

**การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

**โดย**

**กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน**

**กรมกิจการผู้สูงอายุ**

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

**กรมกิจการผู้สูงอายุ**

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นสิ่งสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นทรัพย์สินของกรมกิจการผู้สูงอายุ และยังรวมถึงการปกป้อง ภารกิจขององค์กรให้ปลอดภัยจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงอยู่ตลอดเวลา สำหรับความหมายของบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ กระบวนการการทำงานที่ช่วยให้ IT Managers มีมาตรการในการป้องกันและการบรรลุผลสำเร็จของพันธกิจด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญขององค์กร

๑. ประเภทการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

 การวิเคราะห์ความเสี่ยงด้านสารสนเทศของกรมกิจการผู้สูงอายุสามารถแยกประเภทความเสี่ยงออกเป็น ๔ ประเภท ดังนี้

 ๑.๑ ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือ และอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะ ทำลายระบบจาก Cracker เป็นต้น

 ๑.๒ ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัด ความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบ สารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของกรม ฯ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิด ความเสียหายต่อข้อมูลสารสนเทศได้

 ๑.๓ ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

 ๑.๔ ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากนโยบายหรือการตัดสินใจในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

**๒. การประมาณความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด สำหรับเกณฑ์การประมาณเป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ ระดับความรุนแรงของผลกระทบของความเสี่ยง และแผนภูมิความเสี่ยง ซึ่งกรมกิจการผู้สูงอายุใช้เกณฑ์ ดังนี้

 **๒.๑ ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ**

|  |  |  |
| --- | --- | --- |
| **ระดับ** | **โอกาสที่จะเกิด** | **คำอธิบาย** |
| ๕ | สูงมาก | ๕ ครั้ง/ปี |
| ๔ | สูง | ๔ ครั้ง/ปี |
| ๓ | ปานกลาง | ๓ ครั้ง/ ปี |
| ๒ | น้อย | ๒ ครั้ง/ปี |
| ๑ | น้อยมาก | ไม่เกิน ๑ ครั้ง/ปี |

|  |  |  |
| --- | --- | --- |
| **ระดับ** | **ผลกระทบ** | **คำอธิบาย** |
| ๕ | สูงมาก | เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ |
| ๔ | สูง |  เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความ ปลอดภัย ซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน |
| ๓ | ปานกลาง |  ระบบมีปัญหาและมีความสูญเสียไม่มาก |
| ๒ | น้อย |  เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้ |
| ๑ | น้อยมาก |  เกิดเหตุร้ายที่ไม่มีความสำคัญ |

 **๒.๒ ระดับความรุนแรงของผลกระทบของความเสี่ยง**

 ๒.๓ แผนภูมิความเสี่ยง

การวัดระดับความเสี่ยง

มาก

|  |  |
| --- | --- |
| ความเสี่ยงปานกลาง- ผลกระทบรุนแรงมาก- โอกาสเกิดน้อยผลกระทบ | ความเสี่ยงสูง- ผลกระทบรุนแรงมาก- โอกาสเกิดมาก |
| ความเสี่ยงต่ำ- ผลกระทบน้อย- โอกาสเกิดน้อย | ความเสี่ยงปานกลาง- ผลกระทบน้อย- โอกาสเกิดมาก |

มาก

น้อย

โอกาสที่จะเกิด

**๓. ผลการประมาณความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

| **ประเด็นความเสี่ยง** | **ประเภทความเสี่ยง** | **โอกาสที่เกิดความเสี่ยง** | **ผลกระทบจากความเสี่ยง** | **สรุประดับความเสี่ยง** |
| --- | --- | --- | --- | --- |
| ๑.ความเสี่ยงจากเครื่อง คอมพิวเตอร์หรืออุปกรณ์ ขัดข้อง ไม่สามารถทำงานได้ตามปกติ | ความเสี่ยงด้านเทคนิค | น้อย | ปานกลาง | ต่ำ |
| ๒. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น | ความเสี่ยงจากผู้ปฏิบัติงาน | ปานกลาง | น้อย | ต่ำ |
| ๓. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ | ความเสี่ยงจากผู้ปฏิบัติงาน | ปานกลาง | สูง | ปานกลาง |
| ๔.ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่ | ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน | น้อย | สูง | ปานกลาง |
| ๕.ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี | ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน | น้อยมาก | สูงมาก | ปานกลาง |
| ๖.ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน | ความเสี่ยงด้านการบริหารจัดการ | สูง | สูง | สูง |
| ๗.ความเสี่ยงจากการ เปลี่ยนแปลงนโยบายผู้บริหาร | ความเสี่ยงด้านการบริหารจัดการ | น้อย | สูง | ปานกลาง |
| ๘.ความเสี่ยงต่อการได้รับการสนับสนุน งบประมาณไม่เพียงพอ | ความเสี่ยงด้านการบริหารจัดการ | สูง | สูง | สูง |
| ๙.ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม | ความเสี่ยงจากภัยหรือ สถานการณ์ฉุกเฉิน | น้อยมาก | สูงมาก | ปานกลาง |
| ๑๐.ความเสี่ยงจากการ โจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์ | ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากผู้ปฏิบัติงาน | น้อยมาก | สูงมาก | ปานกลาง |
| **สรุปผลภาพรวมการประมาณความเสี่ยงด้านเทคโนโลยีสารสนเทศ** | **ปานกลาง** |

**๔. การรายงานผลการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

เมื่อประเมินความเสี่ยงแล้วเสร็จ จำเป็นต้องออกรายงานการประเมินเป็นเอกสารที่ผู้อื่นสามารถอ่านได้ เอกสารนี้จะเป็นสาระสำคัญในการสื่อสารให้บุคลากรทั้งองค์กรได้รับรู้ รายงานประกอบด้วยรายละเอียดอย่างน้อยตามลักษณะรายละเอียดของความเสี่ยง และการออกรายงานมีวัตถุประสงค์ให้ส่วนต่าง ๆ ได้รับรู้ดังต่อไปนี้

๔.๑ ฝ่ายบริหาร ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ ดังต่อไปนี้ เช่น

* เข้าใจผลที่กระทบต่อผู้มีส่วนได้เสียต่าง ๆ ในกรณีที่เกิดมีเหตุหรือเหตุการณ์และเกิดผลเสียต่อภารกิจและผลประกอบการ
* ดำเนินการเพื่อสร้างความตระหนักในปัญหาความเสี่ยงให้เกิดการรับรู้ทั่วทั้งองค์กร
* ออกนโยบายบริหารความเสี่ยงที่มีเนื้อหาด้านปรัชญาและความรับผิดขอบของหน่วยงาน และบุคลากรต่าง ๆ ในการบริหารความเสี่ยง

๔.๒ หัวหน้างาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

* ตระหนักในความเสี่ยงอันเกี่ยวข้องกับภาระหน้าที่ของตน ผลกระทบที่อาจมีต่อหน่วยงาน
* รายงานผลกระทบจากความเสี่ยงในกรณีเกิดหรือจะเกิดเหตุและเสนอแนะแนวทางการ แก้ไข

๔.๓ **ผู้**ปฏิบัติงาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

* เข้าใจบทบาทหน้าที่ในความเสี่ยงด้านเทคโนโลยีสารเทศที่เกี่ยวข้องกับความรับผิดชอบของตนเอง
* เข้าใจการบริหารความเสี่ยงและความตระหนักต่อความเสี่ยงในการเป็นวัฒนธรรมองค์กรที่สำคัญอย่างหนึ่ง

๕. กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

 เมื่อผู้บริหารได้รับรายงานการประเมินความเสี่ยงแล้วจำเป็นต้องทำการตัดสินใจ โดยพิจารณาจากหลักเกณฑ์การยอมรับความเสี่ยงที่องค์กรมีอยู่ว่าจะยอมรับโดยไม่ทำอะไร หรือจะดำเนินการบำบัดความเสี่ยง ซึ่งได้แก่กระบวนการ ดังต่อไปนี้

 ๕.๑ การยอมรับความเสี่ยง เป็นการยอมรับในความเสี่ยงโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวจริงเพียงใช้ ID/Password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การให้มีใช้ชีวมาตร เช่น การตรวจลายนิ้วมือหรือม่านตาอาจมีค่าใช้จ่ายสูงไม่คุ้มค่า กรมฯ อาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปโดยไม่ทำอะไร

 ๕.๒ การหลีกเลี่ยงความเสี่ยง ตัวอย่างเช่น องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ใช้บริการ และแนะนำให้บุคลากรของกรมฯ ใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของไวรัสอย่างหนัก องค์กรอาจมีทางเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น

 ๕.๓ การโอนย้ายความเสี่ยง เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกันหรือสัญญาการบำรุงรักษาหลังการขาย (Maintenance Service) เป็นต้น

 ๕.๔ การลดความเสี่ยง ได้แก่ การมีมาตรการควบคุมเข้มงวดมากขึ้นเพื่อลดความเสี่ยง เช่น การใช้ชีวมาตร (biometrics) เพื่อใช้ในการพิสูจน์ตัวจริงนอกเหนือไปจากการใช้ ID/Password ที่มีอยู่เดิม

**๖. การติดตามผลความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

๖.๑ การรายงานความเสี่ยงตกค้าง

 เมื่อมีการบำบัดความเสี่ยงแล้ว จำเป็นต้องมีการรายงานและทบทวนอยู่เสมอเพื่อดูว่ามีการประเมินค่าความเสี่ยงอยู่ตลอดเวลา และดูว่ามาตรการควบคุมต่าง ๆ ที่ออกมาใช้ได้ผลหรือไม่เพียงไร วิธีการมาตรฐานที่ใช้กันโดยทั่วไป คือ การมีหน่วยงานภายในหรือภายนอกทำการตรวจสอบ โดยกระบวนการ IT Auditing ที่เหมาะสม เนื่องจากสิ่งแวดล้อมและกฎระเบียบมีพลวัตรและการเปลี่ยนแปลงเกิดขึ้นตลอดเวลา จึงจำเป็นต้องมีการบริหารความเสี่ยงและการตรวจสอบเป็นประจำ

๖.๒ การเฝ้าสังเกต

 กระบวนการเฝ้าสังเกตเป็นหลักประกันว่าองค์กรมีมาตรการต่าง ๆ ที่จำเป็นและเหมาะสมสำหรับการบริหารความเสี่ยงต่าง ๆ และมาตรการเหล่านั้นมีผู้ปฏิบัติตามและบังเกิดผลจริง ดังนั้น กระบวนการเฝ้าสังเกตพึงพิจารณาดังนี้

 ๑) ได้มีการปฏิบัติตามมาตรการต่าง ๆ และบังเกิดผล

 ๒) กระบวนงานที่กำหนดขึ้นมาสามารถปฏิบัติได้จริง

 ๓) มีการเรียนรู้เกิดขึ้นในหน่วยงานอันเป็นผลมาจากการบริหารความเสี่ยง

-----------------------------------------------------