายก และสามารถสืบค้นข้อมูลได้สะดวก รวดเร็ว ผ่านทางระบบอินเตอร์เน็ต (Internet) เพื่อให้ผู้บริหาร เจ้าหน้าที่พัสดุของส่วนบริหารสินทรัพย์ กองคลัง เจ้าหน้าที่พัสดุของหน่วยงาน และกลุ่มงานตรวจสอบภายใน สามารถติดตาม ตรวจสอบข้อมูลได้ตลอด ๒๔ ชั่วโมง นอกจากนี้ยังสามารถพิมพ์รายงานตรวจนับครุภัณฑ์คงเหลือประจำปีเพื่อใช้เป็นเอกสารอ้างอิงในการตรวจสอบข้อมูลได้ด้วย

๑.๕.๒.๓ ระบบการบริหารจัดการการตัดสินใจเชิงพื้นที่ (Executive Information System-EIS ด้านการพัฒนาที่ดิน) ศูนย์สารสนเทศ ได้ดำเนินการนำเอาระบบเทคโนโลยีทางด้านการจัดการข้อมูลเชิงพื้นที่ มาใช้งานการบริหารจัดการกิจกรรมต่าง ๆ โดยระบบดังกล่าว จะเป็นการผสมผสานเทคโนโลยี ทั้งในรูปแบบของระบบสารสนเทศภูมิศาสตร์ และการบริหารจัดการฐานข้อมูล ตลอดจนการพัฒนาโปรแกรมประยุกต์ ที่มีการใช้เทคโนโลยีสารสนเทศภูมิศาสตร์ทำงานรูปแบบของเว็บแอพพลิเคชั่น (Web Application) ในแต่ละระบบผู้ใช้งานสามารถเข้าถึง เรียกดู และสืบค้นข้อมูล ผ่านทางช่องทางระบบอินเตอร์เน็ต (Internet) หรือ สมาร์ตโฟน (Smart Phone) ได้ มีองค์ประกอบ ๓ ส่วนหลัก คือ

ส่วนที่ ๑ ระบบฐานข้อมูล ซึ่งระบบฐานข้อมูลนี้จะประกอบด้วยทั้งในส่วนของข้อมูลเชิงพื้นที่ และข้อมูลอธิบายประกอบ โดยจะมีข้อมูลอยู่ด้วยกันอยู่ ๒ ลักษณะ คือ

๑) ข้อมูลในรูปแบบของแผนที่ภาพนิ่ง (Static Map) ข้อมูลดังกล่าวจะเป็นข้อมูลที่ไม่มีการเปลี่ยนแปลง เช่น ข้อมูลแผนที่ภาพถ่ายทางอากาศสี มาตรส่วน ๑:๔,๐๐๐ โดยข้อมูลดังกล่าว จะถูกนำมาจัดทำให้อยู่ในรูปแบบของ Tile Image (Map Cache) ซึ่งไม่สามารถที่จะทำการแก้ไขได้ แต่มีประโยชน์ในด้านการแสดงภาพ โดยสามารถแสดงภาพได้อย่างรวดเร็ว ข้อมูลของกรมพัฒนาที่ดิน ที่นำมาจัดทำเป็น Map Cache จำนวน ๖ รายการ ประกอบด้วย

๑.๑) LDD_LU_CACHE แสดงข้อมูลการใช้ประโยชน์ที่ดินของกรมพัฒนาที่ดิน

๑.๒) LDD_BASEMAP_CACHE แสดงข้อมูลแผนที่ฐาน

๑.๓) LDD_RASTER_CACHE แสดงข้อมูลแผนที่ภาพถ่ายทางอากาศสีของกรมพัฒนาที่ดิน มาตราส่วน ๑ : ๔,๐๐๐

๑.๔) LDD_VGT_CACHE แสดงข้อมูลโครงการพื้นที่ปลูกหญ้าแฝกของกรมพัฒนาที่ดิน

๑.๕) LDD_SOIL_CACHE แสดงข้อมูลสารสนเทศภูมิศาสตร์ชุดดินและชั้นความเหมาะสมของพืชกับชุดดินและข้อมูลเกี่ยวกับการจัดการทรัพยากรดินปัญหา และวิธีการแก้ไขปัญหา ครอบคลุมพื้นที่ทั่วประเทศ

๑.๖) LDD_HYBRID_CACHE แสดงข้อมูลแผนที่ฐานสำหรับนำไปใช้ประกอบข้อมูลแผนที่ภาพถ่ายทางอากาศสีของกรมพัฒนาที่ดิน

๒) ข้อมูลในรูปแบบของแผนที่เคลื่อนไหว (Dynamic map) ข้อมูลดังกล่าวจะเป็นข้อมูลที่มีการเปลี่ยนแปลงได้ เช่น ข้อมูลงานโครงการ ข้อมูลการใช้ประโยชน์ที่ดิน เป็นต้น ซึ่งข้อมูลดังกล่าวผู้ใช้งานสามารถทำการแก้ไข เพิ่มเติม ปรับปรุงได้

ส่วนที่ ๒ ระบบซอฟต์แวร์ด้านภูมิสารสนเทศ ประกอบด้วยซอฟต์แวร์ที่ใช้ในการบริหารจัดการข้อมูลภูมิสารสนเทศ มีอยู่ด้วยกัน ๒ ประเภท ได้แก่

๑) ซอฟต์แวร์จัดการและบริการข้อมูลภูมิสารสนเทศผ่านระบบเครือข่าย (GIS Server) ซึ่งจะเป็นซอฟต์แวร์ที่ใช้ในการบริหาร จัดการ และเผยแพร่ข้อมูลผ่านระบบเครือข่ายของกรมพัฒนาที่ดิน ซึ่งสามารถให้บริการได้ทั้งในรูปแบบของระบบอินเตอร์เน็ต (Internet) และ ระบบอินทราเน็ต (Intranet)

๒) ซอฟต์แวร์จัดการการปรับปรุงข้อมูลภูมิสารสนเทศ (GIS Editor) ซึ่งจะเป็นซอฟต์แวร์ที่ใช้งานบนเครื่องคอมพิวเตอร์ Desktop สำหรับการปรับปรุงฐานข้อมูลภูมิสารสนเทศ ให้มีความเป็นปัจจุบัน ตลอดจนการวิเคราะห์ข้อมูลในรูปแบบของการซ้อนทับ

ส่วนที่ ๓ การพัฒนาโปรแกรมประยุกต์ ระบบการบริหารจัดการการตัดสินใจเชิงพื้นที่ (Executive Information System - EIS ด้านการพัฒนาที่ดิน) มีการแสดงผลข้อมูลทั้งในลักษณะเป็นระบบสารสนเทศภูมิศาสตร์ คือแสดงในรูปของแผนที่ และระบบสารสนเทศเพื่อการบริหาร ให้บริการข้อมูลผ่านทางเว็บไซต์ http://eis.ldd.go.th โดยรองรับการแสดงผลผ่าน Internet Explorer ๘ (IE๘) หรือ Mozilla Firefox ๓.๓.๖ หรือ Google Chrome ในส่วนการให้บริการประชาชน/ผู้สนใจทั่วไปมีดังนี้

๑) ระบบเตือนภัยธรรมชาติ (Natural Disasters Warning) เป็นระบบสำหรับการบริหารจัดการ การแจ้งเหตุเมื่อเกิดภัยธรรมชาติ โดยประชาชนในพื้นที่ หรือเจ้าหน้าที่หน่วยงานต่าง ๆ ในพื้นที่ที่เกิดเหตุสามารถทำการรายงาน บันทึก แจ้งเตือน ตรวจสอบ ค้นหาและแสดงผล เหตุการณ์ภัยธรรมชาติที่เกิดขึ้น สามารถรายงานเหตุการณ์ที่เกิดขึ้นด้วยภาพถ่าย หรือวีดีโอตำแหน่งที่เกิดเหตุได้ สามารถค้นหารายงานสรุปเหตุการณ์ภัยธรรมชาติต่าง ๆ ที่เกิดขึ้น แยกตามรายพื้นที่ ระยะเวลา และประเภทของเหตุการณ์ที่เกิดขึ้น ระบบเตือนภัยธรรมชาติ ช่วยในการสนับสนุนข้อมูลด้านต่าง ๆ สำหรับการตัดสินใจของผู้บริหาร ในการปฏิบัติการด้านเหตุวิกฤตภัยธรรมชาติของกรมพัฒนาที่ดิน การวิเคราะห์และบูรณาการสำหรับการตัดสินใจในเชิงรุกของผู้บริหาร รวมถึงการกำหนดนโยบายและยุทธศาสตร์ให้เป็นไปอย่างมีเอกภาพ

๒) ระบบบันทึกตำแหน่งเกิดเหตุผ่านโทรศัพท์มือถือ (Mobile) เป็นระบบสำหรับให้ประชาชน หรือผู้ประสบเหตุ สามารถแจ้งเหตุผ่านโทรศัพท์มือถือเข้ามายังระบบได้ทันที นอกจากนี้ระบบยังสามารถทำการค้นหาตำแหน่งเกิดเหตุ และรายงานการแจ้งเหตุฉุกเฉิน โดยสามารถรายงานเหตุการณ์ที่เกิดขึ้นด้วยภาพถ่าย หรือวีดีโอตำแหน่งที่เกิดเหตุได้ เจ้าหน้าที่ที่รับผิดชอบในพื้นที่สามารถทำการบันทึกข้อมูลและส่งอีเมล์ หรือ SMS แจ้งไปยังผู้เกี่ยวข้องภายในหน่วยงานที่รับผิดชอบ

๓) ระบบตรวจสอบการใช้ประโยชน์ที่ดิน (Present Land use Monitoring) เป็นระบบสำหรับใช้ในการตรวจสอบการใช้ประโยชน์ที่ดินและรายงานการใช้ประโยชน์ที่ดิน ประชาชน เจ้าหน้าที่หน่วยงานที่เกี่ยวข้อง สามารถสอบถามข้อมูลการใช้ประโยชน์ที่ดินในพื้นที่ที่สนใจ หรือค้นหาประเภทการใช้ประโยชน์ที่ดินตามรายชื่อ จังหวัด อำเภอ ตำบล

๔) ระบบบริหารและติดตามโครงการปลูกหญ้าแฝก (Vetiver Grass Tracking) เป็นระบบสำหรับใช้ในการตรวจสอบ บริหารและติดตามโครงการปลูกหญ้าแฝก ที่ได้รับอนุมัติให้ดำเนินการจัดทำให้อยู่ในรูปแบบของระบบสารสนเทศภูมิศาสตร์ เพื่อสะดวกในการบริหารติดตามโครงการฯ สามารถค้นหาข้อมูลการปลูกหญ้าแฝกในพื้นที่ที่สนใจ เป็นข้อมูลสำหรับผู้บริหารสามารถติดตามและจัดการพื้นที่ปลูกหญ้าแฝกเพื่อการดูแลรักษาได้อย่างต่อเนื่อง

๕) ระบบนำเสนอแผนที่ชุดดิน (Soil Series) มาตราส่วน ๑ : ๒๕,๐๐๐ เป็นระบบสำหรับนำเสนอข้อมูลชุดดินและกลุ่มชุดดิน ในประเทศไทย โดยแสดงรายละเอียดเกี่ยวกับ ข้อมูลกลุ่มชุดดิน ชุดดิน ขนาดพื้นที่ คุณสมบัติทางเคมีและกายภาพของแต่ละชุดดิน ปัญหาของดิน ความเหมาะสมของดินในการปลูกพืชแต่ละชนิดในพื้นที่ รวมถึงแนวทางการจัดการดิน สามารถค้นหาจุดเก็บตัวอย่างตามพื้นที่ที่ต้องการ สามารถจัดทำแผนที่ดินและแผนที่ความเหมาะสมในการเพาะปลูกได้ และสามารถจัดทำรายงานการจัดการดิน ค่าสมบัติทางเคมีของดิน สรุปขนาดพื้นที่ข้อมูลดินแยกตามการใช้ประโยชน์ ในพื้นที่ที่ต้องการได้ มีฟังก์ชั่นที่ให้บริการสำหรับประชาชน/ผู้สนใจค้นหาได้ทั้งหมด ๙ ฟังก์ชั่น คือ สอบถามข้อมูลดิน ค้นหาตำแหน่ง (Locator Tools) ค้นหาจุดเก็บตัวอย่างดิน แผนที่ดินระดับตำบล แผนที่ความเหมาะสมในการเพาะปลูก รายงานการจัดการดิน รายงานค่าสมบัติทางเคมีของดิน รายงานสรุปขนาดพื้นที่แยกตามการใช้ประโยชน์ ข้อมูลสารสนเทศทรัพยากรดิน

๖) ระบบบริหารจัดการข้อมูลเกษตรใช้สารอินทรีย์ลดใช้สารเคมีทางการเกษตร/เกษตรอินทรีย์ เป็นระบบเพื่อนำเสนอข้อมูลในรูปแบบเชิงพื้นที่ของระบบภูมิสารสนเทศ ประกอบการวิเคราะห์แผนการปฏิบัติงานและประเมินผลการปฏิบัติงานด้านการพัฒนาที่ดิน การบริหารจัดการและส่งเสริมข้อมูลเกษตร ในการใช้สารอินทรีย์ลดใช้สารเคมีทางการเกษตร/เกษตรอินทรีย์ โดยแสดงให้เห็นถึงตำแหน่งที่ตั้ง ขนาด ของพื้นที่โครงการ/กิจกรรม หรือกลุ่มเกษตรในแผนการปฏิบัติงานต่างๆ รวมทั้งองค์ประกอบและปัจจัยอื่นๆ ในเชิงพื้นที่ ได้อย่างมีประสิทธิภาพและประสิทธิผล สำหรับการวางแผนและการตัดสินใจได้อย่างถูกต้องและรวดเร็ว พร้อมทั้งยังสามารถตอบสนองต่อเหตุการณ์ต่างๆ ได้อย่างทันท่วงที

๗) ระบบบริหารจัดการข้อมูลโรงงานผลิตปุ๋ยอินทรีย์ เป็นระบบเพื่อนำเสนอข้อมูลในรูปแบบเชิงพื้นที่ของระบบภูมิสารสนเทศ ประกอบด้วย ข้อมูลโรงงาน รายละเอียดกิจกรรมการผลิตและการตลาด แหล่งที่มางบประมาณ รายงานรายละเอียดเครื่องมือและอุปกรณ์ของโรงงานปุ๋ยอินทรีย์ รายงานแผนและผลการดำเนินงานขับเคลื่อนโรงปุ๋ยอินทรีย์ชุมชน ข้อมูลโรงปุ๋ยอินทรีย์ที่หยุดดำเนินการผลิต รายงานปริมาณการผลิตปุ๋ยอินทรีย์ในแต่ละปี และรายงานข้อมูลโรงปุ๋ยอินทรีย์ที่ผ่านการรับรองมาตรฐานปัจจัยการผลิตทางการเกษตร เป็นต้น

๑.๖ ระยะเวลาและสถานที่ดำเนินการ

ระยะเวลา : ระหว่างเดือน ตุลาคม ๒๕๕๕ - กันยายน ๒๕๕๖

สถานที่ดำเนินการ : ศูนย์สารสนเทศ กรมพัฒนาที่ดิน

๑.๗ ผู้ดำเนินการ

๑.๗.๑ นางจันทร์เพ็ญ ลาภจิตร

ตำแหน่ง นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ

มีหน้าที่ ศึกษา วิเคราะห์ จัดทำระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กรมพัฒนาที่ดิน ปฏิบัติงาน ๙๐%

๑.๗.๒ นางสาวอริศรา พึ่งพา

ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ

มีหน้าที่ รวบรวมข้อมูล ร่วมศึกษา วิเคราะห์ ปฏิบัติงาน ๑๐%

๑.๘ ประโยชน์ที่ได้รับ

๑.๘.๑ ผู้บริหารได้รับทราบผลสัมฤทธิ์การดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ และสามารถนำการควบคุม/กำกับดูแลและผลการประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ใช้เป็นข้อมูลประกอบในการตัดสินใจเพื่อวางแผนและพัฒนาการดำเนินงานของหน่วยงาน รวมทั้งการกำกับดูแลการปฏิบัติงาน ตลอดจนรายงานต่าง ๆ ที่จัดทำขึ้นมีความถูกต้อง เชื่อถือได้ และทันเวลาตามที่กำหนด

๑.๘.๒ ผู้ปฏิบัติงานมีการปรับปรุงกิจกรรมความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้อย่างเหมาะสม ทันเวลากับสถานการณ์ที่เปลี่ยนแปลงไป

๑.๘.๓ สามารถประหยัดเวลาและค่าใช้จ่ายในการกู้ข้อมูลและการติดตั้งระบบเว็บไซต์ให้บริการต่าง ๆ ที่เกิดปัญหาจากการถูกโจมตี หรือความเสียหายจากการสูญเสียข้อมูลสำคัญ

๑.๘.๔ เพื่อเพิ่มเสถียรภาพและความน่าเชื่อถือ ให้กับระบบเครือข่ายของกรมพัฒนาที่ดิน

๑.๙ คำนิยามศัพท์

๑.๙.๑ หน่วยงาน หรือ องค์กร หมายความว่า กรมพัฒนาที่ดิน

๑.๙.๒ ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑.๙.๓ ระบบเครือข่าย หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

๑.๙.๔ ความมั่นคงปลอดภัย หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๑.๙.๕ ระบบแลน (Local Area Network) และ ระบบอินทราเน็ต (Intranet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๑.๙.๖ ระบบอินเทอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

๑.๙.๗ ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

๑.๙.๘ เครื่องคอมพิวเตอร์ หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

๑.๙.๙ ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑.๙.๑๐ สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

๑.๙.๑๑ ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ กรมพัฒนาที่ดิน

๑.๙.๑๒ ผู้ใช้งาน หรือ **ผู้ใช้บริการ** หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสังกัดหน่วยงาน พนักงานราชการ และหมายรวมถึงบุคคลที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

๑.๙.๑๓ ผู้ดูแลระบบ (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบเครือข่ายและคอมพิวเตอร์ไม่ว่าส่วนหนึ่งส่วนใด

๑.๙.๑๔ สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๑.๙.๑๕ สถานที่หรือพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

๑.๙.๑๕.๑ พื้นที่ทำงาน หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูและระบบ (System Administrator)

๑.๙.๑๕.๒ พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

๑.๙.๑๕.๓ พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

๑.๙.๑๖ จดหมายอิเล็กทรอนิกส์ (e-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

๑.๙.๑๗ รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑.๙.๑๘ บัญชีผู้ใช้บริการ (Account) หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์และบริการในระบบเครือข่ายของหน่วยงาน

๑.๙.๑๙ การตั้งค่าระบบ (Configuration) หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

๑.๙.๒๐ เลขที่อยู่ไอพี (IP Address) หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

๑.๙.๒๑ เลขที่อยู่ไอพีสาธารณะ (Public IP Address) หมายความว่า เลขที่อยู่ ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

๑.๙.๒๒ แบนด์วิดท์ (Bandwidth) หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

๑.๙.๒๓ ชื่อผู้ใช้ (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

๑.๙.๒๔ ลงบันทึกเข้า (Login) หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้ระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

๑.๙.๒๕ ลงบันทึกออก (Logout) หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

๑.๙.๒๖ อัพเดท (Update) หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่าง ๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

๑.๙.๒๗ ไฟร์วอลล์ (Firewall) หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอกเพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๑.๙.๒๘ Web Server หมายความว่า เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่าง ๆ

๑.๙.๒๙ อุปกรณ์จัดเส้นทาง (Router) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๑.๙.๓๐ อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ – ส่งข้อมูล

๑.๙.๓๑ การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

๑.๙.๓๒ แผนผังระบบเครือข่าย (Network Diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

๑.๙.๓๓ Firewall Log หมายความว่า การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่า ไฟล์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

๑.๙.๓๔ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๑.๙.๓๕ ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

๑.๙.๓๖ เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๑.๙.๓๗ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๑.๙.๓๘ ทรัพย์สินสารสนเทศ หมายความว่า ข้อมูล ระบบข้อมูล บุคลากร ผู้ให้บริการภายนอก และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ หมายรวมถึงสิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

๑.๙.๓๙ บัญชีทรัพย์สินสารสนเทศ หมายถึง บันทึกซึ่งแสดงรายการต่างๆ ของทรัพย์สินสารสนเทศขององค์กร ประกอบไปด้วยข้อมูล เช่น เลขทะเบียนทรัพย์สินสารสนเทศ ชื่อเครื่องให้บริการ/รายการอุปกรณ์ ยี่ห้อ/รุ่น/Spec. ลักษณะการใช้งาน/ระบบงาน ที่ตั้ง จำนวน (เครื่อง) ผู้รับผิดชอบ ดูแลจัดการฮาร์ดแวร์ เป็นต้น

๑.๙.๔๐ ความเสี่ยง หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านกลยุทธ์ การปฏิบัติงาน การเงิน และการบริหาร โดยความเสี่ยงนี้จะถูกวัดด้วยผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์ ซึ่งเป็นความเสี่ยงตามความหมายทั่วไป

๑.๙.๔๑ ปัจจัยเสี่ยง หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด เกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

๑.๙.๔๒ ปัจจัยเสี่ยงภายนอก คือ สภาพแวดล้อมภายนอกหน่วยงาน ซึ่งเป็นสิ่งที่ไม่อยู่ในความรับผิดชอบของหน่วยงาน เช่น นโยบายภาครัฐ กฎหมาย หรือระเบียบข้อบังคับ

๑.๙.๔๓ ปัจจัยเสี่ยงภายใน คือ สภาพแวดล้อมภายในหน่วยงาน เช่น รูปแบบการบริหาร สั่งการ การมอบหมายอำนาจหน้าที่ความรับผิดชอบ โครงสร้างองค์กร ระเบียบ ข้อบังคับภายใน

๑.๙.๔๔ ผู้ประเมินความเสี่ยง หมายถึง ผู้เป็นเจ้าของหรือผู้รับผิดชอบทรัพย์สินสารสนเทศขององค์กร

๑.๙.๔๕ การประเมินความเสี่ยง เป็นกระบวนการที่ประกอบด้วย การวิเคราะห์ การประเมินและการจัดระดับความเสี่ยง โดยพิจารณาจากการประเมินโอกาสที่จะเกิดความเสี่ยง และความรุนแรงของผลกระทบจากเหตุการณ์ความเสี่ยง โดยอาศัยเกณฑ์มาตรฐานที่ได้กำหนดไว้ ทำให้การตัดสินใจจัดการกับความเสี่ยงเป็นไปอย่างเหมาะสม

๑.๙.๔๖ ภัยคุกคาม (Threat) หมายถึง ภายที่มีผลในทางลบ เช่น สร้างความเสียหายในลักษณะใดลักษณะหนึ่ง ต่อทรัพย์สินสารสนเทศและการดำเนินกิจกรรมขององค์กร เช่น ไวรัสซึ่งเป็นภัยชนิดหนึ่ง เมื่อภัยนี้เกิดขึ้นจริง จะทำให้การทำงานของระบบเกิดการหยุดชะงักได้

๑.๙.๔๗ ช่องโหว่ (Vulnerability) หมายความว่า สภาพหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์ และหากถูกใช้ให้เป็นประโยชน์โดยภัยคุกคามอาจทำให้ทรัพย์สินสารสนเทศขององค์กรได้รับความเสียหายได้

๑.๙.๔๘ ระดับของโอกาสที่จะเกิดความเสี่ยง หมายถึง ความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้นและมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร พิจารณาจากสถิติการเกิดความเสี่ยง ประวัติของการเกิดความเสี่ยงในอดีต ผลจากระดับการควบคุมในปัจจุบัน หรือการคาดการณ์ล่วงหน้าถึงความถี่ที่จะเกิดขึ้น ซึ่งสามารถกำหนดระดับของโอกาสที่จะเกิดความเสี่ยง โดยแบ่งออกเป็น ๕ ระดับ ได้แก่ สูงมาก (๕), สูง (๔), ปานกลาง (๓), น้อย (๒), และน้อยมาก (๑)

๑.๙.๔๙ ระดับความรุนแรงของผลกระทบของความเสี่ยง หมายถึง ผลจากเหตุการณ์ซึ่งอาจเกิดประการเดียวหรือหลายประการ โดยเกิดได้ทั้งเชิงบวกและเชิงลบ ซึ่งในที่นี้จะหมายถึงความเสียหายที่เกิดกับองค์กร โดยพิจารณาจากระดับความรุนแรง และมูลค่าความเสียหายที่มีต่อองค์กรในกรณีที่ความเสี่ยงนั้นเกิดขึ้น สามารถแบ่งระดับของผลกระทบออกเป็น ๕ ระดับ ได้แก่ สูงมาก (๕), สูง (๔), ปานกลาง (๓), น้อย (๒), และ น้อยมาก (๑)

๑.๙.๕๐ ระดับของความเสี่ยง หมายถึง ระดับของความเสี่ยงที่เกิดจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยง ที่ประเมินได้ตามตารางการวิเคราะห์ความเสี่ยง โดยจัดเรียงตามลำดับค่าจากระดับสูงมาก สูง ปานกลาง น้อย และเลือกความเสี่ยงที่มีระดับสูงมาก และหรือสูง มาจัดทำแผนการบริหารความเสี่ยงในขั้นตอนต่อไป

๑.๙.๕๑ นโยบายรักษาความมั่นคงปลอดภัยระบบสารสนเทศ หมายถึง ข้อกำหนดที่กรมพัฒนาที่ดิน จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามมาตรา ๗ ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๙

บทที่ ๒
แนวคิดและทฤษฎีที่เกี่ยวข้อง

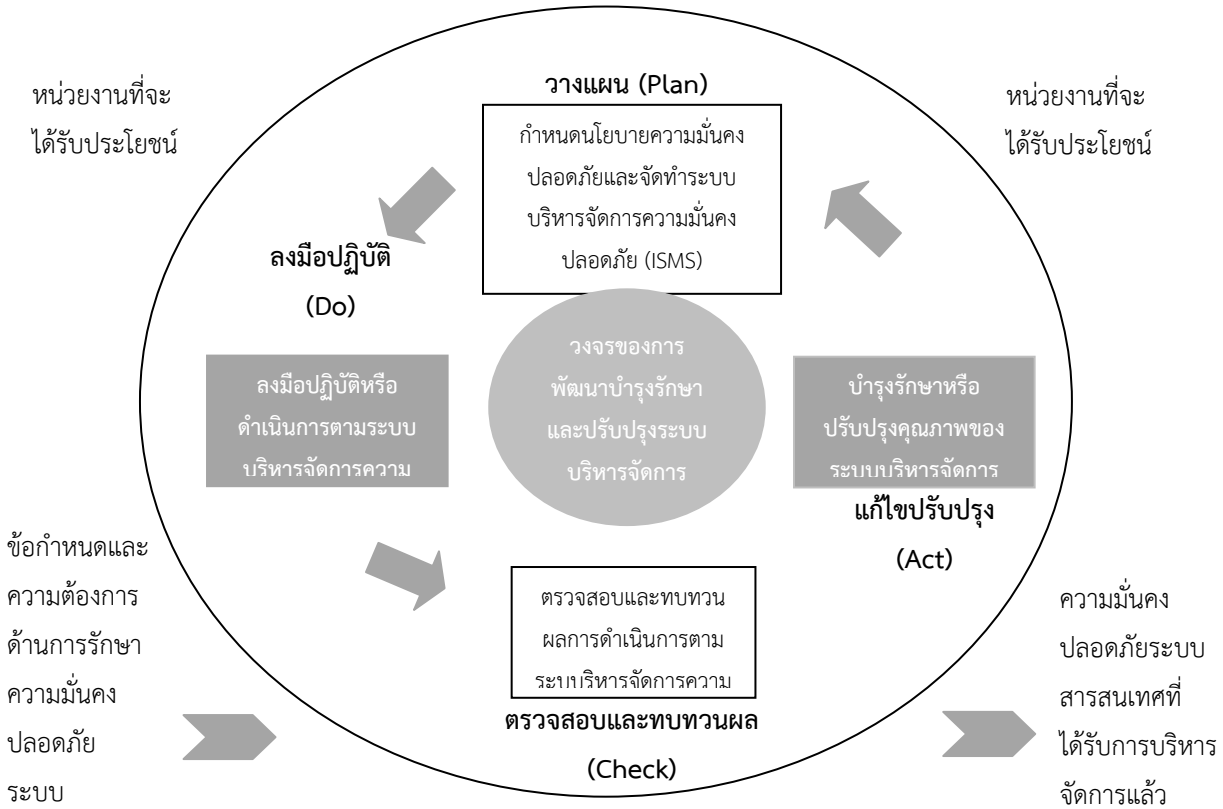
ในการพัฒนาระบบประเมินและวิเคราะห์ความเสี่ยงในการจัดการด้านระบบสารสนเทศ จำเป็นต้องมีความรู้และทฤษฎีพื้นฐานเพื่อที่จะได้นำมาพัฒนาระบบให้เป็นไปตามความต้องการและสามารถตอบสนองความต้องการของผู้ใช้ระบบ ในบทนี้ จะกล่าวถึง พื้นฐานความรู้ต่าง ๆ ที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมพัฒนาที่ดิน ประกอบด้วยหัวข้อต่าง ๆ ดังนี้

๒.๑ กระบวนการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัย สำหรับสารสนเทศ
๒.๒ องค์ประกอบพื้นฐานด้านความปลอดภัยของข้อมูล
๒.๓ การบริหารและประเมินความเสี่ยงของระบบคอมพิวเตอร์และระบบเครือข่าย

๒.๑ กระบวนการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัย สำหรับสารสนเทศ

๒.๑.๑ ข้อกำหนดทั่วไป

องค์กรจะต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุง รักษา และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษร ภายในกรอบกิจกรรมการดำเนินการทางธุรกิจต่าง ๆ รวมทั้งความเสี่ยงที่เกี่ยวข้อง แนวทางที่ใช้ในมาตรฐานฉบับนี้จะใช้กระบวนการ Plan-Do-Check-Act หรือ P-D-C-A มาประยุกต์ใช้ตามแสดงใน ภาพที่ ๒



ภาพที่ ๒ แผนภาพแสดงวงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act
ที่มา : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, ๒๕๕๐

๒.๑.๒ กำหนดและบริหารจัดการ ระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๑.๒.๑ กำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan) องค์กรจะต้องปฏิบัติ ดังนี้

๑) กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยโดยพิจารณาถึงลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี รวมทั้งอาจพิจารณาถึงสิ่งที่ไม่รวมอยู่ในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย

๒) กำหนดนโยบายและความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี นโยบายความมั่นคงปลอดภัยจะต้องมีองค์ประกอบดังนี้

๒.๑) กรอบในการดำเนินการ ทิศทางและหลักการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒.๒) ข้อกำหนดทางธุรกิจ ข้อกำหนดในสัญญาต่าง ๆ ระเบียบปฏิบัติ ข้อบังคับ รวมทั้งกฎหมายของประเทศ

๒.๓) การบริหารจัดการความเสี่ยงเชิงกลยุทธ์ในระดับองค์กร

๒.๔) เกณฑ์ในการประเมินความเสี่ยง

๒.๕) การได้รับการอนุมัติจากผู้บริหาร

๓) กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร

๓.๑) ระบุวิธีการประเมินความเสี่ยงที่เหมาะสมกับระบบบริหารจัดการทางด้านความมั่นคงปลอดภัยขององค์กร

๓.๒) กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระบุระดับความเสี่ยงที่ยอมรับได้

๔) ระบบความเสี่ยง

๔.๑) ระบุทรัพย์สินที่อยู่ในขอบเขตของระบบบริหารจัดการความปลอดภัยรวมทั้งผู้เป็นเจ้าของทรัพย์สินเหล่านั้น

๔.๒) ระบุภัยคุกตามที่มีต่อทรัพย์สินเหล่านั้น

๔.๓) ระบุจุดอ่อนที่ภัยคุกคามอาจจะใช้ให้เป็นประโยชน์

๔.๔) ระบุผลกระทบที่ก่อให้เกิดความสูญเสียทางด้านความลับ ความสมบูรณ์ ความพร้อมใช้ของทรัพย์สินเหล่านั้น

๕) การวิเคราะห์และประเมินความเสี่ยง

๕.๑) ประเมินผลกระทบที่มีต่อธุรกิจซึ่งอาจเป็นผลจากความล้มเหลว ในการรักษาความมั่นคงปลอดภัย โดยพิจารณาผลของการสูญเสียความลับ ความสมบูรณ์ ความพร้อมใช้ของทรัพย์สินเหล่านั้น

๕.๒) กำหนดความน่าจะเป็นของความเสี่ยงอันเกิดจากความล้มเหลวในการรักษาความมั่นคงปลอดภัย

๕.๓) กำหนดระดับความเสี่ยง

๕.๔) กำหนดว่าความเสี่ยงเหล่านั้น สามารถยอมรับได้หรือไม่ โดยใช้เกณฑ์ในการยอมรับความเสี่ยงที่กำหนดไว้

๖) ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้ อาจรวมถึง

๖.๑) ใช้มาตรการที่เหมาะสม

๖.๒) ยอมรับความเสี่ยงเหล่านั้น โดยมีเงื่อนไขว่า ความเสี่ยงเหล่านั้นจะต้องอยู่ภายในเกณฑ์ในการยอมรับความเสี่ยงที่กำหนดไว้

๖.๓) หลีกเลี่ยงความเสี่ยงเหล่านั้น

๖.๔) โอนย้ายความเสี่ยงเหล่านั้นไปสู่ผู้อื่น เช่น บริษัทประกันภัย เป็นต้น

๗) เลือกวัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัย เพื่อจัดการกับความเสี่ยง วัตถุประสงค์และมาตรการดังกล่าว สามารถเลือกมาจากมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์ในตอนท้ายของมาตรฐานฉบับนี้

๘) ขอการอนุมัติและความเห็นชอบสำหรับความเสี่ยงที่ยังหลงเหลืออยู่ในระบบบริหารจัดการความมั่นคงปลอดภัย

๙) ขอการอนุมัติเพื่อลงมือปฏิบัติและดำเนินการ

๑๐) จัดทำเอกสาร SoA (Statement of Applicability) แสดงการใช้งานมาตรการตามที่แสดงไว้ในส่วนของมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์ เอกสารดังกล่าวควรมีองค์ประกอบดังนี้

๑๐.๑) วัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยตามที่ได้เลือก รวมทั้งเหตุผลการใช้งาน

๑๐.๒) วัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยที่ได้ใช้งานอยู่ในปัจจุบัน

๑๐.๓) วัตถุประสงค์และมาตรการความมั่นคงปลอดภัยที่ไม่มีการใช้งาน รวมทั้งเหตุผลที่ไม่มีการใช้งาน

๒.๑.๒.๒ ลงมือปฏิบัติและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติดังนี้ (Do)

๑) จัดทำแผนการจัดการความเสี่ยงซึ่งกล่าวถึงการดำเนินการเชิงบริหารจัดการทรัพยากรที่จำเป็น หน้าที่ความรับผิดชอบ และลำดับการดำเนินการเพื่อบริหารจัดการความเสี่ยงที่พบ

๒) ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงเพื่อบรรลุในวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้

๓) ลงมือปฏิบัติตามมาตรการที่เลือก เพื่อบรรลุวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยของมาตรการดังกล่าว

๔) กำหนดวิธีการในการวัดความสัมฤทธิผลของมาตรการที่เลือกมาใช้งาน การวัดดังกล่าวจะต้องสามารถสร้างผลลัพธ์ที่สามารถเปรียบเทียบได้ รวมทั้งสร้างผลลัพธ์เดิมขึ้นมาอีกครั้งหนึ่งได้

๕) จัดทำและลงมือปฏิบัติตามแผนการอบรมและสร้างความตระหนัก

๖) บริหารการดำเนินงานสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย

๗) บริหารทรัพยากรสำหรับระบบบริหารจัดกาความมั่นคงปลอดภัย

๘) จัดทำและลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ ซึ่งช่วยในการตรวจจับและรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัย

๒.๑.๒.๓ เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติดังนี้ (Check)

๑) ตรวจจับข้อผิดพลาดจากการประมวลผล

๑.๑) ตรวจจับข้อผิดพลาดจากการประมวลผล

๑.๒) ระบุการละเมิดความมั่นคงปลอดภัยและเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

๑.๓) ช่วยให้ผู้บริหารสามารถระบุได้ว่ากิจกรรมทางด้านความมั่นคงปลอดภัยที่มอบหมายให้กับบุคลากรขององค์กรเป็นไปตามที่คาดหมายไว้หรือไม่

๑.๔) ตรวจสอบเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยโดยอาศัยตัวบ่งชี้ต่าง ๆ เพื่อช่วยในการตรวจจับเหตุการณ์ต่าง ๆ ที่ไม่คาดคิด

๑.๕) ตรวจสอบได้ว่าการดำเนินการเพื่อแก้ไขการละเมิดทางด้านความมั่นคงปลอดภัยมีความสัมฤทธิ์ผลหรือไม่

๒) ดำเนินการทบทวนความสัมฤทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยนำสิ่งต่าง ๆ ต่อไปนี้มาพิจารณาร่วมด้วย ได้แก่ ผลการตรวจสอบก่อนหน้านี้ เหตุการณ์ละเมิดความมั่นคงปลอดภัยที่เกิดขึ้น ผลการวัดความสัมฤทธิผล คำแนะนำและผลตอบกลับจากองค์กรหรือหน่วยงานที่เกี่ยวข้อง เป็นต้น

๓) วัดความสัมฤทธิผลของมาตรการทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบว่าเป็นไปตามข้อกำหนดทางด้านความมั่นคงปลอดภัย

๔) ทบทวนผลการประเมินความเสี่ยงตามกรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยงที่ยังเหลืออยู่ และระดับความเสี่ยงที่ยอมรับได้ โดยพิจารณาการเปลี่ยนแปลงของสิ่งต่อไปนี้ประกอบด้วย

๔.๑) องค์กร

๔.๒) เทคโนโลยี

๔.๓) วัตถุประสงค์และกระบวนการทางธุรกิจ

๔.๔) ภัยคุกตามที่ระบุไว้ก่อนหน้านี้ กับสภาพการเปลี่ยนแปลงปัจจุบัน

๔.๕) ความสัมฤทธิผลของมาตรการที่ได้ลงมือปฏิบัติไปแล้ว

๔.๖) เหตุการณ์ภายนอก ได้แก่ การเปลี่ยนแปลงที่มีต่อกฎ ระเบียบกฎหมาย ข้อกำหนดในสัญญาที่ทำไว้ หรือข้อกำหนดอื่น ๆ และการเปลี่ยนแปลงทางสังคม เป็นต้น

๕) ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยภายในองค์กรตามกรอบระยะเวลาที่ได้กำหนดไว้

๖) ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย โดยผู้บริหารอย่างสม่ำเสมอ

๗) ปรับปรุงแผนทางด้านความมั่นคงปลอดภัยโดยนำเผลของการเฝ้าระวังและทบทวนกิจกรรมต่าง ๆ มาพิจารณาร่วมด้วย

๘) บันทึกการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๑.๒.๔ บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติดังนี้ (Act)

๑) ปรับปรุงระบบบริหารจัดการความมั่งคงปลอดภัยตามที่ระบุไว้

๒) ใช้มาตรการเชิงแก้ไขและป้องกันและใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและขององค์กรอื่นมาช่วยในการปรับปรุงให้ดีขึ้น

๓) แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้อง โดยให้รายละเอียดที่เหมาะสมต่อสถานการณ์ที่เกิดขึ้น

๔) ตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

๒.๒ องค์ประกอบพื้นฐานด้านความปลอดภัยของข้อมูล

องค์ประกอบพื้นฐานความปลอดภัยของข้อมูลหลัก ๆ มีอยู่ ๓ อย่าง ซึ่งใช้ตัวย่อ CIA มาจากคำว่า Confidentiality Integrity Availability และยังมีองค์ประกอบอื่น ๆ เพิ่มเติม คือ Authentication Authorization และ Non-repudiation (หรืออาจเรียกรวมได้ว่า CIAAAN)

๒.๒.๑ Confidentiality (ความลับของข้อมูล)

การรักษาความลับของข้อมูล หมายถึง การปกป้องข้อมูลหมายถึง การปกป้องโดยมีเงื่อนไขว่าข้อมูลนั้นใครมีสิทธิ์ที่จะล่วงรู้ เข้าถึงใช้งานได้ และการทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น อาทิเช่น ข้อมูลอีเมล์ในเมล์บ็อกซ์ (Mail Box) ของผู้ใช้ผู้ที่มีสิทธิ์เข้าถึงเมล์บ็อกซ์และเปิดอ่านจดหมายได้จะต้องเป็นเจ้าของเมล์บ็อกซ์นั้นเพียงคนเดียวเท่านั้นที่สามารถเข้าถึงและเปิดอ่านจดหมายได้

๒.๒.๒ Integrity (ความคงสภาพของข้อมูล)

การรักษาความคงสภาพของข้อมูลหมายถึง การปกป้องเพื่อให้ข้อมูลไม่ถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย ถ้าเราสามารถรักษาสภาพของข้อมูลได้ จะทำให้ข้อมูลเหล่านั้นเกิดความน่าเชื่อถือ อาทิเช่น Bob ส่งไฟล์ถึง Alic ไฟล์นั้นจะต้องไม่ถูกแก้ไขหรือเปลี่ยนแปลงโดยบุคคลอื่นในระหว่างทางที่ส่งมา

การรักษาความคงสภาพของส่งข้อมูลนั้นสามารถทำได้หลายวิธี เช่น การ checksum ตัวอย่างเช่น การตรวจสอบไฟล์ที่ดาวน์โหลดมาจากเว็บไซต์ว่าตรงกับต้นฉบับหรือไม่ โดยเราสามารถทำได้โดยตรวจสอบค่า checksum โดยใช้ MD๕ เป็นต้น

๒.๒.๓ Availability (ความพร้อมใช้งานของข้อมูล)

ความพร้อมในการใช้งานของข้อมูล หมายถึง ข้อมูลจะต้องมีสภาพพร้อมใช้งานอยู่ตลอดเวลา อาทิเช่น เมล์เซิร์ฟเวอร์ถูกโจมตีจนไม่สามารถเข้าไปของรับบริการจากเมล์เซิร์ฟเวอร์นั้นได้ ต้องรอจนกว่าผู้ดูแลระบบจะแก้ไขเพื่อให้ระบบสามารถกลับมาให้บริการได้เหมือนเดิม แต่ถ้าหากระบบเมล์นี้ออกแบบให้มีระบบสำรอง (Mail Backup) ที่สามารถทำงานแทนเมล์เซิร์ฟเวอร์ตัวหลักได้ทันที ผู้ใช้ก็จะสามารถใช้บริการระบบสำรองนี้ได้ทันที

๒.๒.๔ Authentication (การพิสูจน์ทราบตัวตนที่แท้จริง)

เนื่องจากการระบุตัวบุคคลนั้นจะต้องใช้กระบวนการพิสูจน์ตัวจริงเพื่อให้ทราบว่าบุคคลผู้นั้นเป็นตัวจริงหรือไม่ อาทิเช่น การล็อกอนเข้าสู่ระบบลงทะเบียนวิชาของนักศึกษา สมาชิก (นักศึกษา) จะต้องใช้ยูสเซอร์เนม และพาสเวิร์ด เพื่อเป็นการพิสูจน์ทราบว่าเป็นผู้ใช้คนนั้นจริง ๆ และการพิสูจน์ทราบตัวตนก็มีอยู่หลากหลายวิธี อาทิเช่น

สิ่งที่คุณรู้ เช่น การใช้ยูสเซอร์เนม และพาสเวิร์ด
สิ่งที่คุณมี เช่น การใช้บัตรประจำตัว
สิ่งที่คุณเป็น เช่น การสแกนลายนิ้วมือ เสียงพูด

อาจมีการผสมผสานการใช้งานได้มากกว่าหนึ่งอย่างเพื่อให้การพิสูจน์ทราบตัวตนมีประสิทธิภาพมากขึ้น เช่น การกดเงินจากตู้ ATM ที่จะต้องใช้ “สิ่งที่คุณมี” คือ บัตร ATM และต้องใช้ “สิ่งที่คุณรู้” นั่นคือต้องทราบรหัสผ่าน หรือการใช้บริการโอนเงินผ่านอินเตอร์เน็ต เพื่อการโอนเงิน คุณจะต้องใช้ “สิ่งที่คุณรู้” คือ ยูสเซอร์เนม และพาสเวิร์ด เพื่อเข้าใช้งานเว็บไซต์ และต้องใช้ “สิ่งที่คุณมี” คือ โทรศัพท์มือถือ เพิ่มใช้รับ OPT (One Time Password) เพื่อนำมาใช้กรอกในเว็บไซต์เพื่อยืนยันการทำรายการ

๒.๒.๕ Authorization (การอนุญาตให้เข้าใช้งานและลำดับสิทธิในการเข้าถึง)

หลังจากได้มีการพิสูจน์ตัวตนแล้ว ระบบจะทำการอนุญาตให้ผู้ใช้คนนั้น ๆ เข้าใช้งานตามสิทธิของผู้ใช้งานคนนั้น ๆ ซึ่งการให้สิทธิ์สามารถแบ่งได้เป็นหลายระดับ อาทิเช่น ผู้ใช้ระดับสูง เช่น Administrator สามารถเปลี่ยนแปลง/แก้ไขข้อมูลได้ทั้งหมด ผู้ใช้งานที่เป็นสมาชิกไปอาจจะแก้ไขข้อมูลได้บางส่วน หรือ ผู้ใช้ระดับ Guest สามารถอ่านข้อมูลได้อย่างเดียว เป็นต้น

๒.๒.๖ Non-repudiation (การไม่สามารถปฏิเสธความรับผิดชอบ)

คือการปฏิเสธไม่ได้ถึงความรับผิดชอบ เช่น ปฏิเสธไม่ได้ว่าข้อความนี้ถูกส่งโดยผู้ใช้งานคนนี้ อาทิเช่น สมาชิกในเว็บบอร์ดที่มีการโพสต์ (Post) ข้อความว่าร้ายผู้อื่นลงไปในระบบเว็บบอร์ด จะต้องมีการบันทึกและแสดงชื่อผู้ใช้ซึ่งจะได้จากการพิสูจน์ตัวตน พร้อมกับข้อความที่โพสต์เพื่อใช้ยืนยันว่าข้อความดังกล่าวถูกโพสต์โดยผู้ใช้ผู้นั้นไม่สามารถปฏิเสธความรับผิดชอบได้

๒.๓ การบริหารและประเมินความเสี่ยงของระบบคอมพิวเตอร์และระบบเครือข่าย

ความเสี่ยง (Risk) หมายถึง ความเสี่ยงรูปแบบต่าง ๆ ที่อาจก่อให้เกิดผลเสียหายต่อข้อมูลสำคัญและระบบ/อุปกรณ์ต่าง ๆ ที่สนับสนุนการทำงานให้กับข้อมูลสำคัญนี้อยู่ โดยขั้นตอนนี้จะเป็นชั้นของการประเมินระดับความเสี่ยง (Risk Level) ที่มีทั้งหมดต่อข้อมูลและทรัพย์สินต่าง ๆ ขององค์กร เพื่อนำความเสี่ยงที่เกินระดับที่องค์กรสามารถยอมรับได้ไปดำเนินการควบคุมและแก้ไขความเสี่ยงในขั้นตอนต่อไป ระดับของความเสี่ยงนั้นจะพิจารณาจาก ๒ ปัจจัย คือ

๑) ความน่าจะเป็น (Probability) โดยปกติจะคำนวณค่าโดยพิจารณาจากการวิเคราะห์ภัยคุกคาม (Threat) ร่วมกับ จุดอ่อน (Vulnerability)

๒) ความรุนแรง (Severity) ความเสียหายที่อาจเกิดขึ้น ซึ่งโดยปกติจะคำนวณค่าโดยการพิจารณาจาก ระดับความสำคัญของข้อมูลหรือทรัพย์สินนั้น ๆ ที่มีต่อองค์กร

หลังจากที่ได้ประเมินความเสี่ยงเราจะต้องมีการบริหารจัดการความเสี่ยงที่มี เช่น การปิดช่องโหว่ หรือจุดอ่อน การติดตั้งระบบรักษาความปลอดภัย การฝึกอบรมพนักงานและเจ้าหน้าที่รักษาความปลอดภัยและการตรวจสอบเพื่อหาช่องโหว่ใหม่ๆ ที่อาจจะเกิดขึ้นการปิดช่องโหว่ของระบบเป็นการลดจำนวนจุดอ่อนให้เหลือน้อยที่สุดเท่าที่จะเป็นไปได้ เช่น หากมีจุดอ่อนอยู่ ๑๐ จุด การปิดช่องโหว่อาจจะทำให้จุดอ่อนถูกกำจัดออกไปจนเหลือจุดอ่อนเพียง ๒ – ๓ จุด เป็นต้น การปิดช่องโหว่ของระบบสารสนเทศและระบบเครือข่ายสามารถทำได้โดยใช้วิธีการที่หลากหลาย บางอย่างเป็นสิ่งที่จำเป็นต้องทำ และบางอยางเป็นเพียงทางเลือกต่อไปนี้ เป็นตัวอย่าของการปิดช่องโหว่ที่สำคัญ ๆ ของระบบ

การปิดช่องโหว่ของเครื่องแม่ข่าย ทำได้โดยปิดบริการ (พอร์ต) ที่ไม่จำเป็น ทำการอัพเดทแพตซ์ติดตั้งแอนตี้ไวรัส ป้องกันโดยใช้ไฟร์วอลล์และ ไอพีเอส/ไอพีเอส (IDS/IPS) ใช้รหัสที่ซับซ้อน ลบผู้ใช้ที่ไม่จำเป็นออกจากระบบตั้งค่าเบอร์มิชชั่น (permission) ของไฟล์ให้รัดกุมหมั่นตรวจสอบโปรแกรมที่แปลกปลอมอย่างสม่ำเสมอ ไม่รีโมตเข้ามายังเครื่องแม่ข่ายด้วยโปรโตคอลที่ไม่ได้เข้ารหัส และจำกัดไอพีแอดเดรสและบัญชีผู้ใช้ของผู้ที่จะรีโมตเข้ามายังเครื่องแม่ข่าย

การปิดช่องโหว่ของระบบแลน (LAN) ป้องกันการโจมตีด้วยแมนอินเอะมิสเติ้ล (Man in the middle : MITM) โดยใช้สวิตช์ที่สามารถตั้งค่าแม็กฟิลเดอร์ (MAC Filter) และไอพีฟิลเดอร์ (IP Filter) บนพอร์ตได้ หรือป้องกันโดยใช้ Static: ARP ควรมีการ Authentication ด้วยยูสเซอร์เนม และพาสเวิร์ด ก่อนอนุญาตให้เชื่อมต่อกับเน็ตเวิร์ด มีการป้องกัน Rogue DHCP และการปลอมไอพีแอดเดรสและแม็กแอดเดรส ติดตั้งแพตซ์ แอนตี้ไวรัสและไฟร์วอลล์

ปิดช่องโหว่ของไวเลสแลน (Wireless LAN) ควรมีการเข้ารหัสด้วยดับเบิ้ลยูพีเอ (WPA) เลือกใช้คีย์ที่มีความซับซอนและความยาว และควรมีการตรวจสอบสิทธิ์ก่อนใช้งานเครือข่ายโดยใช้แอ็กเซสพอยท์ ยูสเซอร์เนมและพาสเวิร์ด ควรติดตั้งเอ็กเซสพอยท์ไว้ในจุดที่ปลอดภัย

จัดการช่องโหว่ด้านนโยบายสำหรับผู้ใช้งาน ควรมีการบังคับใช้รหัสผ่านที่มีความซับซ้อนและมีความยาว เปลี่ยนรหัสผ่านใหม่ทุกเดือน ไม่ใช่รหัสผ่านเดียวกันกับทุกระบบ ไม่นำซอฟต์แวร์ที่มีความเสี่ยงมาใช้ในระบบเครือข่าย กำจัดเวลาในการเข้าออกที่ทำงาน และไม่เปิดเผยข้อมูลแก่ผู้ที่ไม่น่าไว้ใจ สำหรับผู้ดูแลระบบหรือทีมงานควรมาตรการควบคุมการเข้าออกห้องเซิร์ฟเวอร์ ปรับปรุงค่า/กฎไฟร์วอลล์ (Firewall Policy) ให้รัดกุม และควรมีระบบ Backup ข้อมูล

๒.๓.๑ การวิเคราะห์ความเสี่ยงและการประเมินความเสี่ยง

การประเมินความเสี่ยงโดยส่วนมากจะทำการประเมินและให้ค่าต่าง ๆ ในเชิงปริมาณ เนื่องจากผลกระทบต่าง ๆ ที่อาจจะเกิดขึ้นต่อข้อมูลและทรัพย์สินของทางองค์กรนั้น อาจจะก่อให้เกิดความเสียหายในด้านของตัวเงินที่สามารถวัดได้ในเชิงปริมาณ ส่วนการประเมินแบบคุณภาพ ดังนั้น การประเมินความเสี่ยงมีจุดประสงค์เพื่อคาดการณ์ว่ามีเหตุการณ์ความเสี่ยงใดบ้างที่เกี่ยวข้องกับทรัพย์สินสารสนเทศหนึ่ง และมีระดับความเสี่ยงมากน้อยเพียงใด โดยการประเมินเชิงปริมาณ ดังนี้

Risk Value = Likelihood (L) x Impact (I) x Assets Value (AV)

Likelihood คือ โอกาสที่จะเกิด
Impact คือ ผลกระทบ
Assets Value คือ มูลค่าทรัพย์สิน

๒.๓.๒ การประเมินค่าความเสี่ยง (Risk Evaluation)

เมื่อได้ความเสี่ยง โดยมีรายละเอียดและการประมาณความเสี่ยงแล้วจึงมาประเมินค่าความเสี่ยงโดยการเปรียบเทียบกับ ค่าที่ยอมรับความเสี่ยง (Acceptance Risk Value : ARL) คือ ค่าที่ผู้บริหารเป็นผู้กำหนดว่ายอมรับได้ในค่าที่เท่าไร จึงนำค่าที่สูงกว่าค่าที่กำหนดมาพิจารณาจัดทำแผนบริหารความเสี่ยงด้านสารสนเทศ ทั้งนี้ค่าที่ผู้บริหารกำหนดพิจารณาจากงบประมาณที่จะต้องใช้ในการปรับปรุง และเป็นสิ่งที่ผู้บริหารให้ความสำคัญ

๒.๓.๓ การควบคุมและแก้ไขความเสี่ยง (Risk Management)

ทางเลือกในการควบคุมและแก้ไขความเสี่ยงที่ได้แนะนำไว้ในมาตรฐาน ISO ๒๗๐๐๑ นั้นมีอยู่ ๔ ทางเลือก คือ

๒.๓.๓.๑ การลดความเสี่ยง (Risk Reduction) คือ การพิจารณาหาวิธีในการควบคุมและแก้ไขความเสี่ยงให้ลดลงมาอยู่ในระดับที่องค์กรสามารถยอมรับได้

๒.๓.๓.๒ การยอมรับความเสี่ยง (Risk Acceptance) คือ การที่องค์กรพิจารณาแล้วพบว่าการดำเนินการแก้ไขและควบคุมความเสี่ยงนั้นไม่เหมาะสม ไม่สามารถกระทำได้ในการปฏิบัติหรือไม่คุ้มค่า เช่น ค่าใช้จ่ายในการดำเนินการแก้ไขมีมูลค่า สูงกว่ามูลค่าของข้อมูล ทั้งนี้ขึ้นอยู่กับดุลยพินิจของผู้บริหาร

๒.๓.๓.๓ การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การหลีกเลี้ยงความเสี่ยงโดยยกเลิกกระบวนการทำงานหรือทรัพย์สินที่ก่อให้เกิดความเสี่ยงขึ้น ซึ่งมักจะกระทำเมื่อการแก้ไขความเสี่ยงด้วยวิธีการอื่นนั้น ไม่คุ้มกับผลประโยชน์ก็ได้ จากการทำงานด้วยกระบวนการหรือทรัพย์สินนั้น ๆ

๒.๓.๓.๔ การโอนความเสี่ยง (Risk Transfer) คือ การพิจารณาถ่ายโอนความเสี่ยงไปให้ผู้อื่นรับผิดชอบแทน เช่น การซื้อประกันภัย เป็นต้น

บทที่ ๓
การวิเคราะห์และประเมินความเสี่ยง

จากการศึกษาแนวคิด ทฤษฎีที่เกี่ยวข้องจากบทที่ ๒ จึงได้นำเอามาเป็นแนวทางในการดำเนินการวิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมพัฒนาที่ดิน โดยมีรายละเอียด ดังนี้

๓.๑ ขั้นตอนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กรมพัฒนาที่ดิน

๓.๒ การระบุความเสี่ยง (Risk Identification)

๓.๓ การวิเคราะห์และประเมินความเสี่ยงและการกำหนดแนวทางการตอบสนอง (Risk Assessment)

๓.๔ การกำหนดมาตรการ/กิจกรรมควบคุมความเสี่ยง (Risk Control/Treatment)

๓.๑ ขั้นตอนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กรมพัฒนาที่ดิน

กระบวนการบริหารจัดการความเสี่ยงเริ่มต้นจากการรวบรวมข้อมูลทรัพย์สินที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูลระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้น ๆ เพื่อตรียมการป้องกันและควบคุม เพื่อไม่ให้เกิดความสูญเสีย หรือผลกระทบต่อหน่วยงาน โดยแนวทางทางขั้นตอนการบริหารความสี่ยงตามแผนภูมิ ดังนี้

๑. การระบุความเสี่ยง (Risk Identification)	- วิเคราะห์ข้อมูลทรัพย์สินที่เกี่ยวข้อง กิจกรรม/ปัจจัยเสี่ยง ที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ ระบุประเด็นความเสี่ยง ภัยคุกคาม และช่องโหว่ที่อาจจะเกิดขึ้น
๒. การวิเคราะห์และประเมินความเสี่ยงและการกำหนดแนวทางการตอบสนอง (Risk Assessment)	- ประเมินโอกาสที่จะเกิดความรุนแรง ผลกระทบระดับความสำคัญของความเสี่ยงด้านต่างๆ รวมทั้งพิจารณามูลค่าทรัพย์สิน
๓. การกำหนดมาตรการ/กิจกรรมควบคุมความเสี่ยง (Risk Control/Treatment)	- กำหนดแนวทางการตอบสนอง (ยอมรับ , การลด/ควบคุม , การยกเลิก/หลีกเลี่ยง , การถ่ายโอนความเสี่ยง - ดำเนินการกำหนดมาตรการหรือกิจกรรมควบคุมความเสี่ยงที่เกิดขึ้นในแต่ละประเด็น
๔. แผนปฏิบัติการการบริหารความเสี่ยง (Risk Implementation)	- กำหนดแผนงาน/โครงการดำเนินการจัดทำแผนปฏิบัติการบริหารความเสี่ยง
๕. การติดตามและประเมินผลการบริหารจัดการความเสี่ยง (Monitoring & Review)	- ดำเนินการตามแผนปฏิบัติการบริหารความเสี่ยงติดตามตรวจสอบว่ามีการดำเนินการตามแผน - วิเคราะห์ความเสี่ยงคงเหลือ - ย้อนกลับสู่วงจรบริหารความเสี่ยง
๖. สรุปและรายงาน (Report & Summary)	- วิเคราะห์ความเปลี่ยนแปลงและประโยชน์ที่ได้รับจากการบริหารความเสี่ยง สรุปผลการดำเนินงาน

ภาพที่ ๓ แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง

๓.๒ การระบุความเสี่ยง(Risk Identification)

ในการระบุความเสี่ยง ศูนย์สารสนเทศ ได้จัดทำบัญชีรายการทรัพย์สิน (Asset Inventory) ที่มีอยู่ โดยพิจารณาว่าแต่ละเทคโนโลยีมีความเสี่ยงใดบ้างที่อาจเกิดขึ้น เมื่อจัดทำรายการทรัพย์สินแล้วเสร็จ กลุ่มบุคคลที่เกี่ยวข้องของงานจะต้องระบุความเสี่ยง (ภัยคุกคาม/การโจมตี/ช่องโหว่) ที่อาจเกิดขึ้นกับทรัพย์สินแต่ละชนิด พร้อมทั้งประเมินความเสียหายที่เกิดจากความเสี่ยง จึงจะสามารถระบุมาตรการควบคุมความเสี่ยงได้

๓.๒.๑ การจัดทำบัญชีรายการทรัพย์สิน การจัดทำบัญชีรายการทรัพย์สิน มีขั้นตอนต่าง ๆ ดังนี้

๓.๒.๑.๑ ระบุทรัพย์สินประเภทต่าง ๆ ของกรมพัฒนาที่ดิน ได้แก่ บุคลากร (People), ขั้นตอนการทำงาน (Procedure), ข้อมูล (Data), ซอฟต์แวร์ (Software), ฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย (Networking) ทรัพย์สินเหล่านี้ สามารถนำมาแตกย่อยเป็นทรัพย์สินทางด้านการจัดการความเสี่ยงได้ ดังตารางต่อไปนี้

๑) การระบุทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware) อุปกรณ์และเครือข่าย (Network) ได้จัดทำรายการทรัพย์สินซึ่งประกอบด้วยหัวข้อรายละเอียดดังนี้ เลขทะเบียนทรัพย์สินสารสนเทศ ชื่อเครื่องให้บริการ/รายการอุปกรณ์ ยี่ห้อ/รุ่น/Spec. Reference ID ลักษณะการใช้งาน/ระบบงาน ที่ตั้ง จำนวน (เครื่อง) และผู้รับผิดชอบ ดูแลจัดการฮาร์ดแวร์

๒) การระบุทรัพย์สินประเภท ซอฟต์แวร์ (Software) ได้จัดทำรายการทรัพย์สินซึ่งประกอบด้วยหัวข้อรายละเอียดดังนี้ เลขทะเบียนทรัพย์สินสารสนเทศ ชื่อซอฟต์แวร์ เวอร์ชั่น ผู้พัฒนาซอฟต์แวร์ จำนวนลิขสิทธิ์ รายละเอียดซอฟต์แวร์ ผู้รับผิดชอบดูแลจัดการซอฟต์แวร์

๓) รายการทรัพย์สินประเภท ข้อมูล (Information) ได้จัดทำรายการทรัพย์สินซึ่งประกอบด้วยหัวข้อรายละเอียดดังนี้ เลขทะเบียนทรัพย์สินสารสนเทศ ชื่อเอกสารข้อมูล/เอกสารสนเทศ ขนาดข้อมูล(Size) Database(ที่ใช้) รูปแบบที่ให้บริการ ระดับชั้นข้อมูล สื่อบันทึกข้อมูลที่ใช้ในการเก็บ ที่เก็บสารสนเทศ(ชื่อสถานที่) ระยะเวลาการจัดเก็บ ผู้เป็นเจ้าของสารสนเทศ

๔) รายการทรัพย์สินประเภท คน (People ware) ภายในองค์กร ได้จัดทำรายการทรัพย์สินซึ่งประกอบด้วยหัวข้อรายละเอียดดังนี้ รหัสพนักงาน ชื่อ – นามสกุล ตำแหน่ง ส่วนงาน/ฝ่ายงาน หน้าที่ความรับผิดชอบ เบอร์โทรศัพท์ติดต่อ อีเมล์

๕) รายการทรัพย์สินประเภท บริการ (Stakeholders) ได้จัดทำรายการทรัพย์สินซึ่งประกอบด้วยหัวข้อรายละเอียดดังนี้ เลขทะเบียนทรัพย์สินสารสนเทศ ชื่อบริการ รายละเอียดบริการ เจ้าของบริการ ข้อมูลติดต่อผู้ใช้บริการ SLA

๓.๒.๑.๒ จัดหมวดหมู่ทรัพย์สิน หมวดหมู่ของทรัพย์สินที่ใช้ในการจัดการความเสี่ยงที่แตกต่างกัน ซึ่งจะสะท้อนให้ทราบถึงระดับความอ่อนไหว (Sensitivity) และระดับความต้องการความมั่นคงปลอดภัย (Security Priority) ของทรัพย์สินแต่ละประเภท ประกอบด้วย

๑) ชั้นความลับ (Confidential)
๒) ใช้ภายใน (Internal)
๓) สาธารณะ (Public)

๓.๒.๒ กลุ่มบุคคลที่เกี่ยวข้อง กลุ่มบุคคลสำคัญที่เกี่ยวข้องกับการจัดการความเสี่ยง มี ๓ กลุ่ม ดังนี้

๓.๒.๒.๑ **กลุ่มความมั่นคงปลอดภัยของสารสนเทศ (Information Security)** ประกอบด้วย บุคลากรของศูนย์สารสนเทศ ได้แก่ กลุ่มวิเคราะห์และวางระบบข้อมูล กลุ่มระบบเครือข่ายและคอมพิวเตอร์ กลุ่มฐานข้อมูลสารสนเทศ กลุ่มระบบภูมิสารสนเทศ เป็นผู้ที่มีความเข้าใจในภัยคุกคามและการโจมตีแต่ละชนิด ดังนั้น จึงเป็นกลุ่มที่สามารถเป็นผู้นำในการระบุถึงภัยคุกคามที่จัดว่าเป็นความเสี่ยงได้

๓.๒.๒.๒ **กลุ่มเทคโนโลยีสารสนเทศ (Information Technology)** บุคลากรของกลุ่มระบบเครือข่ายและคอมพิวเตอร์ เป็นกลุ่มที่ช่วยสร้างและดำเนินการระบบรักษาความมั่นคงปลอดภัยได้

๓.๒.๒.๓ **กลุ่มผู้บริหารและผู้ใช้ (Management and Users)** เป็นกลุ่มบุคลากรที่ต้องใช้งานสารสนเทศและระบบในทุก ๆ วัน กลุ่มนี้จะเป็นกลุ่มแรกที่ตรวจพบความเสี่ยง ดังนั้น การกำหนดกลไกป้องกันความเสี่ยงด้านสารสนเทศที่ดีให้กับระบบ ส่งผลให้บุคลากรกลุ่มผู้บริหารและผู้ใช้ (Management and Users) สามารถใช้งานได้สารสนเทศได้อย่างมีประสิทธิภาพ

กลุ่มบุคลากรข้างต้น จะต้องทำงานร่วมกันเพื่อระบุความเสี่ยงที่อาจเกิดขึ้นทุกระดับ โดยเรียงลำดับจากความเสี่ยงที่ก่อให้เกิดความเสียหายมากที่สุดไปจนถึงน้อยที่สุด

๓.๒.๓ การระบุภัยคุกคามและช่องโหว่ เป็นการหาจุดอ่อนหรือช่องโหว่ของทรัพย์สินทางเทคโนโลยีสารสนเทศแต่ละชนิด โดยตั้งสมมติฐานว่าทรัพย์สินจะต้องถูกคุกคามจากการโจมตี จะทำให้ขอบเขตการจัดการความเสี่ยงกว้างมากเกินไป และการทำงานซับซ้อนขึ้น วิธีการหนึ่งที่จะช่วยลดขอบเขตของงานจัดการความเสี่ยงลงได้ คือ การเริ่มจากระบุภัยคุกคามจากนั้น ระบุช่องโหว่ แล้วนำมาประเมินผลอีกครั้ง

๓.๒.๓.๑ การระบุภัยคุกคาม (Threat Identification) แสดงภัยคุกคามที่อาจเกิดขึ้นกับทรัพย์สินตามทรัพย์สินทางเทคโนโลยีสารสนเทศ

๓.๒.๓.๒ การระบุช่องโหว่ (Vulnerability Identification) พิจารณาหาช่องโหว่ที่อาจเป็นเหตุให้ถูกโจมตีจากภัยคุกคามตามทรัพย์สินทางเทคโนโลยีสารสนเทศ ดังตารางต่อไปนี้

ตารางที่ ๒ การระบุช่องโหว่ของภัยคุกคามตามทรัพย์สินทางเทคโนโลยีสารสนเทศ

ทรัพย์สินทางเทคโนโลยีสารสนเทศ	ภัยคุกคาม	ช่องโหว่ที่อาจเกิดขึ้น
๑. สถานที่ (Premises)	ไฟฟ้าดับ	ไม่มีการแยกเดินสายไฟฟ้าสำรอง เพื่อรองรับกรณี สายไฟฟ้าหลักมีปัญหา
	ไฟฟ้าลัดวงจร	ไม่มีการตรวจเช็คสายไฟฟ้าอย่างสม่ำเสมอ
		ไม่มีการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบNetwork
		ไม่มีการตรวจสอบความสมบูรณ์ของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network

ทรัพย์สินทางเทคโนโลยีสารสนเทศ	ภัยคุกคาม	ช่องโหว่ที่อาจเกิดขึ้น
	ไฟไหม้	ไม่มีการทดสอบการฉีดก๊าซจากถังดับเพลิงจริง - ถังดับเพลิงชนิดผงเคมีแห้ง (Class A และ B) - ถังดับเพลิงชนิดก๊าซคาร์บอนได้ออกไซด์หรือ CO2 (Class B และ C)
		ไม่มีถังดับเพลิงชนิด HCFC-๑๒๓ (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารโดยเฉพาะ
	น้ำท่วม แผ่นดินไหว	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ
	การชุมนุม จลาจล	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ
๒. เครื่องแม่ข่าย อุปกรณ์ ซอฟต์แวร์ ระบบ และการเชื่อมโยงเครือข่าย (Technology)	ระบบเครือข่ายสื่อสารภายนอก (Internet) เสียหาย/ขัดข้อง	ไม่มีระบบสายสื่อสารสำรองเพื่อรองรับการเชื่อมต่อไปยังผู้ให้บริการเครือข่าย (ISP) หากสายสื่อสารหลักมีปัญหาระบบจะไม่สามารถให้บริการได้
		ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด
		มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายเฉพาะอุปกรณ์ Firewall และ Router เท่านั้น
		ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There’s no Redundant)
		ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ

ทรัพย์สินทางเทคโนโลยีสารสนเทศ	ภัยคุกคาม	ช่องโหว่ที่อาจเกิดขึ้น
	ระบบเครือข่ายสื่อสารภายในกรมพัฒนาที่ดินเสียหาย/ขัดข้อง	ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด
		ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There’s no Redundant)
		ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ
	อุปกรณ์ Hardware ภายในห้องควบคุมระบบNetwork ระบบชำรุด	ขาดแผนในการบริหารจัดการอุปกรณ์ Hardwareภายในห้องควบคุมระบบ Network
		ไม่มีอุปกรณ์สำรอง
	Domain Controller ไม่สามารถให้บริการได้	Resource ไม่เพียงพอ
	ข้อมูล User Profile หาย User ไม่สามารถ Login ได้	ไม่มีเครื่อง Backup Domain Controller ที่ใช้สำรองระบบ
	การโจมตีเครื่องแม่ข่ายเพื่อไม่ให้สามารถใช้การได้ หรือทำให้ประสิทธิภาพลดลง (Denial of Service)	กระบวนการป้องกัน Denial of Service ไม่รองรับการโจมตีในรูปแบบที่ไม่ได้มีการกำหนดไว้
		ขาดกระบวนการป้องกัน Denial of Service
	การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย
		ไม่มีกระบวนการในการติดตามปรับปรุง Software Version ให้ทันสมัย
	การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต	ขาดการติดตามเรื่องการถอดถอนสิทธิของเจ้าหน้าที่ที่ลาออก หรือย้ายแผนกอย่างสม่ำเสมอ

ทรัพย์สินทางเทคโนโลยีสารสนเทศ	ภัยคุกคาม	ช่องโหว่ที่อาจเกิดขึ้น
		ไม่มีมาตรฐานการกำหนดระดับสิทธิ์การเข้าใช้งานของระบบเครือข่าย
		ไม่มีกระบวนการบริหารจัดการสิทธิ์ที่ดีสำหรับผู้ให้บริการภายนอก เช่น ขาดกระบวนการตรวจสอบสิทธิ์ที่ชัดเจน ขาดการกำหนดระยะเวลาการยกเลิกสิทธิ์
	การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย
	ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย	ขาดการตรวจสอบประสิทธิภาพการทำงานของอุปกรณ์บันทึกข้อมูล
		ไม่มีกระบวนการเฝ้าระวังและตรวจสอบ Capacity ของระบบ
		ไม่มีการจัดเก็บหรือป้องกันแผ่นโปรแกรมที่เหมาะสม
	ซอฟต์แวร์ทำงานผิดพลาด	ไม่มีกระบวนการตรวจสอบระบบหรือซอฟต์แวร์ก่อนนำมาใช้งานจริง
		ขาดกระบวนการในการตรวจสอบสถานะการทำงานของระบบ
		ขาดกระบวนการในการปรับปรุงฐานข้อมูลของซอฟต์แวร์ให้ทันสมัย
	เครื่องลูกข่ายโดน Virus โจมตี	เครื่องลูกข่ายไม่ได้ติดตั้งป้องกัน Virus แบบ Client Server ที่สามารถบริหารจัดการจากศูนย์กลางได้
๓. ข้อมูล (Information)	ข้อมูลสูญหาย	ทำการสำรองข้อมูลทุกวันจัดเก็บอยู่ในระบบ NAS ไม่ได้นำออกมาเก็บไว้ที่อื่นอย่างปลอดภัย
		มีการจัดเก็บข้อมูลรายเดือนเป็น Tap Backup สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก
		ไม่ได้ปรับปรุงแผนการสำรองข้อมูลให้เป็นปัจจุบันอย่าง จึงทำให้ฐานข้อมูล/ระบบฯ ที่พัฒนาขึ้นใหม่ อยู่นอกแผนไม่ได้ทำการสำรอง

ทรัพย์สินทางเทคโนโลยีสารสนเทศ	ภัยคุกคาม	ช่องโหว่ที่อาจเกิดขึ้น
	ข้อมูล mailbox สูญหาย	ระบบ Mail Service ชำรุด
๔. ระบบสนับสนุน (Supplies)	กล้อง CCTV เสีย	ไม่มีการตรวจสอบการทำงานของ CCTV Console
	เครื่องปรับอากาศล้มเหลว	ระบบปรับอากาศ (Air-Conditioner) ไม่รับการตรวจสอบความพร้อมใช้
	เครื่องสำรองไฟฟ้า (UPS) ไม่สามารถสำรองไฟได้	ไม่มีการตรวจสอบประสิทธิภาพการทำงานของ Battery อย่างสม่ำเสมอ
	การแอบ/ลักลอบเข้าสู่ห้องควบคุมระบบNetwork หรือ ไม่มีการควบคุมการเข้าออกห้องควบคุมระบบ Network (Finger Scan)	ขาดการทบทวนหรือยกเลิกสิทธิผู้ที่ไม่เกี่ยวข้องในการเข้าถึงห้องควบคุมระบบ Network
๕. ผู้รับบริการ (Stakeholders)	เครือข่ายหลักล่มไม่สามารถใช้งาน Internet ได้ ทำให้การให้บริการล้มเหลว	ไม่มีระบบสื่อสาร Internet พร้อมวงจรเชื่อมโยงสำรอง
	อุปกรณ์สำรองไม่สามารถใช้งานได้	ไม่มีการตรวจสอบอุปกรณ์สำรองที่จะนำมาใช้ทดแทนระบบหลักของผู้ให้บริการภายนอก
๖. บุคลากร (People)	เจ้าหน้าที่ Network Admin หลักไม่สามารถปฏิบัติได้	เจ้าหน้าที่ Network Admin สำรองมีทักษะไม่เท่ากับ Network Admin หลัก
	เจ้าหน้าที่ Programmerไม่สามารถปฏิบัติได้	ไม่มีเจ้าหน้าที่ Programmer สำรอง

๓.๓ การวิเคราะห์และประเมินความเสี่ยงและการกำหนดแนวทางการตอบสนอง (Risk Assessment)

เพื่อพิจารณาความเสี่ยงที่มีอยู่ก่อนการควบคุมใดๆ (Inherent Risk) และทำการประเมินระดับนัยสำคัญของโอกาสเกิดความเสี่ยงหรือความรุนแรงของผลกระทบจากความเสี่ยงที่คาดว่าจะมีขึ้น โดยการประเมินค่าความเสี่ยง (Risk Value) จะมีการวิเคราะห์และประเมินใน ๓ มิติ ดังนี้

ค่าความเสี่ยง (Risk Value)

- **ความเป็นไปได้ที่จะเกิดความเสี่ยง (Likelihood : L)**
  เหตุการณ์มีโอกาสที่จะเกิดความเสี่ยง
  กำหนดเป็นเกณฑ์ ๕ ระดับ
- **ผลกระทบ (Impact : I)**
  หากมีความเสี่ยงเกิดขึ้นแล้ว องค์กรจะได้รับผลกระทบรุนแรงเพียงใด
  กำหนดเป็นเกณฑ์ ๕ ระดับ
- **มูลค่าของทรัพย์สิน (Asset Value : AV)**
  ค่าคะแนนความสำคัญของทรัพย์สิน โดยพิจารณาจากมูลค่าความเสียหาย
  กำหนดเป็นเกณฑ์ ๔ ระดับ

๓.๓.๑ ขั้นตอนการประเมิน

๓.๓.๑.๑ การประเมินโอกาสที่จะเกิดความเสี่ยง การพิจารณาถึงความเป็นไปได้ของโอกาส (Likelihood) ที่ความเสี่ยงจะเกิดขึ้นได้บ่อยครั้งเพียงใด โดยใช้ตารางการคิดค่าคะแนนของโอกาสที่จะเกิดความเสี่ยงประกอบการพิจารณา ดังนี้

ตารางที่ ๓ การประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood Criteria)

ค่าคะแนน	คำอธิบาย โอกาสที่จะเกิด	ความเป็นไปได้ที่จะเกิดความเสี่ยง
๑	ยากมาก	โอกาสที่จะเกิดเหตุการณ์ดังกล่าว น่าจะไม่เกิดขึ้นภายใน ๒ ปี
๒	ไม่น่าจะเป็นไปได้	โอกาสที่จะเกิดเหตุการณ์ดังกล่าว น่าจะไม่เกิดขึ้นภายใน ๑ ปี
๓	น่าจะเป็นไปได้	โอกาสที่จะเกิดเหตุการณ์ดังกล่าว ระหว่าง ๖-๑๒ เดือนต่อครั้ง
๔	เป็นไปได้	โอกาสที่จะเกิดเหตุการณ์ดังกล่าว ระหว่าง ๑-๖ เดือนต่อครั้ง
๕	เกือบจะแน่นอน	โอกาสที่จะเกิดเหตุการณ์ดังกล่าว มากกว่า ๑ ครั้งต่อเดือน

๓.๓.๑.๒ การประเมินผลกระทบที่จะเกิดความเสี่ยง การพิจารณาถึงความเป็นไปได้ผลกระทบ (Impact) หากความเสี่ยงนั้นเกิดขึ้น ความเสียหายมีความรุนแรง ปานกลาง หรือเสียหายมาก โดยใช้ตารางการคิดค่าคะแนนของผลกระทบที่จะเกิดความเสี่ยงประกอบการพิจารณา ดังนี้

๑) ผลกระทบและความเสียหายที่เกิดขึ้นต่อองค์กร
พิจารณาจากปัจจัยภายนอกองค์กรที่ทำให้ระบบไม่สามารถปฏิบัติงานได้
ย่อมาจาก External Impact Criteria : EI

๒) ผลกระทบและความเสียหายที่เกิดขึ้นต่อการปฏิบัติงาน
พิจารณาจากการที่บุคลากรไม่สามารถปฏิบัติงานได้
ย่อมาจาก Personnel Impact Criteria : PI

๓) ผลกระทบอันเนื่องจาก การละเมิดกฎหมาย / สัญญาการให้บริการซึ่งอาจทำให้เกิดการดำเนินคดทางกฎหมาย หรือการฟ้องร้องทางแพ่ง
ย่อมาจาก Law Impact Criteria : LI

๔) ผลกระทบและความเสียหายที่เกิดขึ้นต่อระบบงาน
พิจารณาจากระบบการทำงานภายในองค์กรที่ไม่สามารถปฏิบัติงานได้
ย่อมาจาก Operational Impact Criteria : OI

ตารางที่ ๔ ผลกระทบที่จะเกิดความเสี่ยง (Impact Criteria)

ค่าคะแนน	คำอธิบาย	ผลกระทบและความเสียหายที่เกิดขึ้นต่อองค์กร (EI)	ผลกระทบและความเสียหายที่เกิดขึ้นต่อการปฏิบัติงาน (PI)
๑	น้อยมาก	จำนวนประชาชนที่ได้รับผลกระทบน้อยกว่า ๑๐% ของจำนวนลูกค้าทั้งหมด	คนสามารถปฏิบัติงานได้ แต่ประสิทธิภาพในการทำงานลดลงน้อยว่า ๑๐%
๒	น้อย	จำนวนประชาชนที่ได้รับผลกระทบระหว่าง ๑๐ - ๓๐% ของจำนวนลูกค้าทั้งหมด	คนสามารถปฏิบัติงานได้ แต่ประสิทธิภาพในการทำงานลดลงมากกว่า ๑๐%
๓	ปานกลาง	จำนวนประชาชนที่ได้รับผลกระทบระหว่าง ๓๑ -๕๐% ของจำนวนลูกค้าทั้งหมด	คนสามารถปฏิบัติงานได้ แต่ประสิทธิภาพในการทำงานลดลงมากกว่า ๓๐%
๔	มาก	จำนวนประชาชนที่ได้รับผลกระทบระหว่าง ๕๑ - ๘๐% ของจำนวนลูกค้าทั้งหมด	คนสามารถปฏิบัติงานได้ แต่ประสิทธิภาพในการทำงานลดลงมากกว่า ๕๐%
๕	มากที่สุด	จำนวนประชาชนที่ได้รับผลกระทบระหว่าง ๘๑ - ๑๐๐% ของจำนวนลูกค้าทั้งหมด	คนไม่สามารถปฏิบัติงานได้อย่างสิ้นเชิง

ตารางที่ ๔ ผลกระทบที่จะเกิดความเสี่ยง (Impact Criteria) (ต่อ)

ค่าคะแนน	คำอธิบาย	ผลกระทบอันเนื่องจากการละเมิดกฎหมาย / สัญญาการให้บริการซึ่งอาจทำให้เกิดการดำเนินคดีทางกฎหมาย หรือการฟ้องร้องทางแพ่ง (LI)	ผลกระทบและความเสียหายที่เกิดขึ้นต่อระบบงาน (OI)
๑	น้อยมาก	ไม่มีผลกระทบหากมีการละเมิดกฎหมาย หรือการไม่ปฏิบัติตามสัญญาการให้บริการ (Service Level Agreement)	ผู้ใช้บริการสามารถเรียกใช้บริการได้เป็นปกติ
๒	น้อย	หากการดำเนินการไม่เป็นไปตามข้อกฎหมายหรือสัญญาการให้บริการ (Service Level Agreement) อาจมีผลกระทบต่อองค์กรเล็กน้อย	ผู้ใช้บริการสามารถเรียกใช้บริการได้เป็นปกติ แต่มี Error แจ้งเตือนบางอย่าง ซึ่งไม่ส่งผลกับการบริการ
๓	ปานกลาง	หากการดำเนินการไม่เป็นไปตามข้อกฎหมายหรือสัญญาการให้บริการ (Service Level Agreement) องค์กรอาจถูกปรับตามที่ระบุไว้ในกฎหมายหรือสัญญา	ผู้ใช้บริการไม่สามารถเรียกใช้บริการได้ชั่วคราวเนื่องจากปัญหาบางอย่าง แต่สามารถแก้ไขให้กลับมาใช้บริการได้ภายใน ๖ ชม.
๔	มาก	หากการดำเนินการไม่เป็นไปตามข้อกฎหมายหรือสัญญาการให้บริการ (Service Level Agreement) อาจถูกฟ้องดำเนินคดีทางแพ่ง	ผู้ใช้บริการ ไม่สามารถเรียกใช้บริการได้ แต่สามารถแก้ไขให้กลับมาใช้บริการได้ภายใน ๒๔ ชม.
๕	มากที่สุด	หากการดำเนินการไม่เป็นไปตามข้อกฎหมายหรือสัญญาการให้บริการ (Service Level Agreement) อาจถูกฟ้องดำเนินคดีทางแพ่งและอาญา	ผู้ใช้บริการ ไม่สามารถเรียกใช้บริการได้อย่างสิ้นเชิง

๓.๓.๑.๓ การประเมินมูลค่าของทรัพย์สิน การพิจารณาถึงมูลค่าความเสียหายที่จะเกิดขึ้นกับทรัพย์สิน โดยกำหนดเป็นเกณฑ์ ๔ ระดับ ตามตารางการคิดค่าคะแนนของ Asset Value Criteria ดังนี้

ตารางที่ ๕ การประเมินมูลค่าของทรัพย์สิน (Asset Value Criteria)

ระดับ	คน (People)	สถานที่ (Premises)	อุปกรณ์ (Technology)	ข้อมูล (Information)	ระบบสนับสนุน (Supplies)	ผู้รับบริการ Stakeholders
๔	มีความสำคัญขาดไม่ได้	สถานที่นี้มีความสำคัญต่อองค์กรมากที่สุด	อุปกรณ์มีความสำคัญต่อกระบวนการทำงานมากที่สุด	ขาดหายไม่ได้	ระบบสนับสนุนที่มีความสำคัญต่อกระบวนการทำงานมากที่สุด	ผู้มีส่วนเกี่ยวข้องที่มีความสำคัญต่อองค์กรมากที่สุด
๓	มีความสำคัญต้องใช้เวลาในการหาบุคลากรทดแทน	สถานที่นี้มีความสำคัญต่อองค์กรมาก	อุปกรณ์มีความสำคัญต่อกระบวนการทำงานมาก	ขาดหายได้บางส่วนไม่เกิน ๑๐ เปอร์เซ็นต์	ระบบสนับสนุนที่มีความสำคัญต่อกระบวนการทำงานมาก	ผู้มีส่วนเกี่ยวข้องที่มีความสำคัญต่อองค์กรมาก
๒	สามารถปฏิบัติงานได้แต่ต้องใช้เวลาในการศึกษางาน	สถานที่นี้มีความสำคัญต่อองค์กรปานกลาง	อุปกรณ์มีความสำคัญต่อกระบวนการทำงานปานกลาง	ขาดหายได้บางส่วนไม่เกิน ๕๐ เปอร์เซ็นต์	ระบบสนับสนุนที่มีความสำคัญต่อกระบวนการทำงานปานกลาง	ผู้มีส่วนเกี่ยวข้องที่มีความสำคัญต่อองค์กรปานกลาง
๑	สามารถดำเนินงานต่อไปได้	สถานที่นี้มีความสำคัญต่อองค์กรน้อย	อุปกรณ์มีความสำคัญต่อกระบวนการทำงานน้อย	ขาดหายได้บางส่วนไม่เกิน ๘๐ เปอร์เซ็นต์	ระบบสนับสนุนที่มีความสำคัญต่อกระบวนการทำงานน้อย	ผู้มีส่วนเกี่ยวข้องที่มีความสำคัญต่อองค์กรน้อย

๓.๓.๒ การประเมินค่าระดับของความเสี่ยง เมื่อทราบถึงปัจจัยประเมินความเสียงแล้ว **สามารถประเมินค่าความเสี่ยง (Risk Value : R)** ได้จากสูตรต่อไปนี้

$$R = L * I * AV$$

โดย R คือ ค่าความเสี่ยงที่ประเมินได้ ย่อมาจาก Risk Value
L คือ Likelihood ความเป็นไปได้ที่จะเกิดความเสี่ยง
I คือ Impact ผลกระทบ
AV คือ Asset Value คะแนนความสำคัญของทรัพย์สิน (มูลค่าของทรัพย์สิน)

๓.๓.๓ ค่าระดับความเสี่ยงที่ยอมรับได้ (Acceptance Risk Value : ARL) หมายถึง ประเภทและเกณฑ์ของความเสี่ยง ที่ผู้บริหารศูนย์สารสนเทศ กรมพัฒนาที่ดิน จะยอมรับได้ เพื่อช่วยให้องค์กรบรรลุเป้าหมาย ซึ่งความเสี่ยงที่ยอมรับได้จะกำหนดเป็นค่าเดียว ขึ้นอยู่กับความเหมาะสม ทั้งนี้ ค่าที่ผู้บริหารศูนย์สารสนเทศ กรมพัฒนาที่ดิน เป็นผู้กำหนดว่า **ยอมรับค่าความเสี่ยงได้ที่ระดับ = ๑๕** โดยพิจารณาจากงบประมาณที่ได้รับเพื่อใช้ในการปรับปรุง/จัดหาเพิ่มเติมซึ่งเป็นสิ่งที่ผู้บริหารให้ความสำคัญ

ตารางที่ ๖ การประเมินความเสี่ยง (Risk Assessment)

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๑.	ห้องควบคุมระบบ Network (ชั้น ๑ อาคารตึก ๖ ชั้น กรมพัฒนาที่ดิน จตุจักร กรุงเทพฯ)	ไฟฟ้าดับ	- ไม่มีการแยกเดินสายไฟฟ้าสำรอง เพื่อรองรับกรณีสายไฟฟ้าหลักมีปัญหา	๓	EI ๕	๔	๖๐	**รับไม่ได้**
		ไฟฟ้าลัดวงจร	- ไม่มีการตรวจเช็คสายไฟฟ้าอย่างสม่ำเสมอ	๑	EI ๕	๔	๒๐	**รับไม่ได้**
			- ไม่มีการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network	๑	EI ๕	๔	๒๐	**รับไม่ได้**
			- ไม่มีการตรวจสอบความสมบูรณ์ของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network	๑	EI ๕	๔	๒๐	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
		ไฟไหม้	ไม่มีการทดสอบการฉีดก๊าซจากถังดับเพลิงจริง - ถังดับเพลิงชนิดผงเคมีแห้ง (Class A และ B) - ถังดับเพลิงชนิดก๊าซคาร์บอนได้ออกไซด์หรือ CO๒ (Class B และ C)	๑	EI ๕	๔	๒๐	**รับไม่ได้**
			ไม่มีถังดับเพลิงชนิด HCFC-๑๒๓ (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารโดยเฉพาะ	๑	EI ๕	๔	๒๐	**รับไม่ได้**
		น้ำท่วม แผ่นดินไหว	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ	๑	EI ๕	๔	๒๐	**รับไม่ได้**
		การชุมนุม จลาจล	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ	๑	EI ๕	๔	๒๐	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๒.	รายการทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย (Network) ในส่วนของ - อุปกรณ์ ATM - อุปกรณ์ Core Switch - อุปกรณ์ Gateway Router (ภาคผนวก หน้า ๑๓๙-๑๔๐)	ระบบเครือข่ายสื่อสารภายนอก (Internet) เสียหาย/ขัดข้อง	ไม่มีระบบสื่อสารสำรองเพื่อเชื่อมต่อไปยังผู้ให้บริการเครือข่าย (ISP) รายอื่น หากระบบสื่อสารหลักมีปัญหา จะไม่สามารถให้บริการได้	๓	OI ๔	๔	๔๘	**รับไม่ได้**
			ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด	๓	OI ๔	๔	๔๘	**รับไม่ได้**
			มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่าย เฉพาะอุปกรณ์ Firewall และ Router เท่านั้น	๒	OI ๔	๔	๓๒	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
			ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There's no Redundant)	๒	OI ๔	๔	๓๒	**รับไม่ได้**
			ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	๒	OI ๔	๔	๓๒	**รับไม่ได้**
		ระบบเครือข่ายสื่อสารภายในกรมพัฒนาที่ดินเสียหาย/ขัดข้อง	ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด	๓	OI ๔	๔	๔๘	**รับไม่ได้**
			ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There's no Redundant)	๒	OI ๔	๔	๓๒	**รับไม่ได้**
			ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	๒	OI ๔	๔	๓๒	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๓.	รายการทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย (Network) ในส่วนของ - เครื่องที่ให้บริการ Web Server - เครื่องที่ให้บริการ GIS Server - เครื่องที่ให้บริการ e-Service Server - เครื่องที่ให้บริการ Mail Server - เครื่องที่ให้บริการ e-Office Server - เครื่อง Storage Server - เครื่อง Domain Server - เครื่อง Log Server - เครื่อง Net service Server - อุปกรณ์ Access Switch - อุปกรณ์ Access Point - อุปกรณ์ Firewall - (ภาคผนวก หน้า ๑๓๑-๑๓๙)	อุปกรณ์ Hardware ภายในห้องควบคุมระบบ ชำรุด	ขาดแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ	๒	OI ๔	๓	๒๔	**รับไม่ได้**
			ไม่มีอุปกรณ์สำรอง	๓	OI ๔	๓	๒๔	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๔.	รายการทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย (Network) ในส่วนของ - เครื่อง Domain Server (ภาคผนวก หน้า ๑๓๘)	Domain Controller ไม่สามารถให้บริการได้	Resource ไม่เพียงพอ	๒	OI ๔	๓	๒๔	**รับไม่ได้**
		ข้อมูล User Profile หาย User ไม่สามารถ Login ได้	ไม่มีเครื่อง Backup Domain Controller ที่ใช้สำรองระบบ	๑	OI ๔	๓	๑๒	**รับได้**
๕.	รายการทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย (Network) ในส่วนของ - เครื่องที่ให้บริการ Web Server - เครื่องที่ให้บริการ GIS Server - เครื่องที่ให้บริการ e-Service Server - เครื่องที่ให้บริการ Mail Server - เครื่องที่ให้บริการ e-Office Server - เครื่อง Storage Server - เครื่อง Domain Server - เครื่อง Log Server - เครื่อง Net service Server (ภาคผนวก หน้า ๑๓๑-๑๓๙)	ถูกโจมตีจนไม่สามารถให้บริการได้ (Denial of Service)	กระบวนการป้องกัน Denial of Service ไม่รองรับการโจมตีในรูปแบบที่ไม่ได้มีการกำหนดไว้	๓	OI ๓	๓	๒๗	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๖.	รายการทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย (Network) ในส่วนของ - เครื่องที่ให้บริการ Web Server - เครื่องที่ให้บริการ GIS Serverเครื่องที่ให้บริการ e-Service Server - เครื่องที่ให้บริการ Mail Server - เครื่องที่ให้บริการ e-Office Server - เครื่อง Storage Server - เครื่อง Domain Server - เครื่อง Log Server - เครื่อง Net Service Server (ภาคผนวก หน้า ๑๓๑-๑๓๙)	การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย	๒	OI ๔	๓	๒๔	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๗.	รายการทรัพย์สินประเภท ซอฟต์แวร์ (Software) ในส่วนของ - ซอฟต์แวร์ระบบปฏิบัติการ - ซอฟต์แวร์สำเร็จรูป (ภาคผนวก หน้า ๑๔๒-๑๔๓)	การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	ไม่มีกระบวนการในการติดตามปรับปรุง Software Version ให้ทันสมัย	๓	OI ๔	๒	๒๔	**รับไม่ได้**
๘.	รายการทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย (Network) ในส่วนของ - เครื่อง Domain Server (ภาคผนวก หน้า ๑๓๘)	การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต (Network)	ขาดการติดตามเรื่องการถอดถอนสิทธิของพนักงานที่ลาออก หรือย้ายแผนกอย่างสม่ำเสมอ	๓	OI ๓	๒	๑๘	**รับไม่ได้**
			ไม่มีมาตรฐานการกำหนดระดับสิทธิ์การเข้าใช้งานของระบบเครือข่าย	๑	OI ๓	๒	๖	**รับได้**
			ไม่มีกระบวนการบริหารจัดการสิทธิ์ที่ดี สำหรับผู้ให้บริการภายนอก เช่น ขาดกระบวนการตรวจสอบสิทธิ์ที่ชัดเจน ขาดการกำหนดระยะเวลาการยกเลิกสิทธิ์	๑	OI ๓	๒	๖	**รับได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๙.	รายการทรัพย์สินประเภท ซอฟต์แวร์ (Software) ในส่วนของ - ซอฟต์แวร์ระบบปฏิบัติการ - ซอฟต์แวร์สำเร็จรูป - ซอฟต์แวร์ประยุกต์ (ด้าน GIS e-Service และ e-Office) (ภาคผนวก หน้า ๑๔๒-๑๔๘)	การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย	๒	OI ๔	๒	๑๖	**รับไม่ได้**
๑๐.	รายการทรัพย์สินประเภท ซอฟต์แวร์ (Software) ในส่วนของ - ซอฟต์แวร์ระบบปฏิบัติการ - ซอฟต์แวร์สำเร็จรูป - ซอฟต์แวร์ประยุกต์ (ด้าน GIS e-Service และ e-Office) (ภาคผนวก หน้า ๑๔๒-๑๔๘)	ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย	ขาดการตรวจสอบประสิทธิภาพการทำงานของอุปกรณ์บันทึกข้อมูล	๒	OI ๓	๒	๑๒	**รับได้**
			ไม่มีกระบวนการเฝ้าระวังและตรวจสอบ Capacity ของระบบ	๒	OI ๓	๒	๑๒	**รับได้**
			ไม่มีการจัดเก็บหรือป้องกันแผ่นโปรแกรมที่เหมาะสม	๒	OI ๓	๒	๑๒	**รับได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๑๑.	รายการทรัพย์สินประเภท ซอฟต์แวร์ (Software) ในส่วนของ - ซอฟต์แวร์ระบบปฏิบัติการ - ซอฟต์แวร์สำเร็จรูป - ซอฟต์แวร์ประยุกต์ (ด้าน GIS e-Service และ e-Office) (ภาคผนวก หน้า ๑๔๒-๑๔๘)	ซอฟต์แวร์ทำงานผิดพลาด	ไม่มีกระบวนการตรวจสอบระบบหรือซอฟต์แวร์ก่อนนำมาใช้งานจริง	๒	OI ๓	๒	๑๒	**รับได้**
			ขาดกระบวนการในการตรวจสอบสถานะการทำงานของระบบ	๒	OI ๓	๒	๑๒	**รับได้**
			ขาดกระบวนการในการปรับปรุงฐานข้อมูลของซอฟต์แวร์ให้ทันสมัย	๒	OI ๓	๒	๑๒	**รับได้**
๑๒.	รายการทรัพย์สินประเภท ซอฟต์แวร์ (Software) ในส่วนของ - ซอฟต์แวร์สำเร็จรูป (ภาคผนวก หน้า ๑๔๒-๑๔๓)	เครื่องลูกข่ายโดน Virus โจมตี	เครื่องลูกข่ายไม่ได้ติดตั้งป้องกัน Virus แบบ Client Server ที่สามารถบริหารจัดการจากศูนย์กลางได้	๒	OI ๓	๒	๑๒	**รับได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๑๓.	รายการทรัพย์สินประเภท ข้อมูล ในส่วนของ - ข้อมูลเว็บไซต์หน่วยงานต่างๆ ภายในกรมพัฒนาที่ดิน - ข้อมูลด้าน GIS - ข้อมูลบริการประชาชน - ข้อมูล Intranet (ภาคผนวก หน้า ๑๔๙-๑๕๓)	ข้อมูลสูญหาย	ทำการสำรองข้อมูลทุกวันจัดเก็บอยู่ในระบบ NAS ไม่ได้นำออกมาเก็บไว้ที่อื่นอย่างปลอดภัย	๒	EI ๔	๓	๒๔	**รับไม่ได้**
			มีการจัดเก็บข้อมูลรายเดือนเป็น Tap Backup สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก	๒	EI ๔	๓	๒๔	**รับไม่ได้**
			มีการจัดเก็บข้อมูลรายไตรมาสเป็น External Hard disk สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก	๒	EI ๔	๓	๒๔	**รับไม่ได้**
			ไม่ได้ปรับปรุงแผนการสำรองข้อมูลให้เป็นปัจจุบันอย่าง จึงทำให้ฐานข้อมูล/ระบบฯ ที่พัฒนาขึ้นใหม่ อยู่นอกแผนไม่ได้ทำการสำรอง	๒	EI ๔	๓	๒๔	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๑๔.	รายการทรัพย์สินประเภท ข้อมูล ในส่วนของ - ข้อมูล Mailbox (ภาคผนวก หน้า ๑๕๒)	ข้อมูล mailbox สูญหาย	ระบบ Mail Service ชำรุด	๒	OI ๓	๓	๑๘	**รับไม่ได้**
๑๕.	รายการทรัพย์สินประเภท Supplies (ระบบสนับสนุน) - กล้อง CCTV (ภาคผนวก หน้า ๑๔๑)	กล้อง CCTV เสีย	ไม่มีการตรวจสอบการทำงานของ CCTV Console	๑	OI ๑	๑	๑	**รับได้**
๑๖.	รายการทรัพย์สินประเภท Supplies (ระบบสนับสนุน) - เครื่องปรับอากาศ (ภาคผนวก หน้า ๑๔๑)	เครื่องปรับอากาศล้มเหลว	ระบบปรับอากาศ (Air-Conditioner) ไม่รับการตรวจสอบความพร้อมใช้	๓	OI ๔	๓	๓๖	**รับไม่ได้**
๑๗.	รายการทรัพย์สินประเภท Supplies (ระบบสนับสนุน) - เครื่องสำรองไฟฟ้า (UPS) (ภาคผนวก หน้า ๑๔๑)	เครื่องสำรองไฟฟ้า (UPS) ไม่สามารถสำรองไฟได้	ไม่มีการเปลี่ยน Battery และวัสดุสิ้นเปลือง ตามระยะเวลาที่เหมาะสม	๓	OI ๓	๒	๑๘	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๑๘.	รายการทรัพย์สินประเภท Supplies (ระบบสนับสนุน) - Finger Scan (ภาคผนวก หน้า ๑๔๑)	การแอบ/ลักลอบเข้าสู่ห้องควบคุมระบบ Network หรือ ไม่มีการควบคุมการเข้าออกห้องควบคุมระบบ Network	ขาดการทบทวนหรือยกเลิกสิทธิผู้ที่ไม่เกี่ยวข้องในการเข้าถึงห้องควบคุมระบบNetwork	๑	OI ๒	๑	๒	**รับได้**
๑๙.	รายการทรัพย์สินประเภท บริการ (Stakeholders) - บริษัท กสท. โทรคมนาคม จำกัด (มหาชน) (ภาคผนวก หน้า ๑๕๘)	เครือข่ายหลักล่มไม่สามารถใช้งาน Internet ได้ ทำให้การให้บริการล้มเหลว	ไม่มีระบบสื่อสาร Internet พร้อมวงจรเชื่อมโยงสำรอง	๓	EI ๔	๔	๔๘	**รับไม่ได้**
๒๐.	รายการทรัพย์สินประเภท บริการ (Stakeholders) - บริษัท ดิ เอ็กซ์เพิร์ท ไอซีที จำกัด (ภาคผนวก หน้า ๑๕๘)	อุปกรณ์สำรองไม่สามารถใช้งานได้	ไม่มีการตรวจสอบอุปกรณ์สำรองที่จะนำมาใช้ทดแทนระบบหลักของผู้ให้บริการภายนอก	๓	OI ๔	๓	๓๖	**รับไม่ได้**
๒๑.	รายการทรัพย์สินประเภท คน - กลุ่มระบบเครือข่ายและคอมพิวเตอร์ (ภาคผนวก หน้า ๑๕๕)	เจ้าหน้าที่ Network Admin หลักไม่สามารถปฏิบัติได้	เจ้าหน้าที่ Network Admin สำรองมีทักษะไม่เท่ากับ Network Admin หลัก	๓	PI ๔	๓	๓๖	**รับไม่ได้**

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๒๒.	รายการทรัพย์สินประเภท คน - กลุ่มฐานข้อมูลสารสนเทศ (ภาคผนวก หน้า ๑๕๖)	เจ้าหน้าที่ Programmerไม่สามารถปฏิบัติได้	ไม่มีเจ้าหน้าที่ Programmer สำรอง	๓	PI ๕	๓	๔๕	**รับไม่ได้**

๓.๔ กำหนดมาตรการ/กิจกรรมควบคุมความเสี่ยง (Risk Control/Treatment)

หลังจากที่ได้ดำเนินการประเมินความเสี่ยงเรียบร้อยแล้ว ก็จะเข้าสู่ขั้นตอนสำคัญอีกขั้นตอนหนึ่งของการจัดการความเสี่ยงนั่นคือ “การควบคุมความเสี่ยง (Risk Control)” เป็นกระบวนการปรับใช้มาตรการและกลไกการควบคุมต่าง ๆ เพื่อลดความเสี่ยงต่อระบบสารสนเทศและข้อมูลขององค์กรขั้นตอนการดำเนินการดังนี้

๓.๔.๑ การกำหนดวิธีการบริหารความเสี่ยงหรือแนวทางเลือกการบริหารความเสี่ยง

วิธีการบริหารความเสี่ยงสามารถสรุปได้เป็น ๔ วิธีการหลัก ดังนี้

๓.๔.๑.๑ การยกเลิกหรือหลีกเลี่ยง (Terminate, Avoid) คือ ความเสี่ยงที่ไม่สามารถยอมรับและต้องจัดการให้ความเสี่ยงนั้นไปอยู่นอกเงื่อนไขการดำเนินงาน โดยมีวิธีการจัดการความเสี่ยงในกลุ่มนี้ เช่นการหยุดดำเนินงานหรือกิจกรรมที่ก่อให้เกิดความเสี่ยงนั้น การเปลี่ยนแปลงวัตถุประสงค์ในการดำเนินงาน การลดขนาดของงานที่จะดำเนินการหรือกิจกรรมลง เป็นต้น

๓.๔.๑.๒ การควบคุม (Treat, Reduce) คือความเสี่ยงที่ยอมรับได้แต่ต้องมีการแก้ไขเกี่ยวกับการควบคุมที่มีอยู่ในปัจจุบันเพื่อให้มีการควบคุมที่เพียงพอและเหมาะสม เช่น การปรับปรุงกระบวนการดำเนินงานการจัดอบรมเพิ่มทักษะในการทำงานให้กับพนักงานและการจัดทำคู่มือการปฏิบัติงาน เป็นต้น

๓.๔.๑.๓ การยอมรับ (Take, Accept) หมายถึง การที่ความเสี่ยงนั้นสามารถยอมรับได้ภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งไม่ต้องดำเนินการใด ๆ เช่น กรณีที่มีความเสี่ยงในระดับไม่รุนแรงและไม่คุ้มค่าที่จะดำเนินการใด ๆ ให้ขออนุมัติหลักการรับความเสี่ยงไว้และไม่ดำเนินการใด ๆ

๓.๔.๑.๔ การโอนความเสี่ยง (Transfer) หรือ แบ่ง (Share) คือ ความเสี่ยงที่สามารถโอนไปให้ผู้อื่นได้ เช่น การทำประกันภัย/ประกันทรัพย์สินกับบริษัทประกัน การจ้างบุคคลภายนอกหรือการจ้างบริษัทภายนอกมาจัดการในงานบางอย่างแทน เช่น งานรักษาความปลอดภัย เป็นต้น

๓.๔.๒ การประเมินโอกาสและผลกระทบเพื่อกำหนดกิจกรรมควบคุมความเสี่ยง

เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงต่าง ๆ และประเมินระดับความรุนแรงหรือมูลค่าความเสียหาย จากความเสี่ยง เพื่อให้เห็นถึงระดับของความเสี่ยงที่แตกต่างกัน ทำให้สามารถกำหนดการควบคุมความเสี่ยงได้อย่างเหมาะสม ซึ่งจะช่วยให้หน่วยงานสามารถวางแผนและจัดสรรทรัพยากรได้อย่างถูกต้องภายใต้งบประมาณ กำลังคน หรือเวลาที่มีจำกัด โดยอาศัยเกณฑ์มาตรฐานที่กำหนดไว้ โดยผู้ประเมินของหน่วยงานต้องเป็นผู้มีความรู้ ความชำนาญ และมีประสบการณ์ในเรื่องนั้นๆ

ดังนั้น ศูนย์สารสนเทศ จะเลือกกลยุทธ์ควบคุมความเสี่ยงแต่ละรายการ โดยพิจารณาจาก Risk Value เปรียบเทียบกับ **ระดับความเสี่ยงที่ยอมรับได้ (Acceptance Risk Value : ARL)** ที่ผู้อำนวยการศูนย์สารสนเทศเป็นผู้กำหนด หากค่า Risk Value น้อยกว่าค่า ARL ความเสี่ยงนั้นก็ไม่ต้องดำเนินการ

ตารางที่ ๗ การกำหนดมาตรการ/กิจกรรมควบคุมความเสี่ยง

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
๑.	ห้องควบคุมระบบ Network (ชั้น ๑ อาคารตึก ๖ ชั้น กรมพัฒนาที่ดิน จตุจักร กรุงเทพฯ)	ไฟฟ้าดับ	ไม่มีการแยกเดินสายไฟฟ้าสำรอง เพื่อรองรับกรณี สายไฟฟ้าหลักมีปัญหา	๓	EI ๕	๔	๖๐	**รับไม่ได้**	**Accept ยอมรับ**	- ยอมรับความเสี่ยงที่เกิดขึ้น เนื่องจากไม่สามารถแยกเดินสายไฟฟ้าสำรอง เพื่อรองรับกรณี สายไฟฟ้าหลักมีปัญหา
		ไฟฟ้าลัดวงจร	ไม่มีการตรวจเช็คสายไฟฟ้าอย่างสม่ำเสมอ	๑	EI ๕	๔	๒๐	**รับไม่ได้**	**Transfer โอนถ่าย**	- ขอความอนุเคราะห์ให้สำนักวิศวกรรมศาสตร์เพื่อการพัฒนาที่ดิน เข้าตรวจเช็คสายไฟฟ้าอย่างสม่ำเสมอ พร้อมทั้งจัดทำเป็นแผนการดำเนินการตรวจเช็คสายไฟฟ้าภายในห้องควบคุมระบบ Network

๔๙

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
			ไม่มีการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network	๑	EI ๕	๔	๒๐	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำเป็นข้อกำหนดภายใต้ “นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมพัฒนาที่ดิน”ว่าก่อนนำอุปกรณ์เข้าห้องควบคุมระบบ จะต้องทำการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ เพื่อป้องกันไฟฟ้าลัดวงจร - กำหนดเจ้าหน้าที่รับผิดชอบในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออกจากห้องควบคุมระบบ Network
			ไม่มีการตรวจสอบความสมบูรณ์ของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network	๑	EI ๕	๔	๒๐	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- กำหนดเจ้าหน้าที่รับผิดชอบในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออกจากห้องควบคุมระบบ Network

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
		ไฟไหม้	ไม่มีการทดสอบการฉีดก๊าซจากถังดับเพลิงจริง - ถังดับเพลิงชนิดผงเคมีแห้ง (Class A และ B) - ถังดับเพลิงชนิดก๊าซคาร์บอนได้ออกไซด์หรือ CO2 (Class B และ C)	๑	EI ๕	๔	๒๐	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- ซักซ้อมและทดสอบการฉีดก๊าซจากถังดับเพลิงจริง ปีละ ๒ ครั้ง (ตามแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร IT Contingency Plan)
			ไม่มีถังดับเพลิงชนิด HCFC-123 (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารโดยเฉพาะ	๑	EI ๕	๔	๒๐	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดหาถังดับเพลิงชนิด HCFC-123 (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารโดยเฉพาะ
		น้ำท่วม แผ่นดินไหว	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ	๑	EI ๕	๔	๒๐	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดเตรียมสถานที่สำรองภายนอกกรมพัฒนาที่ดิน ให้พร้อมรองรับอุปกรณ์และระบบเครือข่าย - ซักซ้อมความพร้อมของเจ้าหน้าที่ในการดำเนินงานตามแผนกรณีเกิดน้ำท่วม แผ่นดินไหว จลาจล ให้

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
										สามารถปฏิบัติได้ตามแผนที่กำหนดไว้ ประกอบด้วย o ปิดระบบเครือข่ายทั้งหมด o แผนเตรียมการและขนย้ายเครื่องแม่ข่าย โดยจัดเตรียมสถานที่เก็บเครื่องแม่ข่าย จัดทำบัญชีรายชื่อเครื่องแม่ข่ายและอุปกรณ์เครือข่าย และติดตั้งระบบ o แผนการติดตั้งระบบฯ ให้กลับมาใช้เป็นปกติ - ตรวจสอบบัญชีเครื่องแม่ข่ายและอุปกรณ์เครือข่ายที่ต้องทำการขนย้ายเรียงตามลำดับความสำคัญ - ตรวจสอบความพร้อมใช้ของสถานที่ ระบบไฟฟ้า และระบบเครือข่ายสำรอง ให้อยู่ในสภาพพร้อมใช้งาน

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
		การชุมนุม จลาจล	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ	๑	EI ๕	๔	๒๐	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดเตรียมสถานที่สำรองภายนอกกรมพัฒนาที่ดิน ให้พร้อมรองรับอุปกรณ์และระบบเครือข่าย - ซักซ้อมความพร้อมของเจ้าหน้าที่ในการดำเนินงานตามแผนกรณีเกิดน้ำท่วม แผ่นดินไหว จลาจล ให้สามารถปฏิบัติได้ตามแผนที่กำหนดไว้ ประกอบด้วย o ปิดระบบเครือข่ายทั้งหมด o แผนเตรียมการและขนย้ายเครื่องแม่ข่าย โดยจัดเตรียมสถานที่เก็บเครื่องแม่ข่าย จัดทำบัญชีรายชื่อเครื่องแม่ข่ายและอุปกรณ์เครือข่าย และติดตั้งระบบ o แผนการติดตั้งระบบฯ ให้กลับมาใช้เป็นปกติ

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
										- ตรวจสอบบัญชีเครื่องแม่ข่ายและอุปกรณ์เครือข่ายที่ต้องทำการขนย้ายเรียงตามลำดับความสำคัญ - ตรวจสอบความพร้อมใช้ของสถานที่ ระบบไฟฟ้า และระบบเครือข่ายสำรอง ให้อยู่ในสภาพพร้อมใช้งาน
๒.	รายการทรัพย์สินประเภทฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย(Network) ในส่วนของ - อุปกรณ์ ATM - อุปกรณ์ Core Switch - อุปกรณ์ Gateway Router (ภาคผนวก หน้า ๑๓๙-๑๔๐)	ระบบเครือข่ายสื่อสารภายนอก (Internet) เสียหาย/ขัดข้อง	ไม่มีระบบสื่อสารสำรองเพื่อเชื่อมต่อไปยังผู้ให้บริการเครือข่าย (ISP) รายอื่น หากระบบสื่อสารหลักมีปัญหา จะไม่สามารถให้บริการได้	๓	OI ๔	๔	๔๘	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดหาระบบสื่อสารสำรองจากผู้ให้บริการเครือข่าย (ISP) โดยใช้บริการเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) หรือ ใช้บริการจาก บริษัท ทีโอที จำกัด (มหาชน) เพื่อเป็น Link สำรอง กรณีเครือข่ายหลักที่กรมพัฒนาที่ดินใช้บริการอยู่จาก บริษัท กสท โทรคมนาคม จำกัด (มหาชน) (CAT) เสียหาย/ขัดข้อง

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
			ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด	๓	OI ๔	๔	๔๘	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง (ตามมาตรฐานที่ กรมพัฒนาที่ดินยอมรับได้)
			มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายเฉพาะอุปกรณ์ Firewall และ Router เท่านั้น	๒	OI ๔	๔	๓๒	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายทุกชิ้นที่เชื่อมต่อเข้ามากับระบบ ในส่วนที่สามารถบริหารจัดการได้ทั้งหมด
			ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There's no Redundant)	๒	OI ๔	๔	๓๒	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดหาอุปกรณ์เครือข่ายสำรองเพื่อนำมาทดแทนกรณีอุปกรณ์หลักเครือข่ายหลัก

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
										เสียหาย
			ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	๒	OI ๔	๔	๓๒	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ
		ระบบเครือข่ายสื่อสารภายในกรมพัฒนาที่ดินเสียหาย/ขัดข้อง	ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด	๓	OI ๔	๔	๔๘	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง (ตามมาตรฐานที่ กรมพัฒนาที่ดินยอมรับได้)
			ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There's no Redundant)	๒	OI ๔	๔	๓๒	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดหาอุปกรณ์เครือข่ายสำรองเพื่อนำมาทดแทนกรณีอุปกรณ์หลักเครือข่ายหลักเสียหาย
			ขาดคู่มือการปฏิบัติงาน	๒	OI ๔	๔	๓๒	**รับไม่ได้**	**Reduce**	- จัดทำคู่มือการปฏิบัติงาน

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
			(Work Instruction) ในการกู้คืนระบบ						**ลดความเสี่ยง**	(Work Instruction) ในการกู้คืนระบบ
๓.	รายการทรัพย์สินประเภทฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย(Network) ในส่วนของ - เครื่องที่ให้บริการ Web Server - เครื่องที่ให้บริการ GIS Server - เครื่องที่ให้บริการ e-Service Server - เครื่องที่ให้บริการ Mail Server - เครื่องที่ให้บริการ e-Office Server - เครื่อง Storage Server	อุปกรณ์ Hardware ภายในห้องควบคุมระบบ Network ชำรุด	ขาดแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ	๒	OI ๔	๓	๒๔	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ
			ไม่มีอุปกรณ์สำรอง	๓	OI ๔	๓	๒๔	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดหาอุปกรณ์ Hardware สำรอง ได้แก่ ๑) เครื่องแม่ข่ายสำรอง ๑ เครื่อง สำหรับให้บริการ ๒) อุปกรณ์ Switch จำนวน ๑ เครื่อง

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
	- เครื่อง Domain Server - เครื่อง Log Server - อุปกรณ์ Switch - อุปกรณ์ Firewall - อุปกรณ์ Router - (ภาคผนวก หน้า ๑๓๑-๑๓๙)									
๔.	รายการทรัพย์สินประเภทฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย(Network) ในส่วนของ - เครื่อง Domain Server (ภาคผนวก หน้า ๑๓๘)	Domain Controller ไม่สามารถให้บริการได้	Resource ไม่เพียงพอ	๒	OI ๔	๓	๒๔	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- ปรับปรุงประสิทธิภาพเครื่อง Domain Controller เช่น Upgrade RAM Hard Disk
		ข้อมูล User Profile หาย User ไม่สามารถ Login ได้	ไม่มีเครื่อง Backup Domain Controller ที่ใช้สำรองระบบ	๑	OI ๔	๓	๑๒	**รับได้**	-	-

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
๕.	รายการทรัพย์สินประเภทฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย(Network) ในส่วนของ - เครื่องที่ให้บริการ Web Server - เครื่องที่ให้บริการ GIS Server - เครื่องที่ให้บริการ e-Service Server - เครื่องที่ให้บริการ Mail Server - เครื่องที่ให้บริการ e-Office Server	ถูกโจมตีจนไม่สามารถให้บริการได้ (Denial of Service)	กระบวนการป้องกัน Denial of Service ไม่รองรับการโจมตีในรูปแบบที่ไม่ได้มีการกำหนดไว้	๓	OI ๓	๓	๒๗	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดหาอุปกรณ์ IDS หรือ IPS ที่รองรับการโจมตีชนิด Denial of Service ที่มีความสามารถในการ update รูปแบบต่างๆได้อย่างอัตโนมัติ

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
	- เครื่อง Storage Server - เครื่อง Domain Server - เครื่อง Log Server - เครื่อง Net service Server (ภาคผนวก หน้า ๑๓๑ – ๑๓๙)									
๖.	รายการทรัพย์สินประเภทฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย(Network) ในส่วนของ - เครื่องที่ให้บริการ Web Server - เครื่องที่ให้บริการ GIS Serverเครื่องที่ให้บริการ e-Service Server - เครื่องที่ให้บริการ Mail Server - เครื่องที่ให้บริการ e-Office Server	การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย	๒	OI ๔	๓	๒๔	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำกระบวนการตรวจสอบการปรับปรุง Security Patch ให้ทันสมัยของเครื่อง Server โดยตั้งค่าให้ทำงานแบบอัตโนมัติ และมีการตรวจสอบทุกเดือน

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
	- เครื่อง Storage Server - เครื่อง Domain Server - เครื่อง Log Server - เครื่อง Netservice Server (ภาคผนวก หน้า ๑๓๑-๑๓๙)									
๗.	รายการทรัพย์สินประเภทซอฟต์แวร์ (Software) ในส่วนของ - ซอฟต์แวร์ระบบปฏิบัติการ - ซอฟต์แวร์สำเร็จรูป (ภาคผนวก หน้า๑๔๒-๑๔๓)	การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	ไม่มีกระบวนการในการติดตามปรับปรุง Software Version ให้ทันสมัย	๓	OI ๔	๒	๒๔	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำงบประมาณเพื่อใช้ในการปรับปรุง Software Version ให้ทันสมัยและมีการตรวจสอบเพื่อปรับปรุง Version ทุก ๑ ปี
๘.	รายการทรัพย์สินประเภทฮาร์ดแวร์ (Hardware) และอุปกรณ์เครือข่าย(Network)	การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์	ขาดการติดตามเรื่องการถอดถอนสิทธิของพนักงานที่ลาออก หรือ	๓	OI ๓	๒	๑๘	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำแผนการทบทวนสิทธิปีละ ๒ ครั้ง

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
	ในส่วนของ - เครื่อง Domain Server (ภาคผนวก หน้า ๑๓๘)	ภายในองค์กรโดยไม่ได้รับอนุญาต (Network)	ย้ายแผนกอย่างสม่ำเสมอ							
			ไม่มีมาตรฐานการกำหนดระดับสิทธิ์การเข้าใช้งานของระบบเครือข่าย	๑	OI ๓	๒	๖	**รับได้**	-	-
			ไม่มีกระบวนการบริหารจัดการสิทธิ์ที่ดี สำหรับผู้ให้บริการภายนอก เช่น ขาดกระบวนการตรวจสอบสิทธิ์ที่ชัดเจน ขาดการกำหนดระยะเวลาการยกเลิกสิทธิ์	๑	OI ๓	๒	๖	**รับได้**	-	-
๙.	รายการทรัพย์สินประเภทซอฟต์แวร์ (Software) ในส่วนของ	การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้	๒	OI ๔	๒	๑๖	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำกระบวนการปรับปรุง Security Patch ให้ทันสมัยของซอฟต์แวร์ โดยตั้งค่าให้

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
	- ซอฟต์แวร์ระบบปฏิบัติการ - ซอฟต์แวร์สำเร็จรูป - ซอฟต์แวร์ประยุกต์ (ด้าน GIS e-Service และ e-Office) (ภาคผนวก หน้า๑๔๒-๑๔๘)		ทันสมัย							ทำงานแบบอัตโนมัติ และมีการตรวจสอบทุกเดือน
๑๐.	รายการทรัพย์สินประเภทซอฟต์แวร์ (Software) ในส่วนของ - ซอฟต์แวร์ระบบปฏิบัติการ - ซอฟต์แวร์สำเร็จรูป - ซอฟต์แวร์ประยุกต์ (ด้าน GIS e-Service และ e-Office) (ภาคผนวก หน้า๑๔๒-๑๔๘)	ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย	ขาดการตรวจสอบประสิทธิภาพการทำงานของอุปกรณ์บันทึกข้อมูล	๒	OI ๓	๒	๑๒	**รับได้**	-	-
			ไม่มีกระบวนการเฝ้าระวังและตรวจสอบ Capacity ของระบบ	๒	OI ๓	๒	๑๒	**รับได้**	-	-
			ไม่มีการจัดเก็บหรือป้องกันแผ่นโปรแกรมที่	๒	OI ๓	๒	๑๒	**รับได้**	-	-

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
			เหมาะสม							
๑๑.	รายการทรัพย์สินประเภทซอฟต์แวร์ (Software) ในส่วนของ - ซอฟต์แวร์ระบบปฏิบัติการ - ซอฟต์แวร์สำเร็จรูป - ซอฟต์แวร์ประยุกต์ (ด้าน GIS e-Service และ e-Office) (ภาคผนวก หน้า๑๔๒-๑๔๘)	ซอฟต์แวร์ทำงานผิดพลาด	ไม่มีกระบวนการตรวจสอบระบบหรือซอฟต์แวร์ก่อนนำมาใช้งานจริง	๒	OI ๓	๒	๑๒	**รับได้**	-	-
			ขาดกระบวนการในการตรวจสอบสถานะการทำงานของระบบ	๒	OI ๓	๒	๑๒	**รับได้**	-	-
			ขาดกระบวนการในการปรับปรุงฐานข้อมูลของซอฟต์แวร์ให้ทันสมัย	๒	OI ๓	๒	๑๒	**รับได้**	-	-

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
๑๒.	รายการทรัพย์สินประเภทซอฟต์แวร์ (Software) ในส่วนของ - ซอฟต์แวร์สำเร็จรูป (ภาคผนวก หน้า๑๔๒-๑๔๓)	เครื่องลูกข่ายโดน Virus โจมตี	เครื่องลูกข่ายไม่ได้ติดตั้งป้องกันVirus แบบ Client Server ที่สามารถบริหารจัดการจากศูนย์กลางได้	๒	OI ๓	๒	๑๒	**รับได้**	-	-
๑๓.	รายการทรัพย์สินประเภทข้อมูล ในส่วนของ - ข้อมูลเว็บไซต์หน่วยงานต่างๆ ภายในกรมพัฒนาที่ดิน - ข้อมูลด้าน GIS - ข้อมูลบริการประชาชน - ข้อมูล Intranet (ภาคผนวก หน้า๑๔๙-๑๕๓)	ข้อมูลสูญหาย	ทำการสำรองข้อมูลทุกวันจัดเก็บอยู่ในระบบ NAS ไม่ได้นำออกมาเก็บไว้ที่อื่นอย่างปลอดภัย	๒	EI ๔	๓	๒๔	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำการสำรองข้อมูล (Data Backup) ลงเครื่องแม่ข่ายให้บริการแบบอัตโนมัติ (Internal Media) ณ ห้องควบคุมระบบทุกวัน และทำการสำรองข้อมูล (Data Backup) ไปยังเครื่อง External Storage ทุกวันสัปดาห์ และนำไปเก็บไว้ที่ฝ่ายบริหารทั่วไป ศูนย์สารสนเทศ ชั้น ๒ ตึกอาคาร ๖ ชั้น
			มีการจัดเก็บข้อมูลรายเดือนเป็น Tap Backup	๒	EI ๔	๓	๒๔	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำการสำรองข้อมูล (Data Backup) โดยการบันทึกลง

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
			สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก							ม้วนเทป (Tape Backup) ในการ Backup ณ ห้องควบคุมระบบ เดือนละ ๑ ครั้ง และเก็บไว้ ณ สพข. ๒ (ชลบุรี)
			มีการจัดเก็บข้อมูลรายไตรมาสเป็น External Hard disk สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก	๒	EI ๔	๓	๒๔	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดทำการสำรองข้อมูล (Data Backup) โดยใช้บริการ CAT Internet Data Center (CAT-IDC) บริการคุ้มครองเก็บรักษาข้อมูลบนเซิร์ฟเวอร์ ณ บริษัทฯ CAT สาขาบางรัก ไตรมาสละ ๑ ครั้ง
			ไม่ได้ปรับปรุงแผนการสำรองข้อมูลให้เป็นปัจจุบันอย่าง จึงทำให้ฐานข้อมูล/ระบบฯ ที่พัฒนาขึ้นใหม่ อยู่นอกแผนไม่ได้ทำการสำรอง	๒	EI ๔	๓	๒๔	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	**-** ทบทวนแผนการสำรองข้อมูลให้เป็นปัจจุบันทุกครั้งที่มีการพัฒนาฐานข้อมูล/ระบบฯ ขึ้นใหม่

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
๑๔.	รายการทรัพย์สินประเภทข้อมูลในส่วนของ - ข้อมูล Mailbox (ภาคผนวก หน้า ๑๕๒)	ข้อมูล mailbox สูญหาย	ระบบ Mail Service ชำรุด	๒	OI ๓	๓	๑๘	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- ทำการสำรองข้อมูล mailbox สัปดาห์ละ ๑ ครั้งเพื่อ restore กลับมาใช้งานเมื่อติดตั้ง ระบบ Mail Service ใหม่ติดตั้งเสร็จ
๑๕.	รายการทรัพย์สินประเภท Supplies (ระบบสนับสนุน) - กล้อง CCTV (ภาคผนวก หน้า ๑๔๑)	กล้อง CCTV เสีย	ไม่มีการตรวจสอบการทำงานของ CCTV Console	๑	OI ๑	๑	๑	**รับได้**	-	-
๑๖.	รายการทรัพย์สินประเภท Supplies (ระบบสนับสนุน) - เครื่องปรับอากาศ (ภาคผนวก หน้า ๑๔๑)	เครื่องปรับอากาศไม่ทำงาน	ระบบปรับอากาศ (Air-Conditioner) ไม่ได้รับการตรวจสอบความพร้อมใช้	๓	OI ๔	๓	๓๖	**รับไม่ได้**	**Transfer โอนถ่าย**	- จัดเจ้าหน้าที่คอยดูแล และบำรุงรักษาเครื่องปรับอากาศทุก ๓ เดือน
๑๗.	รายการทรัพย์สินประเภท Supplies (ระบบสนับสนุน) - เครื่องสำรองไฟฟ้า (UPS) (ภาคผนวก หน้า ๑๔๑)	เครื่องสำรองไฟฟ้า (UPS) ไม่สามารถสำรองไฟได้	ไม่มีการเปลี่ยน Battery และวัสดุสิ้นเปลือง ตามระยะเวลาที่เหมาะสม	๓	OI ๓	๒	๑๘	**รับไม่ได้**	**Transfer โอนถ่าย**	- จัดเจ้าหน้าที่คอยดูแล และผนวกเข้ากับสัญญาบำรุงรักษาระบบเครือข่ายกรมพัฒนาที่ดิน
๑๘.	รายการทรัพย์สินประเภท	การแอบ/	ขาดการทบทวนหรือ	๑	OI ๒	๑	๒	**รับได้**	-	-

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
	Supplies (ระบบสนับสนุน) - Finger Scan (ภาคผนวก หน้า ๑๔๑)	ลักลอบเข้าสู่ห้องควบคุมระบบNetwork หรือ ไม่มีการควบคุมการเข้าออกห้องควบคุมระบบNetwork	ยกเลิกสิทธิผู้ที่ไม่เกี่ยวข้องในการเข้าถึงห้องควบคุมระบบ Network							
๑๙.	รายการทรัพย์สินประเภทบริการ(Stakeholders) - บริษัท กสท. โทรคมนาคม จำกัด (มหาชน) (ภาคผนวก หน้า ๑๕๘)	เครือข่ายหลักล่มไม่สามารถใช้งาน Internet ได้ ทำให้การให้บริการล้มเหลว	ไม่มีระบบสื่อสาร Internet พร้อมวงจรเชื่อมโยงสำรอง	๓	EI ๔	๔	๔๘	**รับไม่ได้**	**Transfer โอนถ่าย**	- จัดทำแผนระบบสื่อสารสำรองกับ ISP รายอื่น โดยใช้เป็น link ที่มีความเร็วที่ต่ำกว่า เนื่องจากเป็นการใช้งานทดแทนชั่วคราว โดยเขียนเป็นโครงการเพื่อของบประมาณมาดำเนินการจากกรมฯ
๒๐.	รายการทรัพย์สินประเภทบริการ (Stakeholders) - บริษัท ดิ เอ็กซ์เพิร์ท ไอซี	อุปกรณ์สำรองไม่สามารถใช้งานได้	ไม่มีการตรวจสอบอุปกรณ์สำรองที่จะนำมาใช้ทดแทนระบบหลักของผู้ให้บริการ	๓	OI ๔	๓	๓๖	**รับไม่ได้**	**Transfer โอนถ่าย**	- กำหนดเป็นเงื่อนไขในสัญญาของผู้ให้บริการ ที่ต้องจัดหาอุปกรณ์สำรองที่นำมาใช้

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม
	ที จำกัด (ภาคผนวก หน้า ๑๕๘)		ภายนอก							ทดแทน กรณีอุปกรณ์ระบบหลักชำรุดในทันที และจัดเตรียมงบประมาณที่ต้องนำมาใช้ดำเนินการจากกรมฯ
๒๑.	รายการทรัพย์สินประเภทคน - กลุ่มระบบเครือข่ายและคอมพิวเตอร์ (ภาคผนวก หน้า ๑๕๕)	เจ้าหน้าที่ Network Admin หลักไม่สามารถปฏิบัติได้	เจ้าหน้าที่ Network Admin สำรองมีทักษะไม่เท่ากับ Network Admin หลัก	๓	PI ๔	๓	๓๖	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- ฝึกอบรมเจ้าหน้าที่ Network Admin สำรองให้มีทักษะเทียบเท่ากับ Network Admin หลัก
๒๒.	รายการทรัพย์สินประเภทคน - กลุ่มฐานข้อมูลสารสนเทศ (ภาคผนวก หน้า ๑๕๖)	เจ้าหน้าที่ Programmer ไม่สามารถปฏิบัติได้	ไม่มีเจ้าหน้าที่ Programmerสำรอง	๓	PI ๕	๓	๔๕	**รับไม่ได้**	**Reduce ลดความเสี่ยง**	- จัดส่งเจ้าหน้าที่ไปเข้ารับการฝึกอบรมกับสถาบันที่มีมาตรฐาน เพื่อทำให้มี Programmer มากขึ้น

บทที่ ๔
การบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

กระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นกระบวนการที่สร้างขึ้นโดยมีขั้นตอนที่ช่วยเสริมการทำงานร่วมกับโครงการ หรือภาระงานอื่นใดที่ปฏิบัติการอยู่ด้านสารสนเทศ ให้เป็นไปด้วยความราบรื่นหรือป้องกันโอกาสที่จะเกิดความเสี่ยงและเป็นปัญหาหรืออาจจะกล่าวได้ว่าเป็นการมองไปข้างหน้า ป้องกันเหตุที่อาจจะเกิดขึ้นในอนาคตอย่างมีเหตุมีผล มีหลักการและหาทางลดหรือป้องกันความเสียหายในการทำงานในภารกิจของหน่วยงาน/โครงการที่มีการวางาแผนการปฏิบัติงานไว้แล้วในแต่ละขั้นตอน โดยมีรายละเอียด ดังนี้

๔.๑ แผนปฏิบัติการการบริหารความเสี่ยง (Risk Implementation)

๔.๒ การติดตามและประเมินผลการบริหารจัดการความเสี่ยง (Monitoring & Review)

๔.๑ แผนปฏิบัติการการบริหารความเสี่ยง (Risk Implementation)

ถือเป็นเครื่องมือที่มีความสำคัญเป็นกรอบแนวทางการปฏิบัติงานในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพและประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเหล่านั้นอย่างเป็นระบบโดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยงแล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

ตาราง ๘ แผนปฏิบัติการการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	ระดับความเสี่ยง Risk Value	กิจกรรมในการควบคุม	หน่วยงาน รับผิดชอบ	กำหนดการ ดำเนินการ
๑.	ไฟฟ้าลัดวงจร	ไม่มีการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบNetwork	๒๐	- ทบทวน “นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมพัฒนาที่ดิน” โดยเพิ่มข้อกำหนด การนำอุปกรณ์เข้าห้องควบคุมระบบ จะต้องทำการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ เพื่อป้องกันไฟฟ้าลัดวงจร	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ธันวาคม ๒๕๕๖
				- กำหนดเจ้าหน้าที่รับผิดชอบ ในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออกจากห้องควบคุมระบบ Network	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ทุกครั้งที่มีการนำอุปกรณ์เข้า/ออกจากห้องควบคุมระบบ Network
		ไม่มีการตรวจสอบความสมบูรณ์ของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network	๒๐	กำหนดเจ้าหน้าที่รับผิดชอบ ในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออกจากห้องควบคุมระบบ Network	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ธันวาคม ๒๕๕๖
๒.	ไฟไหม้	ไม่มีการทดสอบการฉีดก๊าซจากถังดับเพลิงจริง - ถังดับเพลิงชนิดผงเคมีแห้ง (Class A และ B) - ถังดับเพลิงชนิดก๊าซคาร์บอนได้ออกไซด์หรือ CO2 (Class B และ C)	๒๐	ซักซ้อมและทดสอบการฉีดก๊าซจากถังดับเพลิงจริง ปีละ ๒ ครั้ง (ตามแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ และการสื่อสาร IT Contingency Plan)	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	เดือนมีนาคม และเดือนกันยายนของทุกปี

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	ระดับความเสี่ยง Risk Value	กิจกรรมในการควบคุม	หน่วยงาน รับผิดชอบ	กำหนดการ ดำเนินการ
		ไม่มีถังดับเพลิงชนิด HCFC-123 (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารโดยเฉพาะ	๒๐	จัดหาถังดับเพลิงชนิด HCFC-123 (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารโดยเฉพาะ	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	มีนาคม ๒๕๕๖
๓.	น้ำท่วม แผ่นดินไหว	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ	๒๐	- จัดเตรียมสถานที่สำรองภายนอกกรมพัฒนาที่ดิน ให้พร้อมรองรับอุปกรณ์และระบบเครือข่าย - ซักซ้อมความพร้อมของเจ้าหน้าที่ในการดำเนินงานตามแผนกรณีเกิดน้ำท่วม แผ่นดินไหว จลาจล ให้สามารถปฏิบัติได้ตามแผนที่กำหนดไว้ ประกอบด้วย o ปิดระบบเครือข่ายทั้งหมด o แผนเตรียมการและขนย้ายเครื่องแม่ข่าย โดยจัดเตรียมสถานที่เก็บเครื่องแม่ข่าย จัดทำบัญชีรายชื่อเครื่องแม่ข่ายและอุปกรณ์เครือข่าย และติดตั้งระบบ o แผนการติดตั้งระบบฯ ให้กลับมาใช้เป็นปกติ - ตรวจสอบบัญชีเครื่องแม่ข่ายและอุปกรณ์เครือข่ายที่ต้องทำการขนย้ายเรียงตามลำดับความสำคัญ - ตรวจสอบความพร้อมใช้ของสถานที่ ระบบไฟฟ้า และระบบเครือข่ายสำรอง ให้อยู่ในสภาพพร้อมใช้งาน	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	มีนาคม ๒๕๕๖

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	ระดับความเสี่ยง Risk Value	กิจกรรมในการควบคุม	หน่วยงานรับผิดชอบ	กำหนดการดำเนินการ
๔.	การชุมนุม จลาจล	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ	๒๐	- จัดเตรียมสถานที่สำรองภายนอกกรมพัฒนาที่ดิน ให้พร้อมรองรับอุปกรณ์และระบบเครือข่าย - ซักซ้อมความพร้อมของเจ้าหน้าที่ในการดำเนินงานตามแผนกรณีเกิดน้ำท่วม แผ่นดินไหว จลาจล ให้สามารถปฏิบัติได้ตามแผนที่กำหนดไว้ ประกอบด้วย o ปิดระบบเครือข่ายทั้งหมด o แผนเตรียมการและขนย้ายเครื่องแม่ข่าย โดยจัดเตรียมสถานที่เก็บเครื่องแม่ข่าย จัดทำบัญชีรายชื่อเครื่องแม่ข่ายและอุปกรณ์เครือข่าย และติดตั้งระบบ o แผนการติดตั้งระบบฯ ให้กลับมาใช้เป็นปกติ - ตรวจสอบบัญชีเครื่องแม่ข่ายและอุปกรณ์เครือข่ายที่ต้องทำการขนย้ายเรียงตามลำดับความสำคัญ - ตรวจสอบความพร้อมใช้ของสถานที่ ระบบไฟฟ้า และระบบเครือข่ายสำรอง ให้อยู่ในสภาพพร้อมใช้งาน	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	กันยายน ๒๕๕๖
๕.	ระบบเครือข่ายสื่อสารภายนอก (Internet) เสียหาย/ขัดข้อง	ไม่มีระบบสื่อสารสำรองเพื่อเชื่อมต่อไปยังผู้ให้บริการเครือข่าย (ISP) รายอื่น หากระบบสื่อสารหลักมีปัญหา จะไม่สามารถให้บริการได้	๔๘	- จัดหาระบบสื่อสารสำรองจาก ผู้ให้บริการเครือข่าย (ISP) โดยใช้บริการเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) หรือ ใช้บริการจาก บริษัท ทีโอที จำกัด (มหาชน) เพื่อเป็น Link สำรอง กรณีเครือข่ายหลักที่กรมพัฒนาที่ดินใช้	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ตุลาคม ๒๕๕๕

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	ระดับความเสี่ยง Risk Value	กิจกรรมในการควบคุม	หน่วยงาน รับผิดชอบ	กำหนดการ ดำเนินการ
				บริการอยู่ จาก บริษัท กสท โทรคมนาคม จำกัด (มหาชน) (CAT) เสียหาย/ขัดข้อง		
		ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด	๔๘	- มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง (ตามมาตรฐานที่ กรมพัฒนาที่ดินยอมรับได้)	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ตุลาคม ๒๕๕๕
		มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่าย เฉพาะอุปกรณ์ Firewall และ Router เท่านั้น	๓๒	- มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายที่สามารถบริหารจัดการได้(Management Device) ทุกเครื่อง ที่เชื่อมต่อเข้ามากับระบบเครือข่ายของกรมพัฒนาที่ดิน	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	เดือนละครั้ง
		ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There's no Redundant)	๓๒	- จัดหาอุปกรณ์เครือข่ายสำรองเพื่อนำมาทดแทนกรณีอุปกรณ์หลักเครือข่ายหลักเสียหาย	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	
		ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	๓๒	- จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	มกราคม ๒๕๕๖

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	ระดับความเสี่ยง Risk Value	กิจกรรมในการควบคุม	หน่วยงานรับผิดชอบ	กำหนดการดำเนินการ
๖.	ระบบเครือข่ายสื่อสารภายในกรมพัฒนาที่ดินเสียหาย/ขัดข้อง	ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด	๔๘	- มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง (ตามมาตรฐานที่ กรมพัฒนาที่ดินยอมรับได้)	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	
		ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There's no Redundant)	๓๒	- จัดหาอุปกรณ์เครือข่ายสำรองเพื่อนำมาทดแทนกรณีอุปกรณ์หลักเครือข่ายหลักเสียหาย	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	
		ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	๓๒	- จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	มกราคม ๒๕๕๖
๗.	อุปกรณ์ Hardware ภายในห้อง ควบคุมระบบ Network ชำรุด	ขาดแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ	๒๔	- จัดทำแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ตุลาคม ๒๕๕๕

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	ระดับความเสี่ยง Risk Value	กิจกรรมในการควบคุม	หน่วยงานรับผิดชอบ	กำหนดการดำเนินการ
		ไม่มีอุปกรณ์สำรอง	๒๔	- จัดหาอุปกรณ์ Hardware สำรอง ได้แก่ ๑) เครื่องแม่ข่ายสำรอง ๑ เครื่อง สำหรับให้บริการ ๒) อุปกรณ์ Switch จำนวน ๑ เครื่อง	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ตุลาคม ๒๕๕๕
๘.	Domain Controller ไม่สามารถให้บริการได้	Resource ไม่เพียงพอ	๒๔	- ปรับปรุงประสิทธิภาพเครื่อง Domain Controller เช่น Upgrade RAM Hard Disk	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	มกราคม ๒๕๕๖
๙.	ถูกโจมตีจนไม่สามารถให้บริการได้ (Denial of Service)	กระบวนการป้องกัน Denial of Service ไม่รองรับการโจมตีในรูปแบบที่ไม้ได้มีการกำหนดไว้	๒๗	- จัดหาอุปกรณ์ IDS หรือ IPS ที่รองรับการโจมตีชนิด Denial of Service ที่มีความสามารถในการ update รูปแบบต่างๆ ได้อย่างอัตโนมัติ	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	
๑๐.	การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย	๒๔	- จัดทำกระบวนการตรวจสอบการปรับปรุง Security Patch ให้ทันสมัยของเครื่อง Server โดยตั้งค่าให้ทำงานแบบอัตโนมัติ และมีการตรวจสอบทุกเดือน	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ทุกเดือน
		ไม่มีกระบวนการในการติดตามปรับปรุง Software Version ให้ทันสมัย	๒๔	- จัดทำงบประมาณเพื่อใช้ในการปรับปรุง Software Version ให้ทันสมัยและมีการตรวจสอบเพื่อปรับปรุง Version ทุก ๑ ปี	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ทุกปี
๑๑.	การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต (Network)	ขาดการติดตามเรื่องการถอดถอนสิทธิของพนักงานที่ลาออก หรือย้ายแผนกอย่างสม่ำเสมอ	๑๘	- จัดทำแผนการทบทวนสิทธิปีละ ๒ ครั้ง	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	เดือนมีนาคม และเดือนกันยายนของทุกปี

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	ระดับความเสี่ยง Risk Value	กิจกรรมในการควบคุม	หน่วยงานรับผิดชอบ	กำหนดการดำเนินการ
๑๒.	การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย	๑๖	- จัดทำกระบวนการปรับปรุง Security Patch ให้ทันสมัยของซอฟต์แวร์ โดยตั้งค่าให้ทำงานแบบอัตโนมัติ และมีการตรวจสอบทุกเดือน	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ทุกเดือน
๑๓.	ข้อมูลสูญหาย	ทำการสำรองข้อมูลทุกวันจัดเก็บอยู่ในระบบ NAS ไม่ได้นำออกมาเก็บไว้ที่อื่นอย่างปลอดภัย	๒๔	- จัดทำการสำรองข้อมูล (Data Backup) ลงเครื่องแม่ข่ายให้บริการแบบอัตโนมัติ (Internal Media) ณ ห้องควบคุมระบบทุกวัน และทำการสำรองข้อมูล (Data Backup) ไปยังเครื่อง External Storage ทุกสัปดาห์ และนำไปเก็บไว้ที่ฝ่ายบริหารทั่วไป ศูนย์สารสนเทศ ชั้น ๒ ตึกอาคาร ๖ ชั้น	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ทุกสัปดาห์
		มีการจัดเก็บข้อมูลรายเดือนเป็น Tap Backup สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก	๒๔	- จัดทำการสำรองข้อมูล (Data Backup) โดยการบันทึกลงม้วนเทป (Tape Backup) ในการ Backup ณ ห้องควบคุมระบบ เดือนละ ๑ ครั้ง และเก็บไว้ ณ สพข. ๒ (ชลบุรี)	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ทุกเดือน
		มีการจัดเก็บข้อมูลรายไตรมาสเป็น External Hard disk สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก	๒๔	- จัดทำการสำรองข้อมูล (Data Backup) โดยใช้บริการ CAT Internet Data Center (CAT-IDC) บริการคุ้มครองเก็บรักษาข้อมูลบนเซิร์ฟเวอร์ ณ บริษัทฯ CAT สาขาบางรัก ไตรมาสละ ๑ ครั้ง	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ไตรมาสละ ๑ ครั้ง
		ไม่ได้ปรับปรุงแผนการสำรองข้อมูลให้เป็นปัจจุบันอย่าง จึงทำให้ฐานข้อมูล/ระบบฯ ที่พัฒนาขึ้นใหม่ อยู่นอกแผนไม่ได้ทำการสำรอง	๒๔	- ทบทวนแผนการสำรองข้อมูลให้เป็นปัจจุบันทุกครั้งที่มีการพัฒนาฐานข้อมูล/ระบบฯ ขึ้นใหม่	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ทุกครั้งที่มีการพัฒนาฐานข้อมูล/ระบบฯ ขึ้นใหม่

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	ระดับความเสี่ยง Risk Value	กิจกรรมในการควบคุม	หน่วยงาน รับผิดชอบ	กำหนดการ ดำเนินการ
๑๔.	ข้อมูล mailbox สูญหาย	ระบบ Mail Service ชำรุด	๑๘	- ทำการสำรองข้อมูล mailbox สัปดาห์ละ ๑ ครั้งเพื่อ restore กลับมาใช้งานเมื่อระบบ Mail Service ใหม่ติดตั้งเสร็จ	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	สัปดาห์ละ ๑
๑๕.	เจ้าหน้าที่ Network Admin หลักไม่สามารถปฏิบัติได้	เจ้าหน้าที่ Network Admin สำรองมีทักษะไม่เท่ากับ Network Admin หลัก	๓๖	- ฝึกอบรมเจ้าหน้าที่ Network Admin สำรองให้มีทักษะเทียบเท่ากับ Network Admin หลัก	กลุ่มระบบเครือข่ายและคอมพิวเตอร์	ปีงบประมาณ ๒๕๕๖ (ตุลาคม ๒๕๕๕-กันยายน๒๕๕๖)
๑๖.	เจ้าหน้าที่ Programmer ไม่สามารถปฏิบัติได้	ไม่มีเจ้าหน้าที่ Programmerสำรอง	๔๕	- จัดส่งเจ้าหน้าที่ไปเข้ารับการฝึกอบรมกับสถาบันที่มีมาตรฐานเพื่อทำให้มี Programmer มากขึ้น	กลุ่มฐานข้อมูลสารสนเทศ	ปีงบประมาณ ๒๕๕๖ (ตุลาคม ๒๕๕๕-กันยายน๒๕๕๖)

๔.๒ การติดตามและการประเมินผลการบริหารจัดการความเสี่ยง

๔.๓.๑ การติดตามการบริหารจัดการความเสี่ยง

การติดตามผลการจัดการความเสี่ยงของศูนย์สารสนเทศ กรมพัฒนาที่ดิน เพื่อให้มั่นใจว่าการบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพสามารถตอบสนองต่อการเปลี่ยนแปลงได้ทันกาล โดยกำหนดให้มีการติดตามผลตามรอบระยะเวลาที่กำหนด และประเมินผลทุกสิ้นปี

ทั้งนี้ การติดตามผลในระหว่างการปฏิบัติงาน (Ongoing Monitoring) ดำเนินการโดยให้เป็นการติดตามที่รวมอยู่ในการดำเนินงานต่างๆ ตามปกติของศูนย์สารสนเทศ และเมื่อการติดตามผลพบสิ่งที่อาจจะก่อให้เกิดความผิดพลาด หรือพบโอกาสในการพัฒนาให้ดีขึ้นเพื่อการบรรลุวัตถุประสงค์ขององค์กร จะต้องมีการรายงานความบกพร่อง (Reporting Deficiencies) ให้ผู้บริหารทราบ

๔.๓.๒ การประเมินผลการบริหารจัดการความเสี่ยง

ประเมินผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศประจำปี โดยการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยงและติดตามผลการจัดการความเสี่ยงว่าความเสี่ยงลดลงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

ตารางที่ ๙ การติดตามและประเมินผลการบริหารจัดการความเสี่ยง

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๑.	ไฟฟ้าลัดวงจร	ไม่มีการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network	- ทบทวน “นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมพัฒนาที่ดิน” โดยเพิ่มข้อกำหนด การนำอุปกรณ์เข้าห้องควบคุมระบบ จะต้องทำการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ เพื่อป้องกันไฟฟ้าลัดวงจร - กำหนดเจ้าหน้าที่รับผิดชอบในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออกจากห้องควบคุมระบบ Network	- จัดทำตารางตรวจสอบการใช้กระแสไฟฟ้าของอุปกรณ์ ทุกชิ้นก่อนติดตั้งในห้องควบคุมระบบ - สรุปปริมาณกระแสไฟฟ้าที่ใช้งานอยู่ในปัจจุบันและความสามารถในการรองรับการใช้งานในอนาคตเพื่อประเมินการติดตั้งระบบไฟฟ้าเพิ่มเติมให้เพียงพอต่อความต้องการ - จัดเจ้าหน้าที่ดูแลรับผิดชอบ คือ นายสุพงษ์ ไพชยนต์ และ นางวราภรณ์ อินทร์ทิพย์ ในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออก จากห้องควบคุมระบบ Network	๑	EI ๓	๔	๑๒	**รับได้**
		ไม่มีการตรวจสอบความสมบูรณ์ของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network	- กำหนดเจ้าหน้าที่รับผิดชอบในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออกจากห้องควบคุมระบบ Network	- จัดเจ้าหน้าที่ดูแลรับผิดชอบ คือ นายสุพงษ์ ไพชยนต์ และ นางวราภรณ์ อินทร์ทิพย์ ในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออก จากห้องควบคุมระบบ Network	๑	EI ๓	๔	๑๒	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๒	ไฟไหม้	ไม่มีการทดสอบการฉีดก๊าซจากถังดับเพลิงจริง - ถังดับเพลิงชนิดผงเคมีแห้ง (Class A และ B) - ถังดับเพลิงชนิดก๊าซคาร์บอนได้ออกไซด์หรือ CO2 (Class B และ C)	- ซักซ้อมและทดสอบการฉีดก๊าซจากถังดับเพลิงจริง ปีละ ๒ ครั้ง (ตามแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร IT Contingency Plan)	- จัดทำแผนทดสอบการทำงานของถังดับเพลิงในเดือน มีนาคม และ กันยายน ของทุกปี เพื่อประเมินประสิทธิภาพในการทำงานของอุปกรณ์ - ทดสอบการฉีดก๊าซจากถังดับเพลิงจริง ปีละ ๒ ครั้ง และสรุปผลการทดสอบ - จัดทำงบประมาณรองรับการเปลี่ยนอุปกรณ์เพื่อให้อุปกรณ์พร้อมในการใช้งาน (ทุก ๕ ปี)	๑	EI ๒	๔	๘	**รับได้**
		ไม่มีถังดับเพลิงชนิด HCFC-123 (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารโดยเฉพาะ	- จัดหาถังดับเพลิงชนิด HCFC-123 (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารโดยเฉพาะ	- เนื่องจากไม่มีงบประมาณจัดซื้อ ถังดับเพลิงชนิด HCFC-๑๒๓ (Halatron) จึงทำให้ไม่สามารถปฏิบัติตามกิจกรรมในการควบคุมที่กำหนดไว้ได้	๑	EI ๕	๔	๒๐	**รับไม่ได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๓	น้ำท่วม แผ่นดินไหว	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ	- จัดเตรียมสถานที่สำรองภายนอกกรมพัฒนาที่ดิน ให้พร้อมรองรับอุปกรณ์และระบบเครือข่าย - ซักซ้อมความพร้อมของเจ้าหน้าที่ในการดำเนินงานตามแผนกรณีเกิดน้ำท่วม แผ่นดินไหว จลาจล ให้สามารถปฏิบัติได้ตามแผนที่กำหนดไว้ ประกอบด้วย ๑) ปิดระบบเครือข่ายทั้งหมด ๒) แผนเตรียมการและขนย้ายเครื่องแม่ข่าย โดยจัดเตรียมสถานที่เก็บเครื่องแม่ข่าย จัดทำบัญชีรายชื่อเครื่องแม่ข่ายและอุปกรณ์เครือข่ายและติดตั้งระบบ ๓) แผนการติดตั้งระบบฯ	- จัดเตรียมแผนการปฏิบัติงานเพื่อเตรียมความพร้อมด้านการจัดการระบบสารสนเทศในภาวะที่ต้องเฝ้าระวังเป็นพิเศษ ทดสอบตามแผนปีละ ๑ ครั้ง ดังนี้ ๑) สถานที่บริการระบบเครือข่ายสำรอง สำนักงานพัฒนาที่ดินเขต ๑ (ปทุมธานี) ๒) วงจรบริการ Internet/Intranet ประสานงานกับ CAT เพื่อ Up Link ประมาณ ๒๐/๑๐๐ Mbps ๓) เตรียมเครื่องแม่ข่ายที่ต้องย้าย ได้แก่ ๓.๑ เครื่อง Web Site กรมพัฒนาที่ดิน ๓.๒ เครื่อง Fire Wall ๓.๓ เครื่อง Mail Server ๓.๔ เครื่อง Web Site กองคลัง (ให้บริการโอนเงิน) ๓.๓ เครื่องระบบบริการประชาชน จำนวน ๒ เครื่อง	๑	EI ๒	๔	๘	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
			ให้กลับมาใช้เป็นปกติ - ตรวจสอบบัญชีเครื่องแม่ข่ายและอุปกรณ์เครือข่ายที่ต้องทำการขนย้ายเรียงตามลำดับความสำคัญ - ตรวจสอบความพร้อมใช้ของสถานที่ ระบบไฟฟ้า และระบบเครือข่ายสำรอง ให้อยู่ในสภาพพร้อมใช้งาน	๓.๔ เครื่อง UPS สำรอง ๓K ๔) การติดตั้งระบบให้กลับมาใช้ได้เป็นปกติ					
๔	การชุมนุมจลาจล	มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ	- จัดเตรียมสถานที่สำรองภายนอกกรมพัฒนาที่ดิน ให้พร้อมรองรับอุปกรณ์และระบบเครือข่าย - ซักซ้อมความพร้อมของเจ้าหน้าที่ในการดำเนินงานตามแผนกรณีเกิดน้ำท่วม แผ่นดินไหว จลาจล ให้สามารถปฏิบัติได้ตามแผนที่กำหนดไว้ ประกอบด้วย ๑) ปิดระบบเครือข่าย	- จัดเตรียมแผนการปฏิบัติงานเพื่อเตรียมความพร้อมด้านการจัดการระบบสารสนเทศในภาวะที่ต้องเฝ้าระวังเป็นพิเศษ ทดสอบตามแผนปีละ ๑ ครั้ง ดังนี้ ๑) สถานที่บริการระบบเครือข่ายสำรอง สำนักงานพัฒนาที่ดินเขต ๑ (ปทุมธานี) ๒) วงจรบริการ Internet/Intranet ประสานงานกับ CAT เพื่อ Up Link ประมาณ ๒๐/๑๐๐ Mbps ๓) เตรียมเครื่องแม่ข่ายที่ต้องย้าย ได้แก่	๑	EI ๒	๔	๘	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
			ทั้งหมด ๒) แผนเตรียมการและขนย้ายเครื่องแม่ข่าย โดยจัดเตรียมสถานที่เก็บเครื่องแม่ข่าย จัดทำบัญชีรายชื่อเครื่องแม่ข่ายและอุปกรณ์เครือข่ายและติดตั้งระบบ ๓) แผนการติดตั้งระบบฯ ให้กลับมาใช้เป็นปกติ - ตรวจสอบบัญชีเครื่องแม่ข่ายและอุปกรณ์เครือข่ายที่ต้องทำการขนย้ายเรียงตามลำดับความสำคัญ - ตรวจสอบความพร้อมใช้ของสถานที่ ระบบไฟฟ้า และระบบเครือข่ายสำรอง ให้อยู่ในสภาพพร้อมใช้งาน	๓.๓ เครื่อง Web Site กรมพัฒนาที่ดิน ๓.๔ เครื่อง Fire Wall ๓.๓ เครื่อง Mail Server ๓.๔ เครื่อง Web Site กองคลัง (ให้บริการโอนเงิน) ๓.๕ เครื่องระบบบริการประชาชน จำนวน ๒ เครื่อง ๓.๖ เครื่อง UPS สำรอง ๓K ๔) การติดตั้งระบบให้กลับมาใช้ได้เป็นปกติ					

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๕.	ระบบเครือข่ายสื่อสารภายนอก (Internet) เสียหาย/ขัดข้อง	ไม่มีระบบสื่อสารสำรองเพื่อเชื่อมต่อไปยังผู้ให้บริการเครือข่าย (ISP) รายอื่น หากระบบสื่อสารหลักมีปัญหา จะไม่สามารถให้บริการได้	- จัดหาระบบสื่อสารสำรองจากผู้ให้บริการเครือข่าย (ISP) โดยใช้บริการเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) หรือ ใช้บริการจาก บริษัท ทีโอที จำกัด (มหาชน) เพื่อเป็น Link สำรอง กรณีเครือข่ายหลักที่กรมพัฒนาที่ดินใช้บริการอยู่จาก บริษัท กสท โทรคมนาคม จำกัด (มหาชน) (CAT) เสียหาย/ขัดข้อง	- ตรวจสอบสถานะการทำงานของอุปกรณ์เครือข่ายหลักที่ใช้งานและอุปกรณ์เครือข่ายสำรองที่เป็นระบบ Backup โดยพิจารณาค่าการทำงานของหน่วยประมวลผล หน่วยความจำ และปริมาณการส่งผ่านข้อมูล(Packet) เข้าออกให้อยู่ในสถานะพร้อมใช้งานได้ตลอดเวลา - ตรวจสอบค่ากำหนดทางด้านมาตรฐานการเชื่อมต่อเครือข่ายอุปกรณ์ให้ถูกต้องตามข้อกำหนดของกรมฯ และตรวจสอบดู Log ค่าเหตุการณ์ ต่าง ๆ ที่แสดงข้อผิดพลาดที่อาจเกิดขึ้นได้ - ทดสอบการทำงานของระบบเครือข่ายหลักตามแบบการบำรุงรักษา ปีละ ๔ ครั้ง (จัดทำแผนการจัดหาระบบสื่อสารสำรอง	๓	OI ๒	๔	**๒๔**	**รับไม่ได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
				จาก ผู้ให้บริการเครือข่าย (ISP) รายอื่นอีก ๑ วงจร ในปีงบประมาณต่อไป)					
		ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด	- มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง (ตามมาตรฐานที่ กรมพัฒนาที่ดินยอมรับได้)	- กำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง ในเอกสารสัญญาของผู้รับจ้าง - ตรวจสอบสถานะการทำงานของระบบเครือข่ายสื่อสารภายใน ว่ามีปริมาณช่วงเวลาที่ใช้งานไม่ได้จำนวนกี่ครั้ง และแต่ละครั้งที่ไม่สามารถใช้งาน จะต้องใช้เวลาในการแก้ไขให้กลับมาใช้งานได้ ไม่เกิน ๔ ชั่วโมง ตามข้อกำหนดที่ตกลงไว้ - ให้ผู้รับจ้างทำการบันทึกเป็นรายงานสถานะการทำงานประจำเดือน เพื่อจัดทำสถิติของการ downtime ของระบบ	๒	OI ๒	๔	**๑๖**	**รับไม่ได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
		มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายเฉพาะอุปกรณ์ Firewall และ Router เท่านั้น	- มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายที่สามารถบริหารจัดการได้(Management Device) ทุกเครื่อง ที่เชื่อมต่อเข้ามากับระบบเครือข่ายของกรมพัฒนาที่ดิน	- จัดทำระบบการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายที่สามารถบริหารจัดการได้ (Management Device) ได้แก่ Switch , Router , firewall , IPS , proxy - ทำการบันทึกเป็นรายงานสถานะการเฝ้าระวังและติดตามประจำเดือน เพื่อเปรียบเทียบสถิติของการทำงานทั้งหมด	๑	OI ๒	๔	**๘**	**รับได้**
		ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There’s no Redundant)	- จัดหาอุปกรณ์เครือข่ายสำรองเพื่อนำมาทดแทนกรณีอุปกรณ์หลักเครือข่ายหลักเสียหาย	- สำรวจจำนวนอุปกรณ์เครือข่ายสำรองที่ต้องการทดแทน กรณีที่อุปกรณ์เครือข่ายหลักเกิดความเสียหายไม่สามารถใช้งานได้ - กำหนดคุณลักษณะของอุปกรณ์เครือข่ายที่ต้องจัดหาเพื่อนำมาทดแทน	๑	OI ๒	๔	๘	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
				- ประสานงานผู้ให้บริการเครือข่ายเพื่อจัดเตรียมอุปกรณ์สำรองในกรณีที่อุปกรณ์หลักเกิดความเสียหายโดยกำหนดเป็นคุณลักษณะในสัญญา					
		ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	- จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	- จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ ประกอบด้วย ๑) เอกสารการกำหนดค่า Configuration อุปกรณ์เครือข่าย (Router, Switch) ๒) เอกสารกำหนดค่า Configuration เครื่องแม่ข่าย Web Server ๓) เอกสารกำหนดค่าConfiguration เครื่องแม่ข่าย Mail Server	๑	OI ๓	๔	**๑๒**	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๖.	ระบบเครือข่ายสื่อสารภายในกรมพัฒนาที่ดินเสียหาย/ขัดข้อง	ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด	- มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง (ตามมาตรฐานที่ กรมพัฒนาที่ดินยอมรับได้)	- กำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง ในเอกสารสัญญาของผู้รับจ้าง - ตรวจสอบสถานะการทำงานของระบบเครือข่ายสื่อสารภายใน ว่ามีปริมาณช่วงเวลาที่ใช้งานไม่ได้จำนวนกี่ครั้ง และแต่ละครั้งที่ไม่สามารถใช้งาน จะต้องใช้เวลาในการแก้ไขให้กลับมาใช้งานได้ ไม่เกิน ๔ ชั่วโมง ตามข้อกำหนดที่ตกลงไว้ - ให้ผู้รับจ้างทำการบันทึกเป็นรายงานสถานะการทำงานประจำเดือน เพื่อจัดทำสถิติของการ downtime ของระบบ	๒	OI ๒	๔	**๑๖**	**รับไม่ได้**
		ไม่มีอุปกรณ์ที่สามารถ	- จัดหาอุปกรณ์เครือข่ายสำรอง	- สำรวจจำนวนอุปกรณ์เครือข่ายสำรองที่	๑	OI ๒	๔	๘	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
		ทำงานทดแทนได้ทันที (There's no Redundant)	เพื่อนำมาทดแทนกรณีอุปกรณ์หลักเครือข่ายหลักเสียหาย	ต้องการทดแทน กรณีที่อุปกรณ์เครือข่ายหลักเกิดความเสียหายไม่สามารถใช้งานได้ - กำหนดคุณลักษณะของอุปกรณ์เครือข่ายที่ต้องจัดหาเพื่อนำมาทดแทน - ประสานงานผู้ให้บริการเครือข่ายเพื่อจัดเตรียมอุปกรณ์สำรองในกรณีที่อุปกรณ์หลักเกิดความเสียหายโดยกำหนดเป็นคุณลักษณะในสัญญา					
		ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	- จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ	- จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ ประกอบด้วย ๑) เอกสารการกำหนดค่า Configuration อุปกรณ์เครือข่าย (Router, Switch) ๒) เอกสารกำหนดค่า Configuration เครื่องแม่ข่าย Web Server ๓) เอกสารกำหนดค่า Configuration เครื่องแม่ข่าย Mail Server	๑	OI ๓	๔	**๑๒**	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
๗.	อุปกรณ์ Hardware ภายในห้องควบคุมระบบ Network ชำรุด	ขาดแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ	- จัดทำแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ	- จัดทำแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ - ทดสอบแผนการบริหารจัดการอุปกรณ์ Hardware ที่จัดทำ ว่าเป็นไปตามวัตถุประสงค์ - สรุปแผนการบริหารจัดการอุปกรณ์ Hardware หลังจากทำการทดสอบแผนทุกๆ ๓ เดือน	๑	OI ๓	๓	๙	**รับได้**
		ไม่มีอุปกรณ์สำรอง	- จัดหาอุปกรณ์ Hardware สำรอง ได้แก่ ๑) เครื่องแม่ข่ายสำรอง ๑ เครื่อง สำหรับให้บริการ ๒) อุปกรณ์ Switch จำนวน ๑ เครื่อง	- ติดตั้งระบบปฏิบัติการสำหรับเครื่องแม่ข่าย กำหนดค่า Configuration ให้กับอุปกรณ์ Hardware สำรอง ได้แก่ เครื่องแม่ข่ายสำรอง ๑ เครื่อง สำหรับให้บริการอุปกรณ์ Switch จำนวน ๑ เครื่อง - ตรวจสอบสถานะการทำงานของอุปกรณ์ให้พร้อมปฏิบัติงาน	๒	OI ๒	๓	๑๒	**รับได้**
๘.	Domain Controller ไม่สามารถให้บริการได้	Resource ไม่เพียงพอ	ปรับปรุงประสิทธิภาพเครื่อง Domain Controller เช่น Upgrade RAM Hard Disk	- ตรวจสอบการทำงานของเครื่อง Domain Controller ในส่วนของอุปกรณ์ที่เป็น Resource ใช้งานในระบบว่ามีการแจ้งเตือน หรือ พบปัญหาอุปกรณ์ที่มีการ	๑	OI ๓	๓	๙	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
				ทำงานประสิทธิภาพลดลง โดยทำการตรวจสอบทุก ๓ เดือน - ปรับปรุงอุปกรณ์ที่พบปัญหาในกรณีที่ไม่สามารถเปลี่ยนแปลงได้ให้จัดหาอุปกรณ์ใหม่มาใช้งานทดแทนอุปกรณ์เดิมที่ชำรุด					
๙.	ถูกโจมตีจนไม่สามารถให้บริการได้ (Denial of Service)	กระบวนการป้องกัน Denial of Service ไม่รองรับการโจมตีในรูปแบบที่ไม้ได้มีการกำหนดไว้	- จัดหาอุปกรณ์ IDS หรือ IPS ที่รองรับการโจมตีชนิด Denial of Service ที่มีความสามารถในการ update รูปแบบต่างๆได้อย่างอัตโนมัติ	- ติดตั้งอุปกรณ์ IPS ที่รองรับการโจมตีชนิด Denial of Service (DOS) ที่มีความสามารถในการ update รูปแบบการป้องกันการโจมตีในรูปแบบต่างๆได้อย่างอัตโนมัติ - การตรวจสอบสถานะการทำงานของอุปกรณ์ IPS โดยตรวจดูประสิทธิภาพการทำงานของหน่วยประมวลผล การทำงานของหน่วยความจำ ปริมาณการตรวจจับการบุกรุกผ่านช่องทางระบบเครือข่าย (Attack) เพื่อให้อุปกรณ์อยู่ในสภาพพร้อมใช้งาน โดยตรวจเช็คเดือนละ ๑ ครั้ง	๒	OI ๑	๓	**๖**	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
				- ทำการบันทึกเป็นรายงานสถานะการทำงานประจำเดือน เพื่อเปรียบเทียบสถิติของการบุกรุก					
๑๐.	การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย	- จัดทำกระบวนการตรวจสอบการปรับปรุง Security Patch ให้ทันสมัยของเครื่อง Server โดยตั้งค่าให้ทำงานแบบอัตโนมัติ และมีการตรวจสอบทุกเดือน	- ทำการตั้งค่าการปรับปรุง Security Patch ให้ทันสมัย (Update) ของเครื่อง Server แบบอัตโนมัติ - ตรวจสอบการทำงาน ของค่าการปรับปรุง Security Patch (Update) โดยตรวจเช็คเดือนละ ๑ ครั้ง - ทำการบันทึกผลการทำงาน ค่าการปรับปรุง Security Patch (Update) ในแต่เดือน	๑	OI ๒	๓	**๖**	**รับได้**
		ไม่มีกระบวนการในการติดตามปรับปรุง Software Version	- จัดทำงบประมาณเพื่อใช้ในการปรับปรุง Software Version ให้ทันสมัยและมีการ	- ทำการตรวจสอบค่า Software Version ที่ใช้งานในปัจจุบันว่าเป็น Version ที่ทันสมัยและรองรับการปรับปรุงระบบให้มี	๒	OI ๓	๒	**๑๒**	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
		ให้ทันสมัย	ตรวจสอบเพื่อปรับปรุง Version ทุก ๑ ปี	ความปลอดภัย โดยมีการตรวจเช็คอย่างน้อยปีละ ๑ ครั้ง - ทำบันทึกค่าใช้จ่ายเพื่อใช้ในการปรับปรุง Software Version เพื่อนำเสนอกรมฯ ให้ตั้งงบประมาณการปรับปรุง Software Version ในปีถัดไป					
๑๑.	การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต (Network)	ขาดการติดตามเรื่องการถอดถอนสิทธิของพนักงานที่ลาออกหรือย้ายแผนกอย่างสม่ำเสมอ	- จัดทำแผนการทบทวนสิทธิปีละ ๒ ครั้ง	กำหนดสิทธิ์ในการเข้าถึงข้อมูลผู้ใช้งาน และผู้ดูแลระบบเทคโนโลยีสารสนเทศ ดังนี้ - เพิ่มข้อมูลการกำหนดสิทธิ์เมื่อเข้ารับราชการใหม่ - ปรับปรุงข้อมูลการกำหนดสิทธิ์เมื่อโยกย้ายตำแหน่ง หรือหน่วยงาน - ลบข้อมูลการกำหนดสิทธิ์เมื่อเกษียณอายุหรือลาออกจากราชการ	๒	OI ๑	๒	๔	**รับได้**
๑๒.	การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย	- จัดทำกระบวนการปรับปรุง Security Patch ให้ทันสมัยของซอฟต์แวร์ โดยตั้งค่าให้	- ทำการตรวจสอบค่า Security Patch ที่ใช้งานในปัจจุบันว่ามีการ update ครบถ้วน และตั้งค่าให้รองรับการ	๑	OI ๒	๒	**๔**	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
			ทำงานแบบอัตโนมัติ และมีการตรวจสอบทุกเดือน	update Security Patch แบบอัตโนมัติ โดยมีการตรวจเช็คผลการupdate เดือนละ ๑ ครั้ง - ทำการบันทึกผลการทำงานของการปรับปรุง Security Patch (Update) ในแต่เดือน เพื่อเฝ้าระวังการที่ระบบไม่ update Patch ที่สำคัญ					
๑๓.	ข้อมูลสูญหาย	ทำการสำรองข้อมูลทุกวันจัดเก็บอยู่ในระบบ NAS ไม่ได้นำออกมาเก็บไว้ที่อื่นอย่างปลอดภัย	- จัดทำการสำรองข้อมูล (Data Backup) ลงเครื่องแม่ข่ายให้บริการแบบอัตโนมัติ (Internal Media) ณ ห้องควบคุมระบบทุกวัน และทำการสำรองข้อมูล (Data Backup) ไปยังเครื่อง External Storage ทุกสัปดาห์ และนำไปเก็บไว้ที่ฝ่ายบริหารทั่วไป ศูนย์สารสนเทศ ชั้น ๒ ตึกอาคาร ๖ ชั้น	- จัดทำการสำรองข้อมูล (Data Backup) ลงเครื่องแม่ข่ายให้บริการแบบอัตโนมัติ (Internal Media) ณ ห้องควบคุมระบบทุกวัน โดยจัดเก็บข้อมูลเป็นรายเครื่องจำแนกตามวัน ได้แก่ วันจันทร์ เครื่อง LDDWEB วันอังคาร เครื่อง NLB๑ และ MordinNew วันพุธ เครื่อง NLB๔ Imail Webtime และ IRV วันพฤหัสบดี เครื่อง NLB๒ และ E-Library	๑	EI ๒	๓	๖	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
				วันศุกร์ เครื่อง TIME eOffice eOfficeData และ NHRM - วิธีการสำรองข้อมูลเป็นลักษณะ Full Backup คือทำการสำรองข้อมูลทั้งระบบ - ทำการสำรองข้อมูล (Data Backup) ไปยังเครื่อง External Storage ทุกสัปดาห์ และนำไปเก็บไว้ที่ฝ่ายบริหารทั่วไป ศูนย์สารสนเทศ ชั้น ๒ ตึกอาคาร ๖ ชั้น					
		มีการจัดเก็บข้อมูลรายเดือนเป็น Tap Backup สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก	- จัดทำการสำรองข้อมูล (Data Backup) โดยการบันทึกลงม้วนเทป (Tape Backup) ในการ Backup ณ ห้องควบคุมระบบ เดือนละ ๑ ครั้ง และเก็บไว้ ณ สพข. ๒ (ชลบุรี)	- จัดทำการสำรองข้อมูล (Data Backup) โดยการบันทึกลงม้วนเทป (Tape Backup) ในการ Backup ณ ห้องควบคุมระบบ เดือนละ ๑ ครั้ง และนำม้วนเทป (Tape Backup) ไปเก็บไว้ ณ สพข. ๒ (ชลบุรี) - ทดสอบการกู้คืนฐานข้อมูลด้วยวิธีการสุ่มจากเครื่องแม่ข่ายที่เก็บฐานข้อมูล ประกอบด้วย เครื่อง NLB๑ NLB๒ LDDWEB MordinNew E-Library NHRM Imail IRV TIME WEBTIME eOffice eOfficedata เดือนละ ๑ ครั้ง	๑	EI ๒	๓	๖	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
				- ทดสอบการกู้คืนระบบสารสนเทศที่ได้พัฒนาขึ้น โดยเมื่อเกิดความเสียหายกับเครื่องคอมพิวเตอร์ สามารถจะติดตั้งและนำระบบสารสนเทศกลับมาใช้งานได้ใหม่					
		มีการจัดเก็บข้อมูลรายไตรมาสเป็น External Hard disk สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก	- จัดทำการสำรองข้อมูล (Data Backup) โดยใช้บริการ CAT Internet Data Center (CAT-IDC) บริการคุ้มครองเก็บรักษาข้อมูลบนเซิร์ฟเวอร์ ณ บริษัทฯ CAT สาขาบางรัก ไตรมาสละ ๑ ครั้ง	- ได้จัดทำการสำรองข้อมูล (Data Backup) จากเครื่องแม่ข่ายลง External Hard disk และนำไปจัดเก็บไว้ที่ CAT Internet Data Center (CAT-IDC) บริการคุ้มครองเก็บรักษาข้อมูลบนเซิร์ฟเวอร์ ณ บริษัทฯ CAT สาขาบางรัก ไตรมาสละ ๑ ครั้ง	๑	EI ๒	๓	๖	**รับได้**
		ไม่ได้ปรับปรุงแผนการสำรองข้อมูลให้เป็นปัจจุบันอย่าง จึงทำให้ฐานข้อมูล/ระบบฯ ที่พัฒนาขึ้นใหม่ อยู่นอก	- ทบทวนแผนการสำรองข้อมูลให้เป็นปัจจุบันทุกครั้งที่มีการพัฒนาฐานข้อมูล/ระบบฯ ขึ้นใหม่	- ดำเนินการทบทวนแผนการสำรองข้อมูลทั้งทุก ๖ เดือน และปรับปรุงแผนการสำรองข้อมูลให้เป็นปัจจุบันทุกครั้งที่มีการพัฒนาฐานข้อมูล/ ระบบฯ ขึ้นใหม่	๑	EI ๒	๓	๖	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
		แผนไม่ได้ทำการสำรอง							
๑๔.	ข้อมูล mailbox สูญหาย	ระบบ Mail Service ชำรุด	- ทำการสำรองข้อมูล mailbox สัปดาห์ละ ๑ ครั้งเพื่อ restore กลับมาใช้งานเมื่อระบบ Mail Service ใหม่ติดตั้งเสร็จ	- ตั้งค่าสำรองข้อมูล (backup) mailbox สัปดาห์ละ ๑ ครั้ง โดยมีการจัดเก็บข้อมูลที่สำรองไว้ที่เครื่อง NAS - จัดเตรียมเครื่องแม่ข่ายสำรอง เพื่อใช้ทดสอบการติดตั้งระบบ Mail Service ใหม่และทดสอบการ restore ข้อมูลกลับมาใช้งานทุกๆ ๓ เดือน	๑	OI ๒	๓	๖	**รับได้**
๑๕.	เจ้าหน้าที่ Network Admin หลักไม่สามารถปฏิบัติได้	เจ้าหน้าที่ Network Admin สำรองมีทักษะไม่เท่ากับ Network Admin หลัก	- ฝึกอบรมเจ้าหน้าที่ Network Admin สำรองให้มีทักษะเทียบเท่ากับ Network Admin หลัก	- เจ้าหน้าที่ได้รับการฝึกอบรมหลักสูตร Network Admin เพื่อให้มีความรู้ทันสมัย เช่น รูปแบบการโจมตีใหม่ ๆ เครื่องมือแฮก รูปแบบใหม่ ๆ เพื่อให้ทราบถึงขีดความสามารถของเครื่องมือและการโจมตี อันตรายที่จะเกิดขึ้นกับระบบ การศึกษาการใช้งานซอฟต์แวร์ประเมินความเสี่ยงและ Tools ชนิดต่างๆ ที่ใช้ในการสแกนเพื่อหาช่องโหว่	๒	PI ๒	๓	๑๒	**รับได้**
๑๖.	เจ้าหน้าที่ Programmer	ไม่มีเจ้าหน้าที่ Programmerสำรอง	- จัดส่งเจ้าหน้าที่ไปเข้ารับการฝึกอบรมกับสถาบันที่มี	- เจ้าหน้าได้รับการฝึกอบรมหลักสูตรนักพัฒนาโปรแกรมและเว็บไซต์ เพื่อให้	๒	PI ๒	๓	๑๒	**รับได้**

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ
	ไม่สามารถปฏิบัติได้		มาตรฐาน เพื่อทำให้มี Programmer มากขึ้น	นักพัฒนาโปรแกรมและเว็บไซต์จะได้มีความรู้ในการเขียนโค้ดที่ปลอดภัยจากการโจมตีแบบต่างๆ เช่น SQL Injection, XSS: Cross Site Scripting และ Remote File Inclusion					

บทที่ ๕
สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรมหน้าที่และกระบวนการทำงานเพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด เนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกลอันทรงพลังในการขับเคลื่อนการดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลมหาสารถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้กับการปฏิบัติงานของทุกหน่วยงานภายในกรมพัฒนาที่ดิน ดังนั้น หนทางที่ดีที่สุดในการป้องกันปัญหาที่จะเกิดขึ้นด้านเทคโนโลยีสารสนเทศ จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือ การจัดการความเสี่ยงในองค์กร นั่นเอง

๕.๑ สรุป

ผลจาการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้มีการดำเนินกิจกรรมเพื่อควบคุมความเสี่ยงในแต่ละปัจจัยเสี่ยงให้ลดลงในระดับที่ยอมรับได้ คือ อยู่ในระดับความเสี่ยงต่ำกว่าค่า ARL = ๑๕ คะแนน และค่าความเสี่ยงที่ยอมรับไม่ได้ คือ ระดับความเสี่ยงที่สูงกว่า ๑๕ คะแนน สรุปได้ดังนี้

๕.๑.๑ ความเสี่ยงที่อยู่ในระดับที่ยอมรับได้ (Acceptance Risk Value : ARL) ความเสี่ยงที่มีค่าตามที่ผู้อำนวยการศูนย์สารสนเทศ กำหนดคือ ความเสี่ยงที่มีค่าอยู่ในระดับ = ๑๕ ดังนั้น กิจกรรมที่ผ่านการควบคุมความเสี่ยงมาแล้ว อยู่ในช่วง ๐-๑๕ ถือว่ายอมรับได้ ประกอบด้วย

๕.๑.๑.๑ ไฟฟ้าลัดวงจร มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ไม่มีการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network

กิจกรรในการควบคุม คือ ทบทวน “นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมพัฒนาที่ดิน” โดยเพิ่มข้อกำหนด การนำอุปกรณ์เข้าห้องควบคุมระบบจะต้องทำการตรวจสอบความต้องการกระแสไฟฟ้าของอุปกรณ์ เพื่อป้องกันไฟฟ้าลัดวงจร และกำหนดเจ้าหน้าที่รับผิดชอบ ในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออกจากห้องควบคุมระบบ Network

รายละเอียดผลดำเนินการ ได้จัดทำตารางตรวจสอบการใช้กระแสไฟฟ้าของอุปกรณ์ ทุกชิ้นก่อนติดตั้งในห้องควบคุมระบบ สรุปปริมาณกระแสไฟฟ้าที่ใช้งานอยู่ในปัจจุบันและความสามารถในการรองรับการใช้งานในอนาคตเพื่อประเมินการติดตั้งระบบไฟฟ้าเพิ่มเติมให้เพียงพอต่อความต้องการ จัดเจ้าหน้าที่ดูแลรับผิดชอบ คือ นายสุพงษ์ ไพชยนต์ และ นางวราภรณ์ อินทร์ทิพย์ ในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออก จากห้องควบคุมระบบ Network

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๑๒ คะแนน** เป็นระดับที่ยอมรับได้

๒) ไม่มีการตรวจสอบความสมบูรณ์ของอุปกรณ์ ก่อนนำเข้าห้องควบคุมระบบ Network

กิจกรรมในการควบคุม คือ กำหนดเจ้าหน้าที่รับผิดชอบ ในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออกจากห้องควบคุมระบบ Network

รายละเอียดผลดำเนินการ ได้จัดเจ้าหน้าที่ดูแลรับผิดชอบ คือ นายสุพงษ์ ไพชยนต์ และ นางวราภรณ์ อินทร์ทิพย์ ในการควบคุม ตรวจสอบการนำอุปกรณ์เข้า/ออก จากห้องควบคุมระบบ Network

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๘ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๒ ไฟฟ้าไหม้ มีช่องโหว่ที่อาจเกิดขึ้น คือ

ไม่มีการทดสอบการฉีดก๊าซจากถังดับเพลิงจริง ประกอบด้วย ถังดับเพลิงชนิดผงเคมีแห้ง (Class A และ B) และ ถังดับเพลิงชนิดก๊าซคาร์บอนได้ออกไซด์หรือ CO_2 (Class B และ C)

กิจกรรมในการควบคุม คือ ซักซ้อมและทดสอบการฉีดก๊าซจากถังดับเพลิงจริง ปีละ ๒ ครั้ง (ตามแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร IT Contingency Plan)

รายละเอียดผลดำเนินการ ได้จัดทำแผนทดสอบการทำงานของถังดับเพลิงในเดือน มีนาคม และ กันยายน ของทุกปี เพื่อประเมินประสิทธิภาพในการทำงานของอุปกรณ์ ทำการทดสอบการฉีดก๊าซจากถังดับเพลิงจริง ปีละ ๒ ครั้ง และสรุปผลการทดสอบ พร้อมทั้ง จัดทำงบประมาณรองรับการเปลี่ยนอุปกรณ์เพื่อให้อุปกรณ์พร้อมในการใช้งาน(ทุก ๕ ปี)

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๑๒ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๓ น้ำท่วม แผ่นดินไหว มีช่องโหว่ที่อาจเกิดขึ้น คือ

มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ

กิจกรรมในการควบคุม คือ จัดเตรียมสถานที่สำรองภายนอกกรมพัฒนาที่ดิน ให้พร้อมรองรับอุปกรณ์และระบบเครือข่าย ซักซ้อมความพร้อมของเจ้าหน้าที่ในการดำเนินงานตามแผนกรณีเกิดน้ำท่วม แผ่นดินไหว จลาจล ให้สามารถปฏิบัติได้ตามแผนที่กำหนดไว้ ประกอบด้วย

๑) ปิดระบบเครือข่ายทั้งหมด

๒) แผนเตรียมการและขนย้ายเครื่องแม่ข่าย โดยจัดเตรียมสถานที่เก็บเครื่องแม่ข่าย จัดทำบัญชีรายชื่อเครื่องแม่ข่ายและอุปกรณ์เครือข่าย และติดตั้งระบบ

๓) แผนการติดตั้งระบบฯ ให้กลับมาใช้เป็นปกติ

ตรวจสอบบัญชีเครื่องแม่ข่ายและอุปกรณ์เครือข่ายที่ต้องทำการขนย้ายเรียงตามลำดับความสำคัญ ตรวจสอบความพร้อมใช้ของสถานที่ ระบบไฟฟ้า และระบบเครือข่ายสำรอง ให้อยู่ในสภาพพร้อมใช้งาน

รายละเอียดผลดำเนินการ ได้จัดเตรียมแผนการปฏิบัติงานเพื่อเตรียมความพร้อมด้านการจัดการระบบสารสนเทศในภาวะที่ต้องเฝ้าระวังเป็นพิเศษและทดสอบตามแผนปีละ ๑ ครั้ง ดังนี้

๑) สถานที่บริการระบบเครือข่ายสำรอง สำนักงานพัฒนาที่ดินเขต ๑ (ปทุมธานี)

๒) วงจรบริการ Internet/Intranet ประสานงานกับ CAT เพื่อ Up Link ประมาณ ๒๐/๑๐๐ Mbps

๓) เตรียมเครื่องแม่ข่ายที่ต้องย้าย ได้แก่

๓.๑ เครื่อง Web Site กรมพัฒนาที่ดิน

๓.๒ เครื่อง Fire Wall

๓.๓ เครื่อง Mail Server

๓.๔ เครื่อง Web Site กองคลัง (ให้บริการโอนเงิน)

๓.๓ เครื่องระบบบริการประชาชน จำนวน ๒ เครื่อง

๓.๔ เครื่อง UPS สำรอง ๓K

๔) การติดตั้งระบบให้กลับมาใช้ได้เป็นปกติ

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๘ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๔ การชุมนุม จลาจล มีช่องโหว่ที่อาจเกิดขึ้น คือ

มีสถานที่สำรองภายนอกกรมพัฒนาที่ดิน แต่ไม่สามารถรองรับอุปกรณ์และระบบเครือข่ายให้เพื่อให้บริการระบบได้เต็มรูปแบบ

กิจกรรมในการควบคุม คือ จัดเตรียมสถานที่สำรองภายนอกกรมพัฒนาที่ดิน ให้พร้อมรองรับอุปกรณ์และระบบเครือข่าย ซักซ้อมความพร้อมของเจ้าหน้าที่ในการดำเนินงานตามแผนกรณีเกิดน้ำท่วม แผ่นดินไหว จลาจล ให้สามารถปฏิบัติได้ตามแผนที่กำหนดไว้ ประกอบด้วย

๑) ปิดระบบเครือข่ายทั้งหมด

๒) แผนเตรียมการและขนย้ายเครื่องแม่ข่าย โดยจัดเตรียมสถานที่เก็บเครื่องแม่ข่าย จัดทำบัญชีรายชื่อเครื่องแม่ข่ายและอุปกรณ์เครือข่าย และติดตั้งระบบ

๓) แผนการติดตั้งระบบฯ ให้กลับมาใช้เป็นปกติ

ตรวจสอบบัญชีเครื่องแม่ข่ายและอุปกรณ์เครือข่ายที่ต้องทำการขนย้ายเรียงตามลำดับความสำคัญ ตรวจสอบความพร้อมใช้ของสถานที่ ระบบไฟฟ้า และระบบเครือข่ายสำรอง ให้อยู่ในสภาพพร้อมใช้งาน

รายละเอียดผลดำเนินการ ได้จัดเตรียมแผนการปฏิบัติงานเพื่อเตรียมความพร้อมด้านการจัดการระบบสารสนเทศในภาวะที่ต้องเฝ้าระวังเป็นพิเศษ ทดสอบตามแผนปีละ ๑ ครั้ง ดังนี้

๑) สถานที่บริการระบบเครือข่ายสำรอง สำนักงานพัฒนาที่ดินเขต ๑ (ปทุมธานี)

๒) วงจรบริการ Internet/Intranet ประสานงานกับ CAT เพื่อ Up Link ประมาณ ๒๐/๑๐๐ Mbps

๓) เตรียมเครื่องแม่ข่ายที่ต้องย้าย ได้แก่

๓.๓ เครื่อง Web Site กรมพัฒนาที่ดิน

๓.๔ เครื่อง Fire Wall

๓.๓ เครื่อง Mail Server

๓.๔ เครื่อง Web Site กองคลัง (ให้บริการโอนเงิน)
๓.๕ เครื่องระบบบริการประชาชน จำนวน ๒ เครื่อง
๓.๖ เครื่อง UPS สำรอง ๓K
๔) การติดตั้งระบบให้กลับมาใช้ได้เป็นปกติ

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๘ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๕ ระบบเครือข่ายสื่อสารภายนอก (Internet) เสียหาย/ขัดข้อง มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายเฉพาะอุปกรณ์ Firewall และ Router เท่านั้น

กิจกรรในการควบคุม คือ มีการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายที่สามารถบริหารจัดการได้(Management Device) ทุกเครื่อง ที่เชื่อมต่อเข้ามากับระบบเครือข่ายของกรมพัฒนาที่ดิน

รายละเอียดผลดำเนินการ ได้จัดทำระบบการเฝ้าระวังและติดตามสถานะของระบบ (Monitoring) อุปกรณ์เครือข่ายที่สามารถบริหารจัดการได้ (Management Device) ได้แก่ Switch , Router , firewall , IPS , proxy และทำการบันทึกเป็นรายงานสถานะการเฝ้าระวังและติดตามประจำเดือน เพื่อเปรียบเทียบสถิติของการทำงานทั้งหมด

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๘ คะแนน** เป็นระดับที่ยอมรับได้

๒) ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There's no Redundant)

กิจกรรในการควบคุม คือ จัดหาอุปกรณ์เครือข่ายสำรองเพื่อนำมาทดแทนกรณีอุปกรณ์หลักเครือข่ายหลักเสียหาย

รายละเอียดผลดำเนินการ ได้สำรวจจำนวนอุปกรณ์เครือข่ายสำรองที่ต้องการทดแทน กรณีที่อุปกรณ์เครือข่ายหลักเกิดความเสียหายไม่สามารถใช้งานได้ กำหนดคุณลักษณะของอุปกรณ์เครือข่ายที่ต้องจัดหาเพื่อนำมาทดแทน ประสานงานผู้ให้บริการเครือข่ายเพื่อจัดเตรียมอุปกรณ์สำรองในกรณีที่อุปกรณ์หลักเกิดความเสียหายโดยกำหนดเป็นคุณลักษณะในสัญญา

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๘ คะแนน** เป็นระดับที่ยอมรับได้

๓) ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ

กิจกรรในการควบคุม จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ

รายละเอียดผลดำเนินการ จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ ประกอบด้วย เอกสารการกำหนดค่า Configuration อุปกรณ์เครือข่าย (Router, Switch) เอกสารกำหนดค่า Configuration เครื่องแม่ข่าย Web Server และ เอกสารกำหนดค่าConfiguration เครื่องแม่ข่าย Mail Server เป็นต้น

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๘ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๖ ระบบเครือข่ายสื่อสารภายในกรมพัฒนาที่ดินเสียหาย/ขัดข้อง มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ไม่มีอุปกรณ์ที่สามารถทำงานทดแทนได้ทันที (There's no Redundant)

กิจกรรมในการควบคุม คือ จัดหาอุปกรณ์เครือข่ายสำรองเพื่อนำมาทดแทนกรณีอุปกรณ์หลักเครือข่ายหลักเสียหาย

รายละเอียดผลดำเนินการ ได้สำรวจจำนวนอุปกรณ์เครือข่ายสำรองที่ต้องการทดแทน กรณีที่อุปกรณ์เครือข่ายหลักเกิดความเสียหายไม่สามารถใช้งานได้ กำหนดคุณลักษณะของอุปกรณ์เครือข่ายที่ต้องจัดหาเพื่อนำมาทดแทน ประสานงานผู้ให้บริการเครือข่ายเพื่อจัดเตรียมอุปกรณ์สำรองในกรณีที่อุปกรณ์หลักเกิดความเสียหายโดยกำหนดเป็นคุณลักษณะในสัญญา

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๘ คะแนน** เป็นระดับที่ยอมรับได้

๒) ขาดคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ

กิจกรรมในการควบคุม คือ จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ

รายละเอียดผลดำเนินการ ได้จัดทำคู่มือการปฏิบัติงาน (Work Instruction) ในการกู้คืนระบบ ประกอบด้วย เอกสารการกำหนดค่า Configuration อุปกรณ์เครือข่าย (Router, Switch) เอกสารกำหนดค่า Configuration เครื่องแม่ข่าย Web Server และ เอกสารกำหนดค่าConfiguration เครื่องแม่ข่าย Mail Server เป็นต้น

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๘ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๗ อุปกรณ์ Hardware ภายในห้อง ควบคุมระบบ Network ชำรุด มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ขาดแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ

กิจกรรมในการควบคุม คือ จัดทำแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ

รายละเอียดผลดำเนินการ ได้จัดทำแผนในการบริหารจัดการอุปกรณ์ Hardware ภายในห้องควบคุมระบบ ทดสอบแผนการบริหารจัดการอุปกรณ์ Hardware ที่จัดทำ ว่าเป็นไปตามวัตถุประสงค์ สรุปแผนการบริหารจัดการอุปกรณ์ Hardware หลังจากทำการทดสอบแผนทุกๆ ๓ เดือน

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๙ คะแนน** เป็นระดับที่ยอมรับได้

๒) ไม่มีอุปกรณ์สำรอง

กิจกรรมในการควบคุม จัดหาอุปกรณ์ Hardware สำรอง ได้แก่ เครื่องแม่ข่ายสำรอง ๑ เครื่อง สำหรับให้บริการ และ อุปกรณ์ Switch จำนวน ๑ เครื่อง

รายละเอียดผลดำเนินการ ติดตั้งระบบปฏิบัติการสำหรับเครื่องแม่ข่าย กำหนดค่า Configuration ให้กับอุปกรณ์ Hardware สำรอง ได้แก่ เครื่องแม่ข่ายสำรอง ๑ เครื่อง สำหรับให้บริการ อุปกรณ์ Switch จำนวน ๑ เครื่อง ตรวจสอบสถานะการทำงานของอุปกรณ์ให้พร้อมปฏิบัติงาน

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๑๒ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๘ Domain Controller ไม่สามารถให้บริการได้ มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) Resource ไม่เพียงพอ

กิจกรรในการควบคุม คือ ปรับปรุงประสิทธิภาพเครื่อง Domain Controller เช่น Upgrade RAM Hard Disk

รายละเอียดผลดำเนินการ ดำเนินการตรวจสอบการทำงานของเครื่อง Domain Controller ในส่วนของอุปกรณ์ที่เป็น Resource ใช้งานในระบบว่ามีการแจ้งเตือน หรือ พบปัญหาอุปกรณ์ที่มีการทำงานประสิทธิภาพลดลง โดยทำการตรวจสอบทุก ๓ เดือน และปรับปรุงอุปกรณ์ที่พบปัญหาในกรณีที่ไม่สามารถเปลี่ยนแปลงได้ให้จัดหาอุปกรณ์ใหม่มาใช้งานทดแทนอุปกรณ์เดิมที่ชำรุด

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน**ระดับค่า ๙ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๙ ถูกโจมตีจนไม่สามารถให้บริการได้ (Denial of Service) มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) กระบวนการป้องกัน Denial of Service ไม่รองรับการโจมตีในรูปแบบที่ไม้ได้มีการกำหนดไว้

กิจกรรในการควบคุม คือ จัดหาอุปกรณ์ IDS หรือ IPS ที่รองรับการโจมตีชนิด Denial of Service ที่มีความสามารถในการ update รูปแบบต่างๆได้อย่างอัตโนมัติ

รายละเอียดผลดำเนินการ ดำเนินการติดตั้งอุปกรณ์ IPS ที่รองรับการโจมตีชนิด Denial of Service (DOS) ที่มีความสามารถในการ update รูปแบบการป้องกันการโจมตีในรูปแบบต่างๆได้อย่างอัตโนมัติ การตรวจสอบสถานะการทำงานของอุปกรณ์ IPS โดยตรวจดูประสิทธิภาพการทำงานของหน่วยประมวลผล การทำงานของหน่วยความจำ ปริมาณการตรวจจับการบุกรุกผ่านช่องทางระบบเครือข่าย (Attack) เพื่อให้อุปกรณ์อยู่ในสภาพพร้อมใช้งาน โดยตรวจเช็คเดือนละ ๑ ครั้ง และทำการบันทึกเป็นรายงานสถานะการทำงานประจำเดือน เพื่อเปรียบเทียบสถิติของการบุกรุก

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๖ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๑๐ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย

กิจกรรในการควบคุม คือ จัดทำกระบวนการตรวจสอบการปรับปรุง Security Patch ให้ทันสมัยของเครื่อง Server โดยตั้งค่าให้ทำงานแบบอัตโนมัติ และมีการตรวจสอบทุกเดือน

รายละเอียดผลดำเนินการ ได้ทำการตั้งค่าการปรับปรุง Security Patch ให้ทันสมัย (Update) ของเครื่อง Server แบบอัตโนมัติ ตรวจสอบการทำงานของค่าการปรับปรุง Security Patch (Update) โดยตรวจเช็คเดือนละ ๑ ครั้ง และ ทำการบันทึกผลการทำงาน ค่าการปรับปรุง Security Patch (Update) ในแต่เดือน

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๖ คะแนน** เป็นระดับที่ยอมรับได้

๒) ไม่มีกระบวนการในการติดตามปรับปรุง Software Version ให้ทันสมัย

กิจกรรมในการควบคุม คือ จัดทำงบประมาณเพื่อใช้ในการปรับปรุง Software Version ให้ทันสมัยและมีการตรวจสอบเพื่อปรับปรุง Version ทุก ๑ ปี

รายละเอียดผลดำเนินการ ได้ทำการตรวจสอบค่า Software Version ที่ใช้งานในปัจจุบันว่าเป็น Version ที่ทันสมัยและรองรับการปรับปรุงระบบให้มีความปลอดภัย โดยมีการตรวจเช็คอย่างน้อยปีละ ๑ ครั้ง และ ทำบันทึกค่าใช้จ่ายเพื่อใช้ในการปรับปรุง Software Version เพื่อนำเสนอกรมฯ ให้ตั้งงบประมาณการปรับปรุง Software Version ในปีถัดไป

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๑๒ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๑๑ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต (Network) มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ขาดการติดตามเรื่องการถอดถอนสิทธิของพนักงานที่ลาออก หรือย้ายแผนกอย่างสม่ำเสมอ

กิจกรรมในการควบคุม คือ จัดทำแผนการทบทวนสิทธิปีละ ๒ ครั้ง

รายละเอียดผลดำเนินการ ได้ กำหนดสิทธิ์ในการเข้าถึงข้อมูลผู้ใช้งาน และผู้ดูแลระบบเทคโนโลยีสารสนเทศ ดังนี้

๑.๑) เพิ่มข้อมูลการกำหนดสิทธิ์เมื่อเข้ารับราชการใหม่

๑.๒) ปรับปรุงข้อมูลการกำหนดสิทธิ์เมื่อโยกย้ายตำแหน่ง หรือหน่วยงาน

๑.๓) ลบข้อมูลการกำหนดสิทธิ์เมื่อเกษียณอายุหรือลาออกจากราชการ

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๔ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๑๒ การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ไม่มีกระบวนการในการติดตามปรับปรุง Security Patch ให้ทันสมัย

กิจกรรมในการควบคุม คือ จัดทำกระบวนการปรับปรุง Security Patch ให้ทันสมัยของซอฟต์แวร์ โดยตั้งค่าให้ทำงานแบบอัตโนมัติ และมีการตรวจสอบทุกเดือน

รายละเอียดผลดำเนินการ ได้ทำการตรวจสอบค่า Security Patch ที่ใช้งานในปัจจุบันว่ามีการ update ครบถ้วน และตั้งค่าให้รองรับการ update Security Patch แบบอัตโนมัติ โดยมีการตรวจเช็คผลการupdate เดือนละ ๑ ครั้ง และ ทำการบันทึกผลการทำงานของการปรับปรุง Security Patch (Update) ในแต่เดือน เพื่อเฝ้าระวังการที่ระบบไม่ update Patch ที่สำคัญ

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๔ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๑๓ ข้อมูลสูญหาย มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ทำการสำรองข้อมูลทุกวันจัดเก็บอยู่ในระบบ NAS ไม่ได้นำออกมาเก็บไว้ที่อื่นอย่างปลอดภัย

กิจกรรในการควบคุม คือ จัดทำการสำรองข้อมูล (Data Backup) ลงเครื่องแม่ข่ายให้บริการแบบอัตโนมัติ (Internal Media) ณ ห้องควบคุมระบบทุกวัน และทำการสำรองข้อมูล (Data Backup) ไปยังเครื่อง External Storage ทุกสัปดาห์ และนำไปเก็บไว้ที่ฝ่ายบริหารทั่วไป ศูนย์สารสนเทศ ชั้น ๒ ตึกอาคาร ๖ ชั้น

รายละเอียดผลดำเนินการ จัดทำการสำรองข้อมูล (Data Backup) ลงเครื่องแม่ข่ายให้บริการแบบอัตโนมัติ (Internal Media) ณ ห้องควบคุมระบบทุกวัน โดยจัดเก็บข้อมูลเป็นรายเครื่องจำแนกตามวัน ได้แก่

วันจันทร์ เครื่อง LDDWEB
วันอังคาร เครื่อง NLB๑ และ MordinNew
วันพุธ เครื่อง NLB๔ Imail Webtime และ IRV
วันพฤหัสบดี เครื่อง NLB๒ และ E-Library
วันศุกร์ เครื่อง TIME eOffice eOfficeData และ NHRM

วิธีการสำรองข้อมูลเป็นลักษณะ Full Backup คือทำการสำรองข้อมูลทั้งระบบ ทำการสำรองข้อมูล (Data Backup) ไปยังเครื่อง External Storage ทุกสัปดาห์ และนำไปเก็บไว้ที่ฝ่ายบริหารทั่วไป ศูนย์สารสนเทศ ชั้น ๒ ตึกอาคาร ๖ ชั้น

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๖ คะแนน** เป็นระดับที่ยอมรับได้

๒) มีการจัดเก็บข้อมูลรายเดือนเป็น Tap Backup สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก

กิจกรรในการควบคุม คือ จัดทำการสำรองข้อมูล (Data Backup) โดยการบันทึกลงม้วนเทป (Tape Backup) ในการ Backup ณ ห้องควบคุมระบบ เดือนละ ๑ ครั้ง และเก็บไว้ ณ สพข. ๒ (ชลบุรี)

รายละเอียดผลดำเนินการ ได้จัดทำการสำรองข้อมูล (Data Backup) โดยการบันทึกลงม้วนเทป (Tape Backup) ในการ Backup ณ ห้องควบคุมระบบ เดือนละ ๑ ครั้ง และนำม้วนเทป (Tape Backup) ไปเก็บไว้ ณ สพข. ๒ (ชลบุรี) ทดสอบการกู้คืนฐานข้อมูลด้วยวิธีการสุ่มจากเครื่องแม่ข่ายที่เก็บฐานข้อมูล ประกอบด้วย เครื่อง NLB๑ NLB๒ LDDWEB MordinNew E-Library NHRM Imail IRV TIME WEBTIME eOffice eOfficedata เดือนละ ๑ ครั้ง และ ทดสอบการกู้คืนระบบสารสนเทศที่ได้พัฒนาขึ้น โดยเมื่อเกิดความเสียหายกับเครื่องคอมพิวเตอร์ สามารถจะติดตั้งและนำระบบสารสนเทศกลับมาใช้งานได้ใหม่

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๖ คะแนน** เป็นระดับที่ยอมรับได้

๓) มีการจัดเก็บข้อมูลรายไตรมาสเป็น External Hard disk สำรองข้อมูลไว้ในที่ปลอดภัย แต่ไม่ได้สำรองไว้ห่างจากสถานที่หลัก

กิจกรรมในการควบคุม คือ จัดทำการสำรองข้อมูล (Data Backup) โดยใช้บริการ CAT Internet Data Center (CAT-IDC) บริการคุ้มครองเก็บรักษาข้อมูลบนเซิร์ฟเวอร์ ณ บริษัทฯ CAT สาขาบางรัก ไตรมาสละ ๑ ครั้ง

รายละเอียดผลดำเนินการ ได้จัดทำการสำรองข้อมูล (Data Backup) จากเครื่องแม่ข่ายลง External Hard disk และนำไปจัดเก็บไว้ที่ CAT Internet Data Center (CAT-IDC) บริการคุ้มครองเก็บรักษาข้อมูลบนเซิร์ฟเวอร์ ณ บริษัทฯ CAT สาขาบางรัก ไตรมาสละ ๑ ครั้ง

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๖ คะแนน** เป็นระดับที่ยอมรับได้

๔) ไม่ได้ปรับปรุงแผนการสำรองข้อมูลให้เป็นปัจจุบันอย่าง จึงทำให้ฐานข้อมูล / ระบบฯ ที่พัฒนาขึ้นใหม่ อยู่นอกแผนไม่ได้ทำการสำรอง

กิจกรรมในการควบคุม คือ ทบทวนแผนการสำรองข้อมูลให้เป็นปัจจุบันทุกครั้งที่มีการพัฒนาฐานข้อมูล/ระบบฯ ขึ้นใหม่

รายละเอียดผลดำเนินการ ทบทวนแผนการสำรองข้อมูลทั้งทุก ๖ เดือน และปรับปรุงแผนการสำรองข้อมูลให้เป็นปัจจุบันทุกครั้งที่มีการพัฒนาฐานข้อมูล/ระบบฯ ขึ้นใหม่

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๖ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๑๔ ข้อมูล mailbox สูญหาย มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ระบบ Mail Service ชำรุด

กิจกรรมในการควบคุม คือ ทำการสำรองข้อมูล mailbox สัปดาห์ละ ๑ ครั้งเพื่อ restore กลับมาใช้งานเมื่อระบบ Mail Service ใหม่ติดตั้งเสร็จ

รายละเอียดผลดำเนินการ ได้ตั้งค่าสำรองข้อมูล (backup) mailbox สัปดาห์ละ ๑ ครั้ง โดยมีการจัดเก็บข้อมูลที่สำรองไว้ที่เครื่อง NAS และจัดเตรียมเครื่องแม่ข่ายสำรอง เพื่อใช้ทดสอบการติดตั้งระบบ Mail Service ใหม่และทดสอบการ restore ข้อมูลกลับมาใช้งานทุกๆ ๓ เดือน

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๖ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๑๕ เจ้าหน้าที่ Network Admin หลักไม่สามารถปฏิบัติได้ มีช่องโหว่ที่อาจเกิดขึ้นคือ

๑) เจ้าหน้าที่ Network Admin สำรองมีทักษะไม่เท่ากับ Network Admin หลัก

กิจกรรมในการควบคุม คือ ฝึกอบรมเจ้าหน้าที่ Network Admin สำรองให้มีทักษะเทียบเท่ากับ Network Admin หลัก

รายละเอียดผลดำเนินการ ฝึกอบรมเจ้าหน้าที่ Network Admin สำรองให้มีทักษะเทียบเท่ากับ Network Admin หลัก โดยส่งเจ้าหน้าที่เข้ารับการฝึกอบรมหลักสูตร Network Admin เพื่อให้มีความรู้ทันสมัย เช่น รูปแบบการโจมตีใหม่ ๆ เครื่องมือแฮก รูปแบบใหม่ ๆ เพื่อให้ทราบถึงขีดความสามารถของเครื่องมือและการโจมตี อันตรายที่จะเกิดขึ้นกับระบบ การศึกษาการใช้งานซอฟต์แวร์ประเมินความเสี่ยงและ Tools ชนิดต่างๆ ที่ใช้ในการสแกนเพื่อหาช่องโหว่

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน**ระดับค่า ๑๒ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๑.๑๖ เจ้าหน้าที่ Programmerไม่สามารถปฏิบัติได้ มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ไม่มีเจ้าหน้าที่ Programmerสำรอง

กิจกรรในการควบคุม คือ ส่งเจ้าหน้าที่ไปเข้ารับการฝึกอบรมกับสถาบันที่มีมาตรฐานเพื่อทำให้มี Programmer มากขึ้น

รายละเอียดผลดำเนินการ ส่งเจ้าหน้าที่ไปเข้ารับการฝึกอบรมกับสถาบันที่มีมาตรฐานเพื่อทำให้มี Programmer มากขึ้น เจ้าหน้าได้รับการฝึกอบรมหลักสูตรนักพัฒนาโปรแกรมและเว็บไซต์เพื่อให้นักพัฒนาโปรแกรมและเว็บไซต์จะได้มีความรู้ในการเขียนโค้ดที่ปลอดภัยจากการโจมตีแบบต่างๆ เช่น SQL Injection, XSS: Cross Site Scripting และ Remote File Inclusion

พบว่าหลักจากดำเนินการตามแผนกิจกรรมควบคุมค่าความเสี่ยงแล้ว ค่าความเสี่ยงลดลงอยู่ใน **ระดับค่า ๑๒ คะแนน** เป็นระดับที่ยอมรับได้

๕.๑.๒ ความเสี่ยงที่มีค่าสูงกว่าระดับที่ยอมรับได้ ความเสี่ยงที่มีค่าสูงกว่าระดับ ๑๕ ดังนั้น ถือว่ายอมรับไม่ได้ ประกอบด้วย

๕.๑.๒.๑ ไฟไหม้ มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ไม่มีถังดับเพลิงชนิด HCFC-๑๒๓ (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารโดยเฉพาะ

กิจกรรมในการควบคุม คือ จัดหาถังดับเพลิงชนิด HCFC-๑๒๓ (Halatron) ใช้กับสถานที่ที่ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารโดยเฉพาะ จัดทำงบประมาณเพื่อซื้อถังดับเพลิงชนิด HCFC-๑๒๓ (Halatron) จัดทำแผนทดสอบการทำงานของอุปกรณ์ถังดับเพลิงโดยฉีดก๊าซจากถังดับเพลิงจริง ปีละ ๒ ครั้ง ในเดือน มีนาคม และ กันยายน ของทุกปี เพื่อประเมินประสิทธิภาพใน และสรุปผลการทดสอบ

รายละเอียดผลดำเนินการ เนื่องจากไม่มีงบประมาณจัดซื้อ ถังดับเพลิงชนิด HCFC-๑๒๓ (Halatron) จึงทำให้ไม่สามารถปฏิบัติตามกิจกรรมในการควบคุมที่กำหนดไว้ได้ ส่งผลให้ค่าความเสี่ยงอยู่ใน **ระดับค่า ๒๐ คะแนน** เป็นระดับที่ยอมรับไม่ได้

๕.๑.๒.๒ ระบบเครือข่ายสื่อสารภายนอก (Internet) เสียหาย/ขัดข้อง มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ไม่มีระบบสื่อสารสำรองเพื่อเชื่อมต่อไปยังผู้ให้บริการเครือข่าย (ISP) รายอื่น หากระบบสื่อสารหลักมีปัญหาจะไม่สามารถให้บริการได้

กิจกรรมในการควบคุม คือ จัดหาระบบสื่อสารสำรองจาก ผู้ให้บริการเครือข่าย (ISP) โดยใช้บริการเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) หรือ ใช้บริการจาก บริษัท ทีโอที จำกัด (มหาชน) เพื่อเป็น Link สำรอง กรณีเครือข่ายหลักที่กรมพัฒนาที่ดินใช้บริการอยู่ จาก บริษัท กสท โทรคมนาคม จำกัด (มหาชน) (CAT) เสียหาย/ขัดข้อง

รายละเอียดผลดำเนินการ ตรวจสอบสถานะการทำงานของอุปกรณ์เครือข่ายหลักที่ใช้งานและอุปกรณ์เครือข่ายสำรองที่เป็นระบบ Backup โดยพิจารณาค่าการทำงานของหน่วยประมวลผล หน่วยความจำ และปริมาณการส่งผ่านข้อมูล(Packet) เข้าออกให้อยู่ในสถานะพร้อมใช้งานได้ตลอดเวลา ตรวจสอบค่ากำหนดทางด้านมาตรฐานการเชื่อมต่อเครือข่ายอุปกรณ์ให้ถูกต้องตามข้อกำหนดของกรมฯ และตรวจสอบดู Log ค่าเหตุการณ์ ต่าง ๆ ที่แสดงข้อผิดพลาดที่อาจเกิดขึ้นได้ ทดสอบการทำงานของระบบเครือข่ายหลักตามแบบการบำรุงรักษา ปีละ ๔ ครั้ง

เนื่องจากไม่สามารถจัดหาผู้ให้บริการเครือข่าย (ISP) รายอื่นได้ทันในปีงบประมาณปัจจุบัน จึงจัดทำแผนการจัดหาระบบสื่อสารสำรองจากผู้ให้บริการเครือข่าย (ISP) รายอื่นอีก ๑ วงจร ในปีงบประมาณต่อไป ส่งผลให้ค่าความเสี่ยงอยู่ใน **ระดับค่า ๒๔ คะแนน** เป็นระดับที่ยอมรับไม่ได้

๒) ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด

กิจกรรมในการควบคุม คือ มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง (ตามมาตรฐานที่ กรมพัฒนาที่ดินยอมรับได้)

รายละเอียดผลดำเนินการ ได้กำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง ในเอกสารสัญญาของผู้รับจ้าง ทำการตรวจสอบสถานะการทำงานของระบบเครือข่ายสื่อสารภายใน ว่ามีปริมาณช่วงเวลาที่ใช้งานไม่ได้จำนวนกี่ครั้ง และแต่ละครั้งที่ไม่สามารถใช้งาน จะต้องใช้เวลาในการแก้ไขให้กลับมาใช้งานได้ ไม่เกิน ๔ ชั่วโมง ตามข้อกำหนดที่ตกลงไว้ ให้ผู้รับจ้างทำการบันทึกเป็นรายงานสถานะการทำงานประจำเดือน เพื่อจัดทำสถิติของการ downtime ของระบบ

เนื่องจาก ในปัจจุบันได้กำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง และผู้รับจ้างสามารถแก้ไขปัญหาและทำการกู้คืนระบบจะให้กลับมาใช้งานได้เป็นปกติ ไม่เกิน ๔ ชั่วโมง ทำให้ค่า “ผลกระทบและความเสียหายที่เกิดขึ้นต่อระบบงาน : Operational Impact Criteria” ที่กำหนดไว้ จากระดับ ๕ ลดลงอยู่ในระดับ ๓ ส่งผลให้คะแนนค่าความเสี่ยงอยู่ใน **ระดับค่า ๑๖ คะแนน** ซึ่งสูงกว่าค่าที่กำหนด จึงเป็นระดับที่ยอมรับไม่ได้

๕.๑.๒.๓ ระบบเครือข่ายสื่อสารภายในกรมพัฒนาที่ดินเสียหาย/ขัดข้อง มีช่องโหว่ที่อาจเกิดขึ้น คือ

๑) ไม่มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่าระบบยอมรับ Downtime ได้เป็นระยะเวลาเท่าไร แต่ปัจจุบันพยายามให้น้อยที่สุด

กิจกรรมในการควบคุม คือ มีการกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง (ตามมาตรฐานที่ กรมพัฒนาที่ดินยอมรับได้)

รายละเอียดผลดำเนินการ ได้กำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง ในเอกสารสัญญาของผู้รับจ้าง ทำการตรวจสอบสถานะการทำงานของระบบเครือข่ายสื่อสารภายใน ว่ามีปริมาณช่วงเวลาที่ใช้งานไม่ได้จำนวนกี่ครั้ง และแต่ละครั้งที่ไม่สามารถใช้งาน จะต้องใช้เวลาในการแก้ไขให้กลับมาใช้งานได้ ไม่เกิน ๔ ชั่วโมง ตาม

ข้อกำหนดที่ตกลงไว้ ให้ผู้รับจ้างทำการบันทึกเป็นรายงานสถานะการทำงานประจำเดือน เพื่อจัดทำสถิติของการ downtime ของระบบ

เนื่องจาก ในปัจจุบันได้กำหนดระดับการให้บริการ (Service Level Agreement : SLA) ว่ายอมรับ Downtime ได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง และผู้รับจ้างสามารถแก้ไขปัญหาและทำการกู้คืนระบบจะให้กลับมาใช้งานได้เป็นปกติ ไม่เกิน ๔ ชั่วโมง ทำให้ค่า “ผลกระทบและความเสียหายที่เกิดขึ้นต่อระบบงาน : Operational Impact Criteria” ที่กำหนดไว้ จากระดับ ๕ ลดลงอยู่ในระดับ ๓ ส่งผลให้คะแนนค่าความเสี่ยงอยู่ใน **ระดับค่า ๑๖ คะแนน** ซึ่งสูงกว่าค่าที่กำหนด จึงเป็นระดับที่ยอมรับไม่ได้

สรุปผลการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กรมพัฒนาที่ดิน มีความเสี่ยงทั้งหมด ๑๙ รายการ เป็นความเสี่ยงที่อยู่ในระดับที่ยอมรับได้ (Acceptance Risk Value : ARL = ๑๕) จำนวน ๑๖ รายการ และเป็นความเสี่ยงที่มีค่าสูงกว่าระดับที่ยอมรับได้ (สูงกว่าค่า ARL) จำนวน ๓ รายการ

๕.๒ ข้อเสนอแนะ

๕.๒.๑ ควรมีการทบทวน/ประเมินความเสี่ยงด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กรมพัฒนาที่ดิน แผนบริหารความเสี่ยง เป็นประจำทุกปี

๕.๒.๒ ควรจัดให้มีการวิเคราะห์และประเมินความเสี่ยงที่เกิดขึ้น ทั้งภายในและภายนอกองค์กรอย่างต่อเนื่องเป็นประจำทุกปี

๕.๒.๓ ควรมีการทบทวน ภัยคุกคาม ช่องโหว่ที่อาจเกิดขึ้น ค่าโอกาสที่จะเกิด (Likelihood Criteria) ค่าผลกระทบและความเสียหายที่เกิดขึ้น (Impact Criteria) และ การกำหนดมูลค่าทรัพย์สิน (Asset Value Criteria) ให้เหมาะสมกับสถานการณ์ปัจจุบัน (ทุกปี)

๕.๒.๔ ควรทำการปรับปรุงบัญชีรายการทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูล (Information) คน (People ware) และ บริการ (Stakeholders) ให้เป็นปัจจุบัน

๕.๒.๕ การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอ เพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ

๕.๒.๖ การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

๕.๒.๖.๑ พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

๕.๒.๖.๒ พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง

๕.๒.๖.๓ กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

๕.๒.๗ การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอ เพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ

บรรณานุกรม

กรมพัฒนาที่ดิน. ๒๕๕๒. **แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน พ.ศ. ๒๕๕๒-๒๕๕๖.** กรมพัฒนาที่ดิน, กระทรวงเกษตรและสหกรณ์.

กองแผนงาน. ๒๕๕๖. **คู่มือแนวทางการจัดทำการบริหารความเสี่ยงสำหรับใช้เป็นเครื่องมือในการจัดทำการบริหารความเสี่ยง.** กรมพัฒนาที่ดิน, กระทรวงเกษตรและสหกรณ์.

จิรประภา อัครบวร และ ภูมิพร ธรรมสถิตย์เดช. ๒๕๕๒. **การบริหารความเสี่ยง Risk Management. สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานเบกษา,** กรุงเทพฯ. ๑๓๓ หน้า

ธวัชชัย ชมศิริ. ๒๕๕๓. **Computer&Network Security ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์.** โปรวิชั่น, กรุงเทพฯ. ๓๑๒ หน้า

พนิดา พานิชกุล. ๒๕๕๓. **ความมั่นคงปลอดภัยของสารสนเทศและการจัดการ (Information Security and Management).** เคทีพี, กรุงเทพฯ. ๓๖๔ หน้า

ภูริต มิตรสมหวัง. (กันยายน ๒๕๕๗). **Risk Management.** เอกสารประกอบการฝึกอบรมการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศกรมพัฒนาที่ดิน, บริษัท กสท. โทรคมนาคม จำกัด (มหาชน). กรุงเทพฯ.

ศูนย์สารสนเทศ. ๒๕๕๕. **นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมพัฒนาที่ดิน.** กรมพัฒนาที่ดิน, กระทรวงเกษตรและสหกรณ์.

สำนักบริหารการเปลี่ยนแปลงและนวัตกรรม. ๒๕๕๒. **คู่มือคำอธิบายตัวชี้วัดการพัฒนาคุณภาพการบริหารจัดการภาครัฐ ปีงบประมาณ ๒๕๕๓ สำหรับส่วนราชการระดับกรม.** สำนักงานคณะกรรมการพัฒนาระบบราชการ, กรุงเทพฯ. ๒๑๑.

หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ. ๒๕๕๐. **มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี ๒๕๕๐.** ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, กรุงเทพฯ. ๖๔ หน้า

ภาคผนวก ก

แบบฟอร์มการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กรมพัฒนาที่ดิน

ตารางภาคผนวกที่ ๑ แบบฟอร์มการระบุช่องโหว่ของภัยคุกคามตามทรัพย์สินทางเทคโนโลยีสารสนเทศ

ทรัพย์สินทางเทคโนโลยีสารสนเทศ	ภัยคุกคาม	ช่องโหว่ที่อาจเกิดขึ้น
๑. Premises (สถานที่)		
๒. Technology (เครื่องแม่ข่าย อุปกรณ์ ซอฟต์แวร์ ระบบ และการเชื่อมโยงเครือข่าย)		
๓. Information (ข้อมูล)		
๔. Supplies (ระบบสนับสนุน)		
๕. Stakeholders (ผู้รับบริการ)		
๖. People (บุคลากร)		

ตารางภาคผนวกที่ ๒ แบบฟอร์มการประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood Criteria)

ค่าคะแนน	คำอธิบาย โอกาสที่จะเกิด	ความเป็นไปได้ที่จะเกิดความเสี่ยง
๑	ยากมาก	
๒	ไม่น่าจะเป็นไปได้	
๓	น่าจะเป็นไปได้	
๔	เป็นไปได้	
๕	เกือบจะแน่นอน	

ตารางภาคผนวกที่ ๓ ผลกระทบที่จะเกิดความเสี่ยง (Impact Criteria)

ค่าคะแนน	คำอธิบาย	ผลกระทบและความเสียหายที่เกิดขึ้น .....
๑	น้อยมาก	
๒	น้อย	
๓	ปานกลาง	
๔	มาก	
๕	มากที่สุด	

ตารางภาคผนวกที่ ๔ การประเมินมูลค่าของทรัพย์สิน (Asset Value Criteria)

ระดับ	People	Premises	Technology	Information	Supplies	Stakeholders
๔						
๓						
๒						
๑						

ตารางภาคผนวกที่ ๕ แบบฟอร์มรายการทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware)

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/ รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแล จัดการฮาร์ดแวร์

ตารางภาคผนวกที่ ๖ แบบฟอร์มรายการทรัพย์สินประเภท ซอฟต์แวร์ (Software)

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	เวอร์ชั่น	ผู้พัฒนาซอฟต์แวร์	จำนวนลิขสิทธิ์	รายละเอียด ซอฟต์แวร์	ผู้รับผิดชอบ ดูแล จัดการซอฟต์แวร์

ตารางภาคผนวกที่ ๗ แบบฟอร์มรายการทรัพย์สินประเภท ข้อมูล (Information)

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อเอกสารข้อมูล/ เอกสารสนเทศ	ขนาดข้อมูล (Size)	Database (ที่ใช้)	รูปแบบที่ ให้บริการ	ระดับ ชั้นข้อมูล	สื่อบันทึกข้อมูลที่ใช้ ในการเก็บ	ที่เก็บสารสนเทศ (ชื่อสถานที่)	ระยะเวลา การจัดเก็บ	ผู้เป็น เจ้าของ สารสนเทศ

ตารางภาคผนวกที่ ๘ แบบฟอร์มรายการทรัพย์สินประเภท คน (People ware) ภายในองค์กร

รหัสพนักงาน	ชื่อ - นามสกุล	ตำแหน่ง	ส่วนงาน/ฝ่ายงาน	หน้าที่ความรับผิดชอบ	เบอร์โทรศัพท์ติดต่อ	อีเมล์

ตารางภาคผนวกที่ ๙ แบบฟอร์มรายการทรัพย์สินประเภท บริการ (Stakeholders)

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อบริการ	รายละเอียดบริการ	เจ้าของบริการ	ข้อมูลติดต่อ	ผู้ใช้บริการ	SLA

ตารางภาคผนวกที่ ๑๐ แบบฟอร์มการประเมินความเสี่ยง (Risk Assessment)

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง Risk Value	ระดับการยอมรับ

ตารางภาคผนวกที่ ๑๑ แบบฟอร์มการกำหนดมาตรการ/กิจกรรมควบคุมความเสี่ยง

ลำดับ	ทรัพย์สินทางเทคโนโลยีสารสนเทศ (Resource)	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ	การควบคุมความเสี่ยง	กิจกรรมในการควบคุม

ตารางภาคผนวกที่ ๑๒ แบบฟอร์มแผนปฏิบัติการการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	ระดับความเสี่ยง (Risk Value)	กิจกรรมในการควบคุม	หน่วยงานรับผิดชอบ	กำหนดการดำเนินการ

ตารางภาคผนวกที่ ๑๓ แบบฟอร์มการติดตามและประเมินผลการบริหารจัดการความเสี่ยง

ลำดับ	ภัยคุกคาม (Threats)	ช่องโหว่ที่อาจเกิดขึ้น (Vulnerability)	กิจกรรมในการควบคุม	รายละเอียดผลดำเนินการ	โอกาส (Likelihood)	ผลกระทบ (Impact)	ความสำคัญของทรัพย์สิน (Assets Value)	ระดับความเสี่ยง (Risk Value)	ระดับการยอมรับ

ภาคผนวก ข

รายการทรัพย์สินด้านสารสนเทศ กรมพัฒนาที่ดิน

ตารางภาคผนวกที่ ๑๔ รายการทรัพย์สินประเภท ฮาร์ดแวร์ (Hardware)

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแลจัดการฮาร์ดแวร์
ประเภทเครื่องที่ให้บริการ : Web Server							
HW-๐๐๑	NLB๑ (VM)	แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๐๑	- บริการเว็บไซต์กรมฯ	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๕๒	ชนิด Blade สำหรับ ตู้ Enclosure/	INF-๐๐๒	- เว็บไซต์กลุ่มงานตรวจสอบภายใน	(Server)		และคอมพิวเตอร์
		Chassis แบบที่ ๒	INF-๐๐๓	- เว็บไซต์กลุ่มพัฒนาระบบบริหาร	ศูนย์สารสนเทศ		
		- ยี่ห้อ : HP	INF-๐๐๔	- เว็บไซต์กองการเจ้าหน้าที่	กรมพัฒนาที่ดิน		
		- รุ่น : ProLiant BL๖๖๐c	INF-๐๐๕	- เว็บไซต์สำนักวิศวกรรมเพื่อการพัฒนา			
		Generation ๘		ที่ดิน			
		- CPU : ๘ Core ๒.๔ GHz จำนวน	INF-๐๐๖	- เว็บไซต์ศูนย์สารสนเทศ			
		๒ หน่วย	INF-๐๓๕	- ระบบบริหารครุภัณฑ์ Online			
		- RAM : ชนิด ECC DDR๓ ขนาด					
		๑๖ GB					
		- HDD : ชนิด SAS ความจุ					
		๓๐๐๐ GB จำนวน ๒ หน่วย					
HW-๐๐๒	FID (VM)	แผงวงจรเครื่องคอมพิวเตอร์	INF-๐๐๘	- เว็บไซต์กองคลัง	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๕๕	แม่ข่าย ชนิด Blade สำหรับ			(Server)		และคอมพิวเตอร์
		ตู้ Enclosure/Chassis			ศูนย์สารสนเทศ		
		แบบที่ ๒			กรมพัฒนาที่ดิน		
		- ยี่ห้อ : HP					
		- รุ่น : ProLiant BL๖๖๐c					
		Generation ๘					
		- CPU : ๘ Core ๒.๔ GHz จำนวน					
		๒ หน่วย					
		- RAM : ชนิด ECC DDR๓ ขนาด					
		๑๖ GB					
		- HDD : ชนิด SAS ความจุ					
		๓๐๐๐ GB จำนวน ๒ หน่วย					

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแลจัดการฮาร์ดแวร์
ประเภทเครื่องที่ให้บริการ : Web Application Server							
HW-๐๐๓	SQL (VM)	แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๓๙	- ระบบ e-Search LDD	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๕๓	ชนิด Blade สำหรับ ตู้ Enclosure/	INF-๐๒๔	- โปรแกรมระบบบริการประชาชน	(Server)		และคอมพิวเตอร์
		Chassis แบบที่ ๒	INF-๐๒๘	- ฐานข้อมูลแหล่งน้ำขนาดเล็ก	ศูนย์สารสนเทศ		
		- ยี่ห้อ : HP			กรมพัฒนาที่ดิน		
		- รุ่น : ProLiant BL๖๖๐c					
		Generation ๘					
		- CPU : ๘ Core ๒.๔ GHz จำนวน					
		๒ หน่วย					
		- RAM : ชนิด ECC DDR๓ ขนาด					
		๑๖ GB					
		- HDD : ชนิด SAS ความจุ					
		๓๐๐๐ GB จำนวน ๒ หน่วย					
HW-๐๐๔	Sim-Farm	แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย		- ระบบ Sim-Farm	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๕๖	ชนิด Blade สำหรับ ตู้ Enclosure/			(Server)		และคอมพิวเตอร์
		Chassis แบบที่ ๒			ศูนย์สารสนเทศ		
		- ยี่ห้อ : HP			กรมพัฒนาที่ดิน		
		- รุ่น : ProLiant BL๖๖๐c					
		Generation ๘					
		- CPU : ๘ Core ๒.๔ GHz จำนวน					
		๒ หน่วย					
		- RAM : ชนิด ECC DDR๓ ขนาด					
		๑๖ GB					
		- HDD : ชนิด SAS ความจุ					
		๓๐๐๐ GB จำนวน ๒ หน่วย					

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแล จัดการฮาร์ดแวร์
HW-๐๐๕	LDDMAPSERVER	เครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๒๖	- โปรแกรมบันทึก Stock วัสดุการเกษตร	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	(VM)	**- ยี่ห้อ :** HP	INF-๐๒๗	- โปรแกรมรายงานผลวิเคราะห์ตัวอย่าง	(Server)		และคอมพิวเตอร์
	IP : ๑๐.๑.๑.๑๙๙	**- รุ่น :** Proliant DL๑๖๐		ดิน น้ำ ปุ๋ย	ศูนย์สารสนเทศ		
		- CPU : Xeon ๒.๖๗ GNz			กรมพัฒนาที่ดิน		
		- RAM : ๓๒ GB					
		- HDD : ๑๖ TB					
ประเภทเครื่องที่ให้บริการ : GIS Server							
HW-๐๐๖	GisWater (VM)	แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๔๐	- ระบบบริหารจัดการฐานข้อมูลแหล่งน้ำ	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๕๑	ชนิด Blade สำหรับ ตู้ Enclosure/		ขนาดเล็ก	(Server)		และคอมพิวเตอร์
		Chassis แบบที่ ๒			ศูนย์สารสนเทศ		
		- ยี่ห้อ : HP			กรมพัฒนาที่ดิน		
		- รุ่น : ProLiant BL๖๖๐c					
		Generation ๘					
		- CPU : ๘ Core ๒.๔ GHz จำนวน					
		๒ หน่วย					
		- RAM : ชนิด ECC DDR๓ ขนาด					
		๑๖ GB					
		- HDD : ชนิด SAS ความจุ					
		๓๐๐๐ GB จำนวน ๒ หน่วย					
HW-๐๐๗	EIS_Database	เครื่องคอมพิวเตอร์แม่ข่ายสำหรับ		Databse ระบบ EIS จำนวน ๘ ระบบ	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	Server	Database	INF-๐๑๖	๑. ระบบเตือนภัยธรรมชาติ (Natural	(Server)		และคอมพิวเตอร์
	IP : ๑๐.๑.๑.๑๒๔	**- ยี่ห้อ :** HP		Disasters Warning)	ศูนย์สารสนเทศ		
		- รุ่น : ProLiant ML๓๕๐ G๖ และ	INF-๐๑๗	๒. ระบบบันทึกตำแหน่งเกิดเหตุผ่าน	กรมพัฒนาที่ดิน		
		D๒๖๐๐ Disk Enclosure		โทรศัพท์มือถือ (Mobile)			

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแลจัดการฮาร์ดแวร์
		- CPU : ชนิด Six-Core Intel®	INF-๐๑๘	๓. ระบบตรวจสอบการใช้ประโยชน์ที่ดิน			
		Xeon® X๕๖๕๐ มีความเร็ว		(Present Land Use Monitoring)			
		๒.๖๖ GHz, ๑๒MB L๓	INF-๐๑๙	๔. ระบบบริหารและติดตามโครงการปลูก			
		Cache จำนวน ๑ CPU		หญ้าแฝก (Vetiver Grass Tracking)			
		- RAM : ชนิด DDR๓ ๑๖ GB	INF-๐๒๐	๕. ระบบนำเสนอแผนที่ชุดดิน (Soil Series)			
		- HDD : ชนิด SATA Hot Plug		มาตราส่วน ๑ : ๒๕,๐๐๐			
		ขนาดความจุ ๒TB จำนวน	INF-๐๒๑	๖. ระบบบริหารจัดการข้อมูลเกษตรใช้สาร			
		๘ ลูก		อินทรีย์ลดใช้สารเคมีทางการเกษตร/			
				เกษตรอินทรีย์			
			INF-๐๒๒	๗. ระบบบริหารจัดการข้อมูลโรงงานผลิต			
				ปุ๋ยอินทรีย์			
			INF-๐๒๓	๘. ระบบฐานข้อมูลแหล่งน้ำในไร่นานอก			
				เขตชลประทาน เพื่อการบริหารจัดการ			
				ในเชิงพื้นที่			
HW-๐๐๘	EIS_Web/Map	เครื่องคอมพิวเตอร์แม่ข่ายสำหรับ		ให้บริการระบบ EIS จำนวน ๘ ระบบ	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	Server (VM)	Web/Map	INF-๐๑๖	๑. ระบบเตือนภัยธรรมชาติ (Natural	(Server)		และคอมพิวเตอร์
	IP : ๑๐.๑.๑.๑๒๐	**- ยี่ห้อ :** HP		Disasters Warning)	ศูนย์สารสนเทศ		
		- รุ่น : ProLiant ML๓๕๐ G๖	INF-๐๑๗	๒. ระบบบันทึกตำแหน่งเกิดเหตุผ่าน	กรมพัฒนาที่ดิน		
		- CPU : ชนิด Six-Core Intel®		โทรศัพท์มือถือ (Mobile)			
		Xeon® X๕๖๕๐ มีความเร็ว	INF-๐๑๘	๓. ระบบตรวจสอบการใช้ประโยชน์ที่ดิน			
		๒.๖๖ GHz, ๑๒MB L๓		(Present Land Use Monitoring)			
		Cache จำนวน ๒ CPU	INF-๐๑๙	๔. ระบบบริหารและติดตามโครงการปลูก			
		- RAM : ชนิด DDR๓ ๑๖ GB		หญ้าแฝก (Vetiver Grass Tracking)			
		- HDD : ชนิด SATA Hot Plug	INF-๐๒๐	๕. ระบบนำเสนอแผนที่ชุดดิน (Soil Series)			
		ขนาดความจุ ๒TB จำนวน		มาตราส่วน ๑ : ๒๕,๐๐๐			
		๘ ลูก	INF-๐๒๑	๖. ระบบบริหารจัดการข้อมูลเกษตรใช้สาร			
				อินทรีย์ลดใช้สารเคมีทางการเกษตร/			
				เกษตรอินทรีย์			

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแล จัดการฮาร์ดแวร์
			INF-๐๒๒	๗. ระบบบริหารจัดการข้อมูลโรงงานผลิต			
				ปุ๋ยอินทรีย์			
			INF-๐๒๓	๘. ระบบฐานข้อมูลแหล่งน้ำในไร่นานอก			
				เขตชลประทาน เพื่อการบริหารจัดการ			
				ในเชิงพื้นที่			
ประเภทเครื่องที่ให้บริการ : e-Service Server							
HW-๐๐๙	NLB๒ (VM)	แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๓๓	- ระบบการประชุมอิเล็กทรอนิกส์	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๓๑	ชนิด Blade สำหรับ ตู้ Enclosure/		(e-Meeting)	(Server)		และคอมพิวเตอร์
		Chassis แบบที่ ๑	INF-๐๓๖	- ระบบบริหารครุภัณฑ์ต่ำกว่าเกณฑ์	ศูนย์สารสนเทศ		
		- ยี่ห้อ : HP			กรมพัฒนาที่ดิน		
		- รุ่น : ProLiant BL๔๖๐c					
		Generation ๘					
		- CPU : ๖ Core ๒.๕ GHz จำนวน					
		๑ หน่วย					
		- RAM : ชนิด ECC DDR๓ ขนาด					
		๘ GB					
		- HDD : ชนิด SAS ความจุ ๓๐๐ GB					
		จำนวน ๒ หน่วย					
HW-๐๑๐	TIME	เครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๔๑	- ระบบลงเวลาทำงาน	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๑๖	**- ยี่ห้อ :** IBM			(Server)		และคอมพิวเตอร์
		- รุ่น : Xseries ๒๒๖			ศูนย์สารสนเทศ		
		- CPU : Xeon ๒.๘ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๑ GB					
		- HDD : ๓๗.๒๖ GB					

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแล จัดการฮาร์ดแวร์
HW-๐๑๑	Webtime	เครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๓๗	- ระบบตรวจสอบเวลาการทำงาน	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๕	**- ยี่ห้อ :** Mission		ผ่าน Web	(Server)		และคอมพิวเตอร์
		- รุ่น :			ศูนย์สารสนเทศ		
		- CPU : Pentium๔ ๓.๐ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๑ GB					
		- HDD : ๑๒๐ GB					
HW-๐๑๒	Security	เครื่องคอมพิวเตอร์แม่ข่าย		- ระบบ Security	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๘	**- ยี่ห้อ :** HP			(Server)		และคอมพิวเตอร์
		- รุ่น : A๑๒๕๐๑			ศูนย์สารสนเทศ		
		- CPU : Pentium๔ ๓.๐๖ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๕๑๒ MB					
		- HDD : ๘๐ GB					
HW-๐๑๓	Broadcast (VM)	เครื่องคอมพิวเตอร์แม่ข่าย		- ระบบถ่ายทอดสดการประชุมผ่าน	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๑๙๙	**- ยี่ห้อ :** HP		เครือข่ายอินเตอร์เน็ต (Broadcast	(Server)		และคอมพิวเตอร์
		- รุ่น : Proliant DL๑๖๐		Streaming System)	ศูนย์สารสนเทศ		
		- CPU : Xeon ๒.๖๗ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๓๒ GB					
		- HDD : ๑๖ TB					
ประเภทเครื่องที่ให้บริการ : Mail Server							
HW-๐๑๔	LDDMAIL	เครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๔๒	- ระบบจดหมายอิเล็กทรอนิกส์ไปรษณีย์	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๓	**- ยี่ห้อ :** Dell		พด. LDD Mail (ระบบใหม่)	(Server)		และคอมพิวเตอร์
		- รุ่น : Power edge R๓๒๐			ศูนย์สารสนเทศ		
		- CPU : Xeon ๒.๔ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๑๖ GB					
		- HDD : ๑ TB					

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแลจัดการฮาร์ดแวร์
ประเภทเครื่องที่ให้บริการ : e-Office Server							
HW-๐๑๕	LDDWEB	เครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๓๔	- ระบบสารบรรณอิเล็กทรอนิกส์	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๑๓	**- ยี่ห้อ :** IBM			(Server)		และคอมพิวเตอร์
		- รุ่น : Xseries ๒๓๖			ศูนย์สารสนเทศ		
		- CPU : Xeon ๒.๘ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๒.๕ GB					
		- HDD : ๔๘.๘๓ GB					
HW-๐๑๖	eOffice	เครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๓๘	- ระบบสำนักงานอิเล็กทรอนิกส์	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๑๙๐	**- ยี่ห้อ :** Fujitsu		(e-Office)	(Server)		และคอมพิวเตอร์
		- รุ่น :			ศูนย์สารสนเทศ		
		- CPU : Xeon ๓.๒ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๒ GB					
		- HDD : ๑๔๖ GB					
HW-๐๑๗	eOfficedata	เครื่องคอมพิวเตอร์แม่ข่าย	INF-๐๓๘	- ระบบสำนักงานอิเล็กทรอนิกส์	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๑๙๓	**- ยี่ห้อ :** HP		(e-Office) (Database)	(Server)		และคอมพิวเตอร์
		- รุ่น : ML๓๗๐ G๕			ศูนย์สารสนเทศ		
		- CPU : Xeon ๒.๓๓ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๒ GB					
		- HDD : ๒๗๓.๔๐ GB					
ประเภทเครื่องที่ให้บริการ : Storage Server							
HW-๐๑๘	NAS	เครื่องคอมพิวเตอร์แม่ข่าย		- จัดเก็บข้อมูล Network Attach	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๙๑.๑๑	**- ยี่ห้อ :**		Storage System	(Server)		และคอมพิวเตอร์
		- รุ่น : Storage Flex			ศูนย์สารสนเทศ		
		- CPU : Xeon ๒.๘ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๑ GB					
		- HDD : ๘ TB					

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแลจัดการฮาร์ดแวร์
ประเภทเครื่องที่ให้บริการ : Domain Server							
HW-๐๑๙	BDC๑	เครื่องคอมพิวเตอร์แม่ข่าย		- ระบบ Domain Controller Service	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๔๑	**- ยี่ห้อ :** Gateway			(Server)		และคอมพิวเตอร์
		- รุ่น : ALR๗๐๐๐			ศูนย์สารสนเทศ		
		- CPU : Pentium๒ ๒.๐ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๓๒๐ MB					
		- HDD : ๘ GB					
HW-๐๒๐	PDC๑	เครื่องคอมพิวเตอร์แม่ข่าย		- ระบบ Backup Domain Controller	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๖๘	**- ยี่ห้อ :** IBM		Service	(Server)		และคอมพิวเตอร์
		- รุ่น : Think centre			ศูนย์สารสนเทศ		
		- CPU : Pentium๔ ๓.๐ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๒๕๖ MB					
		- HDD : ๔๐ GB					
ประเภทเครื่องที่ให้บริการ : Log Server							
HW-๐๒๑	Log	เครื่องคอมพิวเตอร์แม่ข่าย		- ระบบ Device Logs Service	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๑๖๖	**- ยี่ห้อ :** HP			(Server)		และคอมพิวเตอร์
		- รุ่น : Proliant ML ๓๓๐			ศูนย์สารสนเทศ		
		- CPU : Xeon ๒.๘ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๕๑๒ MB					
		- HDD : ๓๗.๒๗ GB					
ประเภทเครื่องที่ให้บริการ : Netservice Server							
HW-๐๒๒	ACS	เครื่องคอมพิวเตอร์แม่ข่าย		- ระบบ ACS ควบคุมการใช้งานอุปกรณ์	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๙๙	**- ยี่ห้อ :** IBM		เครือข่าย	(Server)		และคอมพิวเตอร์
		- รุ่น : X series ๒๓๖			ศูนย์สารสนเทศ		
		- CPU : Intel Xeon ๒.๘ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๑ GB					
		- HDD : ๘๐ GB					

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแล จัดการฮาร์ดแวร์
HW-๐๒๓	Proxy	เครื่องคอมพิวเตอร์แม่ข่าย		- ระบบ Proxy	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๒	**- ยี่ห้อ :** Dell			(Server)		และคอมพิวเตอร์
		- รุ่น : Power Edge ๒๙๐๐			ศูนย์สารสนเทศ		
		- CPU : Intel Xeon ๑.๘๖ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๒ GB					
		- HDD : ๓๐๐ GB					
HW-๐๒๔	Firewall	เครื่องคอมพิวเตอร์แม่ข่าย		- ระบบ Firewall	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๑๕	**- ยี่ห้อ :** Dell			(Server)		และคอมพิวเตอร์
		- รุ่น : Power Edge ๒๙๐๐			ศูนย์สารสนเทศ		
		- CPU : Intel Xeon ๑.๘๖ GHz			กรมพัฒนาที่ดิน		
		- RAM : ๑ GB					
		- HDD : ๓๐๐ GB					
HW-๐๒๕	DNS	เครื่องคอมพิวเตอร์แม่ข่าย		- ระบบ DNS	ห้องควบคุมระบบ	๑	กลุ่มระบบเครือข่าย
	IP : ๑๐.๑.๑.๔	**- ยี่ห้อ :** Commaq			(Server)		และคอมพิวเตอร์
		- รุ่น : ML๓๕๐			ศูนย์สารสนเทศ		
		- CPU : Intel x๘๖ Family๖			กรมพัฒนาที่ดิน		
		- RAM : ๒๕๖ MB					
		- HDD : ๒๐ GB					
HW-๐๒๖		เครื่องคอมพิวเตอร์ลูกข่าย			ส่วนกลางและ	๑,๖๔๒	กลุ่มระบบเครือข่าย
					ส่วนภูมิภาค		และคอมพิวเตอร์
อุปกรณ์ ATM							
NET-๐๐๑	ATM Core Router ๔๕๐๐	Cisco ๔๕๐๐		- อุปกรณ์กำหนดเส้นทางเครือข่ายชนิด ATM	ศูนย์สารสนเทศ	๑	กลุ่มระบบเครือข่าย
							และคอมพิวเตอร์
NET-๐๐๒	ATM Core Switch ๕๐๐๐	Cisco ๕๐๐๐		- อุปกรณ์กระจายสัญญาณเครือข่ายชนิด ATM	ศูนย์สารสนเทศ	๒	"
NET-๐๐๓	ATM LightStream ๑๐๑๐	Cisco ๑๐๑๐		- อุปกรณ์เชื่อมสัญญาณเครือข่ายชนิด ATM	ศูนย์สารสนเทศ	๒	"

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแล จัดการฮาร์ดแวร์
อุปกรณ์ Switch							
NET-๐๐๔	Gigagit Core Switch	Cisco ๖๕๐๖		- อุปกรณ์เครือข่ายหลักชนิด Gigagit	ศูนย์สารสนเทศ	๕	กลุ่มระบบเครือข่าย
		รุ่น ๓๗๐๐ และ รุ่น ๖๕๐๐					และคอมพิวเตอร์
NET-๐๐๕	Gigabit Distributed Switch	Cisco ๒๙๖๐		- อุปกรณ์กระจายสัญญาณเครือข่ายชนิด Gigagit	ศูนย์สารสนเทศ	๔	"
		รุ่น ๒๙๖๐					
NET-๐๐๖	Fast Ethernet Access	Cisco ๒๙๕๐		- อุปกรณ์เชื่อมสัญญาณเครือข่ายชนิด Fast	ศูนย์สารสนเทศ	๑๑	"
	Switch Managed ๒๙๕๐			Ethernet			
NET-๐๐๗	Fast Ethernet Access	๓COM		- อุปกรณ์เชื่อมสัญญาณเครือข่ายชนิด Fast	ศูนย์สารสนเทศ	๖	"
	Switch Unmanaged			Ethernet			
NET-๐๐๘	Gigabit Edge Switch	Cisco ๒๙๖๐		- อุปกรณ์กระจายสัญญาณเครือข่ายชนิด	ส่วนภูมิภาค	๑๕	"
	Managed ๒๙๖๐			Gigagit			
NET-๐๐๙	Fast Ethernet Switch	SMC		- อุปกรณ์เชื่อมสัญญาณเครือข่ายชนิด Fast	ส่วนภูมิภาค	๑๐๙	"
	Unmanaged			Ethernet			
อุปกรณ์ Access Point							
NET-๐๑๐	Access Point	Cisco ๑๒๕๐		- อุปกรณ์เชื่อมสัญญาณเครือข่ายชนิดไร้สาย	ศูนย์สารสนเทศ/	๓๐	กลุ่มระบบเครือข่าย
					ส่วนภูมิภาค		และคอมพิวเตอร์
อุปกรณ์ Router							
NET-๐๑๑	Router	Cisco		- อุปกรณ์กำหนดเส้นทางเครือข่าย	ศูนย์สารสนเทศ	๓	กลุ่มระบบเครือข่าย
		รุ่น ๓๖๐๐ , รุ่น ๓๗๐๐					และคอมพิวเตอร์
		และ รุ่น ๗๒๐๐					
NET-๐๑๒	Router	Cisco		- อุปกรณ์กำหนดเส้นทางเครือข่าย	ส่วนภูมิภาค	๑๐๙	"
		รุ่น ๑๘๐๐ และ รุ่น ๒๘๐๐					

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเครื่องให้บริการ/รายการอุปกรณ์	ยี่ห้อ/รุ่น/Spec.	Reference ID	ลักษณะการใช้งาน/ระบบงาน	ที่ตั้ง	จำนวน (เครื่อง)	ผู้รับผิดชอบ ดูแล จัดการฮาร์ดแวร์
อุปกรณ์ Firewall							
NET-๐๑๓	Firewall Device	Cisco		- อุปกรณ์ป้องกันการบุกรุกเครือข่าย	ศูนย์สารสนเทศ	๑	กลุ่มระบบเครือข่าย
		รุ่น ASA ๕๕๐๐					และคอมพิวเตอร์
อุปกรณ์ รักษาความปลอดภัยห้องควบคุมระบบ							
NET-๐๑๔	Finger Scan	ZKT eco		- อุปกรณ์ป้องกันการผ่านเข้าออกห้องด้วย	ศูนย์สารสนเทศ	๑	กลุ่มระบบเครือข่าย
		รุ่น iClock		ระบบสแกนลายนิ้วมือ			และคอมพิวเตอร์
NET-๐๑๕	กล้อง CCTV	IR Bullet Camera		- อุปกรณ์กล้องวีดีโอ CCTV ติดตามผู้บุกรุก	ศูนย์สารสนเทศ	๒	กลุ่มระบบเครือข่าย
		รุ่น HP-๙๕๑๑DIR		ผ่านเครือข่ายอินเตอร์เน็ต			และคอมพิวเตอร์
อุปกรณ์ เครื่องปรับอากาศห้องควบคุมระบบ Network							
NET-๐๑๖	เครื่องปรับอากาศ	Unimaster		- อุปกรณ์เครื่องปรับอากาศห้องควบคุม	ศูนย์สารสนเทศ	๒	กลุ่มระบบเครือข่าย
				ระบบ Network			และคอมพิวเตอร์
NET-๐๑๗	เครื่องปรับอากาศ	Central Air		- อุปกรณ์เครื่องปรับอากาศห้องควบคุม	ศูนย์สารสนเทศ	๑	กลุ่มระบบเครือข่าย
				ระบบ Network			และคอมพิวเตอร์
NET-๐๑๘	เครื่องปรับอากาศ	Fujibishi		- อุปกรณ์เครื่องปรับอากาศห้องควบคุม	ศูนย์สารสนเทศ	๑	กลุ่มระบบเครือข่าย
				ระบบ Network			และคอมพิวเตอร์
อุปกรณ์ เครื่องสำรองไฟฟ้า							
NET-๐๑๗	เครื่องสำรองไฟฟ้า	Sydome		- อุปกรณ์เครื่องสำรองไฟฟ้าระบบเครือข่าย	ศูนย์สารสนเทศ	๕	กลุ่มระบบเครือข่าย
							และคอมพิวเตอร์
NET-๐๑๘	เครื่องสำรองไฟฟ้า	Victron		- อุปกรณ์เครื่องสำรองไฟฟ้าระบบเครือข่าย	ศูนย์สารสนเทศ	๒	กลุ่มระบบเครือข่าย
							และคอมพิวเตอร์

ตารางภาคผนวกที่ ๑๕ รายการทรัพย์สินประเภท ซอฟต์แวร์ (Software)

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	เวอร์ชั่น	ผู้พัฒนาซอฟต์แวร์	จำนวนลิขสิทธิ์	รายละเอียด ซอฟต์แวร์	ผู้รับผิดชอบ ดูแล จัดการซอฟต์แวร์
	๑. ซอฟท์แวร์ระบบปฏิบัติการ					
	(Operating System : OS)					
SW-๐๐๑	Windows Server	๒๐๐๐	บริษัท ไมโครซอฟท์	๒	Operation System	กลุ่มระบบเครือข่ายและ
			(ประเทศไทย) จำกัด			คอมพิวเตอร์
SW-๐๐๒	Windows Server	๒๐๐๓	"	๑๐	"	"
SW-๐๐๓	Windows Server	๒๐๐๘	"	๕	"	"
SW-๐๐๔	Windows Server	๒๐๑๒	"	๖	"	"
SW-๐๐๕	Windows	๗	"	๒๐๐	"	"
	๒. ซอฟท์แวร์สำเร็จรูป					
SW-๐๐๖	Microsoft Office	๒๐๑๐	บริษัท ไมโครซอฟท์	๔๐	ซอฟท์แวร์สำหรับโปรแกรมสำนักงาน	กลุ่มระบบเครือข่ายและ
			(ประเทศไทย) จำกัด			คอมพิวเตอร์
SW-๐๐๗	NOD๓๒	ESET ENDPOINT	บริษัท ESET	๑	ซอฟท์แวร์สำหรับป้องกันไวรัส	"
		SECURITY	ประเทศไทย			
SW-๐๐๘	SQL Server	๒๐๐๐, ๒๐๐๕,	บริษัท ไมโครซอฟท์	๑, ๑, ๒	ซอฟท์แวร์สำหรับบริหารจัดการ	"
		๒๐๐๘	(ประเทศไทย) จำกัด		ฐานข้อมูล	
SW-๐๐๙	Oracle	๑๐	บริษัท ออราเคิล	๑	ซอฟท์แวร์สำหรับบริหารจัดการ	"
			คอปอร์เรชั่น		ฐานข้อมูล	

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	เวอร์ชั่น	ผู้พัฒนาซอฟต์แวร์	จำนวนลิขสิทธิ์	รายละเอียด ซอฟต์แวร์	ผู้รับผิดชอบ ดูแล จัดการซอฟต์แวร์
SW-๐๑๐	ArcGIS	๙.๒	บริษัท อีเอสอาร์ไอ	๑	ซอฟท์แวร์สำหรับโปรแกรมจัดการ	กลุ่มระบบเครือข่ายและ
			(ประเทศไทย) จำกัด		ข้อมูลสารสนเทศทางภูมิศาสตร์	คอมพิวเตอร์
SW-๐๑๑	ArcGIS Server Standard	๑๐	"	๑	ซอฟท์แวร์โปรแกรมจัดการและจัดเก็บ	"
	Enterprise				ข้อมูลสารสนเทศทางภูมิศาสตร์ผ่าน	
					ระบบฐานข้อมูลเชิงสัมพันธ์ RDBMS	
					และเผยแพร่ข้อมูลสารสนเทศทาง	
					ภูมิศาสตร์ (GIS) ผ่านระบบเครือข่าย	
SW-๐๑๒	ArcEditor	๑๐	"	๔	โปรแกรมจัดการข้อมูลสารสนเทศ	"
					ทางภูมิศาสตร์ (GIS) ผ่านระบบ	
					ฐานข้อมูลเชิงสัมพันธ์ RDBMS	
SW-๐๑๓	Arc Spatial Analyst	-	"	๑	โปรแกรมสำหรับการวิเคราะห์เชิง	"
					พื้นที่ (Spatial Analyst)	
SW-๐๑๔	Arc ๓D Analyst	-	"	๑	โปรแกรมสำหรับการแสดงผลข้อมูล	"
					ภูมิสารสนเทศแบบ ๓ มิติ (๓D	
					Analyst)	

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	เวอร์ชั่น	ผู้พัฒนาซอฟต์แวร์	จำนวนลิขสิทธิ์	รายละเอียด ซอฟต์แวร์	ผู้รับผิดชอบ ดูแล จัดการซอฟต์แวร์
	๓. ซอฟท์แวร์ประยุกต์					
	๓.๑ ซอฟท์แวร์ประยุกต์					
	ด้าน GIS					
SW-๐๑๕	ระบบเตือนภัยธรรมชาติ	-	กลุ่มบริษัทธุรกิจค้าร่วม	๑	โปรแกรมสำหรับการบริหารจัดการ	กลุ่มระบบภูมิสารสนเทศ
	(Natural Disasters Warning)		บริษัท อีเอสอาร์ไอ		การแจ้งเหตุเมื่อเกิดภัยธรรมชาติ	
			(ประเทศไทย) จำกัด และ		ช่วยในการสนับสนุนข้อมูลด้านต่าง ๆ	
			บริษัท แพกซ์ ไอที จำกัด		สำหรับการตัดสินใจของผู้บริหาร ใน	
					การปฏิบัติการด้านเหตุวิกฤติภัยธรรม	
					ชาติของกรมพัฒนาที่ดิน	
SW-๐๑๖	ระบบบันทึกตำแหน่งเกิดเหตุผ่าน	-	"	๑	โปรแกรมสำหรับให้ประชาชนหรือผู้	"
	โทรศัพท์มือถือ (Mobile)				ประสบเหตุ สามารถแจ้งเหตุผ่าน	
					โทรศัพท์มือถือเข้ามายังระบบได้ทันที	
SW-๐๑๗	ระบบตรวจสอบการใช้ประโยชน์	-	"	๑	โปรแกรมสำหรับใช้ในการตรวจสอบ	"
	ที่ดิน (Present Land Use				การใช้ประโยชน์ที่ดินและรายงานการ	
	Monitoring)				ใช้ประโยชน์ที่ดิน	
SW-๐๑๘	ระบบบริหารและติดตามโครง	-	"	๑	โปรแกรมสำหรับใช้ในการตรวจสอบ	"
	การปลูกหญ้าแฝก (Vetiver				บริหารและติดตามโครงการปลูกหญ้า	
	Grass Tracking)				แฝก	
SW-๐๑๙	ระบบนำเสนอแผนที่ชุดดิน	-	"	๑	โปรแกรมสำหรับนำเสนอข้อมูลชุดดิน	"
	(Soil Series) มาตราส่วน				และกลุ่มชุดดินในประเทศไทย	
	๑ : ๒๕,๐๐๐					

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	เวอร์ชั่น	ผู้พัฒนาซอฟต์แวร์	จำนวนลิขสิทธิ์	รายละเอียด ซอฟต์แวร์	ผู้รับผิดชอบ ดูแล จัดการซอฟต์แวร์
SW-๐๒๐	ระบบบริหารจัดการข้อมูลเกษตร	-	กลุ่มบริษัทธุรกิจค้าร่วม	๑	โปรแกรมสำหรับนำเสนอข้อมูลในรูป	กลุ่มระบบภูมิสารสนเทศ
	ใช้สารอินทรีย์ลดใช้สารเคมีทาง		บริษัท อีเอสอาร์ไอ		แบบเชิงพื้นที่ของระบบภูมิสารสนเทศ	
	การเกษตร/เกษตรอินทรีย์		(ประเทศไทย) จำกัด และ		การบริหารจัดการและส่งเสริมข้อมูล	
			บริษัท แพกซ์ ไอที จำกัด		เกษตร ในการใช้สารอินทรีย์ลดใช้สาร	
					เคมีทางการเกษตร/เกษตรอินทรีย์	
SW-๐๒๑	ระบบบริหารจัดการข้อมูล	-	"	๑	โปรแกรมสำหรับนำเสนอข้อมูลในรูป	"
	โรงงานผลิตปุ๋ยอินทรีย์				แบบเชิงพื้นที่ของระบบภูมิสารสนเทศ	
					ประกอบด้วย ข้อมูลโรงงาน รายละเอียด	
					กิจกรรมการผลิตและการตลาด	
SW-๐๒๒	ระบบฐานข้อมูลแหล่งน้ำในไร่นา	-	บริษัท ดาต้า มายนิ่ง จำกัด	๑	โปรแกรมสำหรับให้เกษตรกรสามารถ	"
	นอกเขตชลประทาน เพื่อการ				ยื่นคำขอแหล่งน้ำในไร่นานอกเขต	
	บริหารจัดการในเชิงพื้นที่				ชลประทาน และแสดงผลข้อมูลทั้งใน	
					ลักษณะสารสนเทศภูมิศาสตร์	
	๓.๒ ซอฟท์แวร์ประยุกต์					
	ด้าน e-Service					
SW-๐๒๓	โปรแกรมระบบบริการประชาชน	-	ศูนย์สารสนเทศ	๑	โปรแกรมสำหรับให้เกษตรกร และผู้	กลุ่มฐานข้อมูลสารสนเทศ
			กรมพัฒนาที่ดิน		สนใจขอรับบริการสารเร่ง พด. ต่าง ๆ	
					ผ่านทางเครือข่าย Internet	
SW-๐๒๔	บัญชี Stock วัสดุการเกษตร	-	"	๑	โปรแกรมสำหรับผู้ขอรับบริการตรวจ	"
					สอบยอดคงเหลือวัสดุการเกษตรแต่ละ	
					ชนิด ก่อนขอรับบริการ	

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	เวอร์ชั่น	ผู้พัฒนาซอฟต์แวร์	จำนวนลิขสิทธิ์	รายละเอียด ซอฟต์แวร์	ผู้รับผิดชอบ ดูแล จัดการซอฟต์แวร์
SW-๐๒๕	รายงานผลวิเคราะห์ตัวอย่างดิน	-	ศูนย์สารสนเทศ	๑	โปรแกรมสำหรับผู้ขอรับบริการตรวจ	กลุ่มฐานข้อมูลสารสนเทศ
	น้ำ ปุ๋ย		กรมพัฒนาที่ดิน		สอบข้อมูลผลการวิเคราะห์ดิน น้ำ ปุ๋ย	
					ผ่านเครือข่ายอินเตอร์เน็ต	
SW-๐๒๖	ฐานข้อมูลแหล่งน้ำขนาดเล็ก	-	"	๑	โปรแกรมสำหรับติดตามความก้าวหน้า	"
					การดำเนินการก่อสร้างแหล่งน้ำขนาด	
					เล็กในพื้นที่ต่าง ๆ ผ่านระบบ Internet	
SW-๐๒๗	ระบบฐานข้อมูลจุดสำรวจ	-	"	๑	โปรแกรมสำหรับนักสำรวจดินของ	"
	ทรัพยากรดิน				กรมพัฒนาที่ดิน เพื่อจัดเก็บรวบรวม	
					ข้อมูลการเก็บและวิเคราะห์ดิน ซึ่งเป็น	
					การเก็บข้อมูลตัวอย่างดินภาคสนาม	
					และผลการวิเคราะห์ดินจากห้อง	
					ปฏิบัติการ	
SW-๐๒๘	ระบบบริหารจัดการฐานข้อมูล	-	"	๑	โปรแกรมสำหรับบริหารจัดการข้อมูล	กลุ่มระบบภูมิสารสนเทศ
	แหล่งน้ำขนาดเล็ก				แหล่งน้ำ วิเคราะห์และวางแผนบำรุง	
					รักษา แบ่งเป็น ๓ ส่วน ได้แก่ ส่วน	
					สืบค้นข้อมูล ส่วนแสดงผลราย	
					ละเอียดข้อมูลเชิงบรรยาย ส่วนนำ	
					เข้าข้อมูลและส่วนแสดงผลข้อมูลใน	
					รูปแบบแผนที่	

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	เวอร์ชั่น	ผู้พัฒนาซอฟต์แวร์	จำนวนลิขสิทธิ์	รายละเอียด ซอฟต์แวร์	ผู้รับผิดชอบ ดูแล จัดการซอฟต์แวร์
SW-๐๒๙	ระบบฐานข้อมูลหมอดินอาสา	-	ศูนย์สารสนเทศ	๑	โปรแกรมสำหรับรวบรวมข้อมูลประวัติ	กลุ่มระบบเครือข่ายและ
			กรมพัฒนาที่ดิน		หมอดินอาสาประจำหมู่บ้าน ตำบล	คอมพิวเตอร์
					อำเภอ และจังหวัด	
SW-๐๓๐	ระบบ e-Search LDD	-	"	๑	โปรแกรมสำหรับค้นหาข้อมูลวิชาการ	"
					ผลงานวิจัย งานบริการกรมพัฒนาที่ดิน	
SW-๐๓๑	ระบบการประชุมอิเล็กทรอนิกส์	-	บริษัท แพรกซิส โซลูชั่น	๑	โปรแกรมสำหรับนำวาระการประชุม	"
	e-Meeting		จำกัด		และเอกสารประกอบการประชุมเข้าสู่	
					ระบบอิเล็กทรอนิกส์ ผู้เข้าร่วมประชุม	
					สามารถเรียกดูเอกสารประกอบการ	
					ประชุมผ่านทาง Internet	
	๓.๓ ซอฟท์แวร์ประยุกต์					
	ด้าน e-Office					
SW-๐๓๒	ระบบจดหมายอิเล็กทรอนิกส์	-	บริษัท พี.เอฟ เอ็นจิเนียริ่ง	๑	โปรแกรมสำหรับใช้ในการรับ-ส่งเมล์	กลุ่มระบบเครือข่ายและ
	ไปรษณีย์ พ.ด. LDD Mail		แอนด์ เซอร์วิส จำกัด		ของกรมพัฒนาที่ดิน	คอมพิวเตอร์
	ระบบใหม่					
SW-๐๓๓	ระบบสารบรรณอิเล็กทรอนิกส์	-	บริษัท เอ็กซ์เซล ลิงค์ จำกัด	๑	โปรแกรมสำหรับลงรับหนังสือราชการ	"
					ผ่านระบบอิเล็กทรอนิกส์ โดยระบบจะ	
					ออกเลขหนังสือให้อัตโนมัติ	
SW-๐๓๔	- ฐานข้อมูลบริหารครุภัณฑ์	-	ศูนย์สารสนเทศ	๑	โปรแกรมสำหรับจัดเก็บฐานข้อมูล	"
	Online		กรมพัฒนาที่ดิน		ครุภัณฑ์ของกรมพัฒนาที่ดินทั้งหมด	
					สามารถสืบค้นข้อมูลได้สะดวก รวดเร็ว	
					ผ่านทางระบบ Internet	

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	เวอร์ชั่น	ผู้พัฒนาซอฟต์แวร์	จำนวนลิขสิทธิ์	รายละเอียด ซอฟต์แวร์	ผู้รับผิดชอบ ดูแล จัดการซอฟต์แวร์
SW-๐๓๕	- ฐานข้อมูลบริหารครุภัณฑ์	-	ศูนย์สารสนเทศ	๑	โปรแกรมสำหรับจัดเก็บฐานข้อมูล	กลุ่มระบบเครือข่ายและ
	ต่ำกว่าเกณฑ์		กรมพัฒนาที่ดิน		ครุภัณฑ์ต่ำกว่าเกณฑ์ของกรมพัฒนา	คอมพิวเตอร์
					ที่ดินทั้งหมดสามารถสืบค้นข้อมูลได้	
					รวดเร็วผ่านทางระบบ Interneet	
SW-๐๓๖	ระบบตรวจสอบเวลาการทำงาน	-	"	๑	โปรแกรมสำหรับข้าราชการและลูกจ้าง	"
	ผ่าน Web				ประจำกรมพัฒนาที่ดิน (ส่วนกลาง)	
					สามารถตรวจสอบเวลาการทำงาน	
					ของตนเองได้หลังจากทาบบัตรประจำ	
					ตัวอิเล็กทรอนิกส์กับเครื่องบันทึกเวลา	
					แล้ว	
SW-๐๓๗	- ระบบลงเวลาทำงาน	-	"	๑	โปรแกรมสำหรับดึงข้อมูลเวลาจาก	"
					เครื่องทาบบัตรทั้ง ๙ จุด มาจัดเก็บไว้	
					และบริหารจัดการเกี่ยวกับข้อมูล	
					บัตรข้าราชการ/ลูกจ้างประจำ	
					อิเล็กทรอนิกส์	
SW-๐๓๘	ระบบสำนักงานอิเล็กทรอนิกส์	-	บริษัท แมกซ์เซฟวิ่งส์	๑	โปรแกรมสำหรับการจัดทำใบลา และ	กลุ่มวิเคราะห์และ
	e-Office		(ประเทศไทย) จำกัด		การเบิกวัสดุสำนักงานสิ้นเปลือง โดย	วางระบบข้อมูล
					กรอกข้อมูลตามแบบฟอร์มที่กำหนด	
					พร้อมลงนามลายมือชื่ออิเล็กทรอนิกส์	
					เพื่อขออนุมัติ	

ตารางภาคผนวกที่ ๑๖ รายการทรัพย์สินประเภท ข้อมูล (Information)

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเอกสารข้อมูล/เอกสารสนเทศ	ขนาดข้อมูล (Size)	Database (ที่ใช้)	รูปแบบที่ให้บริการ	ระดับชั้นข้อมูล	สื่อบันทึกข้อมูลที่ใช้ในการเก็บ	ที่เก็บสารสนเทศ (ชื่อสถานที่)	ระยะเวลาการจัดเก็บ	ผู้เป็นเจ้าของสารสนเทศ
ข้อมูลเว็บไซต์									
INF-๐๐๑	- ข้อมูลเว็บไซต์กรมฯ	๔๒.๖ GB	SQL	Web Site	เปิดเผย	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๙ ปี	ศูนย์สารสนเทศ
	(http://www.ldd.go.th)								
INF-๐๐๒	- ข้อมูลเว็บไซต์กลุ่มงานตรวจสอบ	๑.๖๐ GB	-	"	เปิดเผย	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๖ ปี	กลุ่มงานตรวจ
	ภายใน								สอบภายใน
INF-๐๐๓	- ข้อมูลเว็บไซต์กลุ่มพัฒนาระบบ	๑๐๗ MB	-	"	เปิดเผย	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๕ ปี	กลุ่มพัฒนา
	บริหาร								ระบบบริหาร
INF-๐๐๔	- ข้อมูลเว็บไซต์กองการเจ้าหน้าที่	๑.๓๐ GB	-	"	เปิดเผย	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๙ ปี	กองการ
									เจ้าหน้าที่
INF-๐๐๕	- ข้อมูลเว็บไซต์สำนักวิศวกรรมเพื่อ	๒.๒๖ GB	-	"	เปิดเผย	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๙ ปี	สำนักวิศวกรรม
	การพัฒนาที่ดิน								เพื่อการพัฒนา
									ที่ดิน
INF-๐๐๖	- ข้อมูลเว็บไซต์ศูนย์สารสนเทศ	๑.๓๒ GB	-	"	เปิดเผย	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๙ ปี	ศูนย์สารสนเทศ
INF-๐๐๗	- ข้อมูลเว็บไซต์สำนักงาน	๒ GB	Access	"	เปิดเผย	ไฟล์ข้อมูล	สำนักงาน	๙ ปี	สำนักงาน
	เลขานุการกรม						เลขานุการกรม		เลขานุการกรม
INF-๐๐๘	- ข้อมูลเว็บไซต์กองคลัง	๒ GB	My SQL	"	เปิดเผย	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๙ ปี	กองคลัง
INF-๐๐๙	- ข้อมูลเว็บไซต์กองแผนงาน	๒ GB	-	"	เปิดเผย	ไฟล์ข้อมูล	กองแผนงาน	๙ ปี	กองแผนงาน

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเอกสารข้อมูล/เอกสารสนเทศ	ขนาดข้อมูล (Size)	Database (ที่ใช้)	รูปแบบที่ให้บริการ	ระดับชั้นข้อมูล	สื่อบันทึกข้อมูลที่ใช้ในการเก็บ	ที่เก็บสารสนเทศ (ชื่อสถานที่)	ระยะเวลาการจัดเก็บ	ผู้เป็นเจ้าของสารสนเทศ
INF-๐๑๐	- ข้อมูลเว็บไซต์สำนักเทคโนโลยีการ	๒ GB	My SQL	"	เปิดเผย	ไฟล์ข้อมูล	สำนักเทคโน	๙ ปี	สำนักเทคโน
	สำรวจและทำแผนที่						โลยีการสำรวจ		โลยีการสำรวจ
							และทำแผนที่		และทำแผนที่
INF-๐๑๑	- ข้อมูลเว็บไซต์สำนักวิจัยและ	๒ GB	My SQL	Web Site	เปิดเผย	ไฟล์ข้อมูล	สำนักวิจัยและ	๙ ปี	สำนักวิจัยและ
	พัฒนาการจัดการที่ดิน						พัฒนาการ		พัฒนาการ
							จัดการที่ดิน		จัดการที่ดิน
INF-๐๑๒	- ข้อมูลเว็บไซต์สำนักวิทยาศาสตร์	๒ GB	My SQL	"	เปิดเผย	ไฟล์ข้อมูล	สำนักวิทยา	๙ ปี	สำนักวิทยา
	เพื่อการพัฒนาที่ดิน						ศาสตร์เพื่อการ		ศาสตร์เพื่อการ
							พัฒนาที่ดิน		พัฒนาที่ดิน
INF-๐๑๓	- ข้อมูลเว็บไซต์สำนักสำรวจดินและ	๒ GB	-	"	เปิดเผย	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๙ ปี	สำนักสำรวจ
	วิจัยทรัพยากรดิน								ดินและวิจัย
									ทรัพยากรดิน
INF-๐๑๔	- ข้อมูลเว็บไซต์กองนโยบายและ	๒ GB	My SQL	"	เปิดเผย	ไฟล์ข้อมูล	กองนโยบาย	๔ ปี	กองนโยบาย
	แผนการใช้ที่ดิน						และแผนการ		และแผนการ
							ใช้ที่ดิน		ใช้ที่ดิน
INF-๐๑๕	- ข้อมูลเว็บไซต์กองเทคโนโลยี	๒ GB	My SQL	"	เปิดเผย	ไฟล์ข้อมูล	กองเทคโนโลยี	๔ ปี	กองเทคโนโลยี
	ชีวภาพทางดิน						ชีวภาพทางดิน		ชีวภาพทางดิน
ข้อมูลด้าน GIS									
INF-๐๑๖	- ข้อมูลของระบบเตือนภัยธรรมชาติ (Natural	๒๘.๑ GB	SQL	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๓ ปี	กลุ่มระบบภูมิ
	Disasters Warning)	(Databese รวม							สารสนเทศ
		ของระบบ EIS)							
INF-๐๑๗	- ข้อมูลของระบบบันทึกตำแหน่งเกิดเหตุผ่าน	"	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๓ ปี	"
	โทรศัพท์มือถือ (Mobile)								

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเอกสารข้อมูล/เอกสารสนเทศ	ขนาดข้อมูล (Size)	Database (ที่ใช้)	รูปแบบที่ให้บริการ	ระดับชั้นข้อมูล	สื่อบันทึกข้อมูลที่ใช้ในการเก็บ	ที่เก็บสารสนเทศ (ชื่อสถานที่)	ระยะเวลาการจัดเก็บ	ผู้เป็นเจ้าของสารสนเทศ
INF-๐๑๘	- ข้อมูลของระบบตรวจสอบการใช้ประโยชน์	๒๘.๑ GB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๓ ปี	กลุ่มระบบภูมิ
	ที่ดิน (Present Land Use	(Databese รวม							สารสนเทศ
	Monitoring)	ของระบบ EIS)							
INF-๐๑๙	- ข้อมูลของระบบบริหารและติดตามโครง	"	SQL	Web Application	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๓ ปี	"
	การปลูกหญ้าแฝก (Vetiver								
	Grass Tracking)								
INF-๐๒๐	- ข้อมูลของระบบนำเสนอแผนที่ชุดดิน (Soil	"	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๓ ปี	"
	Series) มาตราส่วน ๑ : ๒๕,๐๐๐								
INF-๐๒๑	- ข้อมูลของระบบบริหารจัดการข้อมูลเกษตร	"	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๒ ปี	"
	ใช้สารอินทรีย์ลดใช้สารเคมีทาง								
	การเกษตร/เกษตรอินทรีย์								
INF-๐๒๒	- ข้อมูลของระบบบริหารจัดการข้อมูลโรงงาน	"	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๒ ปี	"
	ผลิตปุ๋ยอินทรีย์								
INF-๐๒๓	- ข้อมูลของระบบฐานข้อมูลแหล่งน้ำในไร่นา	"	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑ ปี	"
	นอกเขตชลประทาน เพื่อการ								
	บริหารจัดการในเชิงพื้นที่								
ข้อมูลบริการประชาชน									
INF-๐๒๔	- ข้อมูลของโปรแกรมระบบบริการประชาชน	๘.๑๙ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑๑ ปี	กลุ่มฐานข้อมูล
									สารสนเทศ
INF-๐๒๕	- ข้อมูลของระบบบัญชี Stock วัสดุการเกษตร	๑๔๖.๑๙ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑๑ ปี	"

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเอกสารข้อมูล/เอกสารสนเทศ	ขนาดข้อมูล (Size)	Database (ที่ใช้)	รูปแบบที่ให้บริการ	ระดับชั้นข้อมูล	สื่อบันทึกข้อมูลที่ใช้ในการเก็บ	ที่เก็บสารสนเทศ (ชื่อสถานที่)	ระยะเวลาการจัดเก็บ	ผู้เป็นเจ้าของสารสนเทศ
INF-๐๒๖	- ข้อมูลของระบบรายงานผลวิเคราะห์ตัวอย่างดิน	๑๘๙.๕๖ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๔ ปี	กลุ่มฐานข้อมูล
	น้ำ ปุ๋ย								สารสนเทศ
INF-๐๒๗	- ข้อมูลของระบบฐานข้อมูลแหล่งน้ำขนาดเล็ก	๒๖.๑๙ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑๒ ปี	"
INF-๐๒๘	- ข้อมูลของระบบฐานข้อมูลจุดสำรวจ	๒๗.๙๔ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑ ปี	"
	ทรัพยากรดิน								
INF-๐๒๙	- ข้อมูลของระบบบริหารจัดการฐานข้อมูล	๒ GB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๗ ปี	กลุ่มระบบ
	แหล่งน้ำขนาดเล็ก								ภูมิสารสนเทศ
INF-๐๓๐	- ข้อมูลของระบบฐานข้อมูลหมอดินอาสา	๒.๑๑ GB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑๒ ปี	กลุ่มระบบเครือข่าย
									และคอมพิวเตอร์
INF-๐๓๑	- ข้อมูลของระบบ e-Search LDD	๑.๑๓ MB	"	"	เปิดเผย	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๒ ปี	"
INF-๐๓๒	- ข้อมูลของระบบการประชุมอิเล็กทรอนิกส์	๗.๒๕ MB	SQL	Web Application	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๘ ปี	"
	e-Meeting								
ข้อมูล Intranet									
INF-๐๓๓	- ข้อมูลของระบบจดหมายอิเล็กทรอนิกส์	๕๐๐ GB	Smarter Mail DB	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑ ปี	กลุ่มระบบเครือข่าย
	ไปรษณีย์พด. LDD Mail (Mailbox)								และคอมพิวเตอร์
	(ระบบใหม่)								
INF-๐๓๔	- ข้อมูลของระบบสารบรรณอิเล็กทรอนิกส์	๓๖๙.๖๓ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑๓ ปี	"
INF-๐๓๕	- ข้อมูลของระบบฐานข้อมูลบริหารครุภัณฑ์ Online	๑๒๙.๔๔ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๗ ปี	"
INF-๐๓๖	- ข้อมูลของระบบฐานข้อมูลบริหารครุภัณฑ์ต่ำกว่า	๙๗.๑๙ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๔ ปี	"
	เกณฑ์								

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อเอกสารข้อมูล/เอกสารสนเทศ	ขนาดข้อมูล (Size)	Database (ที่ใช้)	รูปแบบที่ให้บริการ	ระดับชั้นข้อมูล	สื่อบันทึกข้อมูลที่ใช้ในการเก็บ	ที่เก็บสารสนเทศ (ชื่อสถานที่)	ระยะเวลาการจัดเก็บ	ผู้เป็นเจ้าของสารสนเทศ
INF-๐๓๗	- ข้อมูลของระบบตรวจสอบเวลาการทำงาน	๘๕๔ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑๓ ปี	กลุ่มระบบเครือข่าย
	ผ่าน Web								และคอมพิวเตอร์
INF-๐๓๘	- ข้อมูลของระบบลงเวลาทำงาน	๖๓๒ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๑๓ ปี	"
INF-๐๓๙	- ข้อมูลของระบบสำนักงานอิเล็กทรอนิกส์	๙๙๐.๗๕ MB	"	"	ลับ	ไฟล์ข้อมูล	ศูนย์สารสนเทศ	๘ ปี	กลุ่มวิเคราะห์
	e-Office								และวางระบบข้อมูล

ตารางภาคผนวกที่ ๑๗ รายการทรัพย์สินประเภท คน (People ware) ภายในองค์กร

รหัสพนักงาน	ชื่อ - นามสกุล	ตำแหน่ง	ส่วนงาน/ฝ่ายงาน	หน้าที่ความรับผิดชอบ	เบอร์โทรศัพท์ติดต่อ	อีเมล์
EMP-๐๐๑	นางอรนาฏ โอวาทตระกูล	ผู้อำนวยการศูนย์สารสนเทศ		- กำกับ ควบคุม ดูแล และบริหารจัดการระบบ	๐-๒๙๔๑-๒๑๓๑	cit_1@ldd.go.th
				สารสนเทศทั้งทางด้านวิเคราะห์และวางระบบ		
				ข้อมูล ด้านระบบเครือข่ายและคอมพิวเตอร์		
				ด้านฐานข้อมูลสารสนเทศ และด้านระบบภูมิ		
				สารสนเทศ		
	กลุ่มวิเคราะห์และวางระบบ					
	ข้อมูล					
EMP-๐๐๒	นางกุลวดี ภาร์ดวาจ	ผู้อำนวยการกลุ่มวิเคราะห์และ	กลุ่มวิเคราะห์และวาง	- กำกับ แนะนำ ตรวจสอบการปฏิบัติงานของ	๐-๒๕๗๙-๔๕๔๘	cit_4@ldd.go.th
		วางระบบข้อมูล	ระบบข้อมูล	ผู้ร่วมปฏิบัติงาน โดยใช้ความรู้ ความสามารถ		
				ประสบการณ์ และความชำนาญงานสูงมากใน		
				งานวิชาการด้านวิเคราะห์และวางระบบข้อมูล		
				และปฏิบัติงานที่ต้องตัดสินใจหรือแก้ปัญหา		
				ที่ยากมาก		
EMP-๐๐๓	นางเกษร สวนศรี	บรรณารักษ์ชำนาญการ	กลุ่มวิเคราะห์และวาง	- ดูแลระบบห้องเรียนอิเล็กทรอนิกส์	Call Center	kesorn@ldd.go.th
			ระบบข้อมูล	(e-Learning) และห้องสมุดอิเล็กทรอนิกส์	๑๗๖๐ ต่อ ๑๒๗๔	
				(e-Library)		
				- ดูแลห้องสมุด กรมพัฒนาที่ดิน		
EMP-๐๐๔	นางสาวฐิติพร วีระประสิทธิ์	นักวิชาการคอมพิวเตอร์ชำนาญการ	กลุ่มวิเคราะห์และวาง	- ศึกษา และวางระบบคอมพิวเตอร์ทั้งด้าน	๐-๒๕๖๒-๕๑๑๖	thitipn@ldd.go.th
			ระบบข้อมูล	Hardware/Software การสื่อสาร		

รหัสพนักงาน	ชื่อ - นามสกุล	ตำแหน่ง	ส่วนงาน/ฝ่ายงาน	หน้าที่ความรับผิดชอบ	เบอร์โทรศัพท์ติดต่อ	อีเมล์
				- จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ		
				แผนปฏิบัติการของกรมฯ ให้สอดคล้องกับของชาติ		

รหัสพนักงาน	ชื่อ - นามสกุล	ตำแหน่ง	ส่วนงาน/ฝ่ายงาน	หน้าที่ความรับผิดชอบ	เบอร์โทรศัพท์ติดต่อ	อีเมล์
	กลุ่มระบบเครือข่ายและ					
	คอมพิวเตอร์					
EMP-๐๐๕	นางจันทร์เพ็ญ ลาภจิตร	ผู้อำนวยการกลุ่มระบบเครือข่าย	กลุ่มระบบเครือข่ายและ	- กำกับ แนะนำ ตรวจสอบการปฏิบัติงานของ	๐-๒๕๗๙-๑๑๘๑	cit_5@ldd.go.th
		และคอมพิวเตอร์	คอมพิวเตอร์	ผู้ร่วมปฏิบัติงาน โดยใช้ความรู้ ความสามารถ		
				ประสบการณ์ และความชำนาญงานสูงมากใน		
				งานวิชาการด้านเครือข่ายและคอมพิวเตอร์ และ		
				ปฏิบัติงานที่ต้องตัดสินใจหรือแก้ปัญหาที่ยากมาก		
EMP-๐๐๖	นายสุพงษ์ ไพชยนต์	นักวิเคราะห์นโยบายและแผน	กลุ่มระบบเครือข่ายและ	- ซ่อมบำรุงระบบเครือข่ายและคอมพิวเตอร์	๐-๒๕๖๒-๕๑๒๙	supong@ldd.go.th
		ชำนาญการ	คอมพิวเตอร์			
EMP-๐๐๗	นายไกรฤกษ์ ปานทอง	นักวิชาการคอมพิวเตอร์ชำนาญการ	กลุ่มระบบเครือข่ายและ	- ดูแลการถ่ายทอดสดการบรรยายการฝึกอบรม	Call Center	krirerk@ldd.go.th
			คอมพิวเตอร์	คอมพิวเตอร์ผ่าน Web Site	๑๗๖๐ ต่อ ๑๓๗๘	
				- จัดทำวีดีโอบันทึกการบรรยายการฝึกอบรม		
				สำหรับให้เจ้าหน้าที่ Download ผ่าน Intranet		
EMP-๐๐๘	นางวราภรณ์ อินทร์ทิพย์	นักวิชาการคอมพิวเตอร์ชำนาญการ	กลุ่มระบบเครือข่ายและ	- บริหารจัดการผู้ใช้งานบนระบบเครือข่าย	๐-๒๕๗๙-๑๑๘๑	waraporn@ldd.go.th
			คอมพิวเตอร์	- สำรองข้อมูลบนระบบเครือข่าย		
EMP-๐๐๙	นางสาวอริศรา พึ่งพา	นักวิชาการคอมพิวเตอร์ชำนาญการ	กลุ่มระบบเครือข่ายและ	- ดูแล ออกแบบ พัฒนา Web Site กรมพัฒนา	๐-๒๕๗๙-๑๑๘๑	arissara@ldd.go.th
			คอมพิวเตอร์	ที่ดิน (Webmaster)		
EMP-๐๑๐	นายธวัชชัย สมบูรณ์	นายช่างไฟฟ้าชำนาญงาน	กลุ่มระบบเครือข่ายและ	- ดูแลระบบ Call Center (Software ระบบ	๐-๒๕๖๒-๕๑๐๙	twatchai@ldd.go.th
			คอมพิวเตอร์	บริหารจัดการ Call Center และตู้ชุมสาย		
				โทรศัพท์)		

รหัสพนักงาน	ชื่อ - นามสกุล	ตำแหน่ง	ส่วนงาน/ฝ่ายงาน	หน้าที่ความรับผิดชอบ	เบอร์โทรศัพท์ติดต่อ	อีเมล์

รหัสพนักงาน	ชื่อ - นามสกุล	ตำแหน่ง	ส่วนงาน/ฝ่ายงาน	หน้าที่ความรับผิดชอบ	เบอร์โทรศัพท์ติดต่อ	อีเมล์
	กลุ่มฐานข้อมูลสารสนเทศ					
EMP-๐๑๑	นางดวงดอม กำเนิดทรัพย์	ผู้อำนวยการกลุ่มฐานข้อมูล	กลุ่มฐานข้อมูลสารสนเทศ	- กำกับ แนะนำ ตรวจสอบการปฏิบัติงานของ	๐-๒๕๗๙-๑๙๓๗	cit_3@ldd.go.th
		สารสนเทศ		ผู้ร่วมปฏิบัติงาน โดยใช้ความรู้ ความสามารถ		
				ประสบการณ์ และความชำนาญงานสูงมากใน		
				งานวิชาการด้านฐานข้อมูลสารสนเทศ และ		
				ปฏิบัติงานที่ต้องตัดสินใจหรือแก้ปัญหาที่ยากมาก		
EMP-๐๑๒	นายพนัสบดี ธัชโอภาส	นักวิชาการคอมพิวเตอร์ชำนาญการ	กลุ่มฐานข้อมูลสารสนเทศ	- โปรแกรมเมอร์	๐-๒๕๗๙-๑๙๓๗	panast@ldd.go.th
EMP-๐๑๓	นางสาวรุจิรัตน์ รุจิรกุล	นักวิชาการคอมพิวเตอร์ชำนาญการ	กลุ่มฐานข้อมูลสารสนเทศ	- ติดตามผลการดำเนินงานโครงการที่สำคัญ	๐-๒๕๗๙-๑๙๓๗	rujirat@ldd.go.th
				ผ่านระบบสารสนเทศของกรมพัฒนาที่ดิน		

รหัสพนักงาน	ชื่อ - นามสกุล	ตำแหน่ง	ส่วนงาน/ฝ่ายงาน	หน้าที่ความรับผิดชอบ	เบอร์โทรศัพท์ติดต่อ	อีเมล์

รหัสพนักงาน	ชื่อ - นามสกุล	ตำแหน่ง	ส่วนงาน/ฝ่ายงาน	หน้าที่ความรับผิดชอบ	เบอร์โทรศัพท์ติดต่อ	อีเมล์
	กลุ่มระบบภูมิสารสนเทศ					
EMP-๐๑๔	นายอิทธิศักดิ์ ขุนทอง	ผู้อำนวยการกลุ่มระบบภูมิสารสนเทศ	กลุ่มระบบภูมิสารสนเทศ	- กำกับ แนะนำ ตรวจสอบการปฏิบัติงานของ	๐-๒๕๗๙-๑๙๓๗	cit_6@ldd.go.th
				ผู้ร่วมปฏิบัติงาน โดยใช้ความรู้ ความสามารถ		
				ประสบการณ์ และความชำนาญงานสูงมากใน		
				งานวิชาการด้านภูมิสารสนเทศ และปฏิบัติงาน		
				ที่ต้องตัดสินใจหรือแก้ปัญหาที่ยากมาก		
EMP-๐๑๕	นายศรัณย์นพ อินทเสน	นักวิชาการแผนที่ภาพถ่าย	กลุ่มระบบภูมิสารสนเทศ	- บริการข้อมูลด้านระบบสารสนเทศภูมิศาสตร์	Call Center	sryanope@ldd.go.th
		ชำนาญการ		แก่ผู้บริหาร ผู้เกี่ยวข้องและประชาชน	๑๗๖๐ ต่อ ๑๒๒๒	
EMP-๐๑๖	นายวีระ ปะทะขีนัง	นักวิชาการแผนที่ภาพถ่าย	กลุ่มระบบภูมิสารสนเทศ	- จัดเก็บ รวบรวมและปรับปรุงข้อมูลสารสนเทศ	๐-๒๙๔๑-๒๗๗๑	weerapt@ldd.go.th
		ชำนาญการ		ด้านภูมิศาสตร์ให้เป็นปัจจุบัน เพื่อเข้าสู่ระบบ		
				เครือข่ายกลาง		
				- จัดทำ รวบรวมข้อมูล (Meta Data) ด้าน		
				ภาพถ่ายทางอากาศ ภาพถ่ายดาวเทียมและ		
				แฟ้มข้อมูลแผนที่ทุกประเภท เพื่อเป็นฐานข้อมูล		
				สำหรับบริการหน่วยงานต่าง ๆ ของกรมฯ และ		
				กระทรวงเกษตรและสหกรณ์		
				- จัดทำมาตรฐานข้อมูล (Meta Data) ด้านภูมิ		
				สารสนเทศ เพื่อใช้แลกเปลี่ยนและบริการ		

รหัสพนักงาน	ชื่อ - นามสกุล	ตำแหน่ง	ส่วนงาน/ฝ่ายงาน	หน้าที่ความรับผิดชอบ	เบอร์โทรศัพท์ติดต่อ	อีเมล์

ตารางภาคผนวกที่ ๑๘ รายการทรัพย์สินประเภท บริการ (Stakeholders)

เลขทะเบียน ทรัพย์สินสารสนเทศ	ชื่อบริการ	รายละเอียดบริการ	เจ้าของบริการ	ข้อมูลติดต่อ	ผู้ใช้บริการ	SLA
SERV-๐๐๑	บำรุงรักษาเครื่องคอมพิวเตอร์	บำรุงรักษาเครื่องคอมพิวเตอร์	บริษัท พี.เอฟ เอ็นจิเนียริ่ง	๗/๗๑ ม.๑๑ ถ.รามอินทรา	กลุ่มระบบเครือข่าย	๔ hr
	และระบบเครือข่าย	และระบบเครือข่าย	แอนด์ เซอร์วิส จำกัด	แขวงคันนายาว	และคอมพิวเตอร์	
				เขตคันนายาว กทม.		
				๑๐๒๓๐		
SERV-๐๐๒	บำรุงรักษาระบบประชุมทางไกล	บำรุงรักษาระบบประชุมทางไกล	บริษัท ดิ เอ็กซ์เพิร์ท	อาคาร SV ซิตี้ พระราม ๓	กลุ่มระบบเครือข่าย	๓ hr
	ผ่านจอภาพ (Video Conference)	ผ่านจอภาพ (Video Conference)	ไอซีที จำกัด	๘๙๖/๒๕ ถนนพระราม ๓	และคอมพิวเตอร์	
				แขวงบางโพงพาง		
				เขตยานนาวา กทม.		
				๑๐๑๒๐		
SERV-๐๐๓	ระบบสื่อสารอินเตอร์เน็ตพร้อมวงจร	ระบบสื่อสารอินเตอร์เน็ตพร้อม	บริษัท กสท. โทรคมนาคม	๙๙ ม.๓ ถนนแจ้งวัฒนะ	กลุ่มระบบเครือข่าย	๔ hr
	เชื่อมโยง	วงจรเชื่อมโยง	จำกัด (มหาชน)	แขวงทุ่งสองห้อง	และคอมพิวเตอร์	
				เขตหลักสี่ กทม. ๑๐๒๑๐		
SERV-๐๐๔	บำรุงรักษาโปรแกรมระบบห้องสมุด	บำรุงรักษาโปรแกรมระบบห้องสมุด	บริษัท ลิบเน็ทส์ จำกัด	๑๒๘/๗๔ อาคารพญาไท-	กลุ่มวิเคราะห์และ	๔ hr
	อัตโนมัติ (e-Library)	อัตโนมัติ (e-Library)		พลาซ่า ชั้น ๗ ห้อง ๗F	วางระบบข้อมูล	
				ถนนพญาไท แขวงทุ่ง-		
				พญาไท เขตราชเทวี		
				กทม. ๑๐๔๐๐		