การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและทางไซเบอร์

คำนำ

การตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและทางไซเบอร์ของกรมกิจการเด็กและเยาวชน ฉบับนี้ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านระบบฐานข้อมูล ระบบเทคโนโลยีสารสนเทศ และทางไซเบอร์ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่ เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น

กองยุทธศาสตร์และแผนงาน กลุ่มสารสารสนเทศและเทคโนโลยี หวังเป็นอย่างยิ่งว่า การดำเนินงานตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและทางไซเบอร์ของกรมกิจการเด็กและเยาวชน ฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของกรมกิจการเด็กและเยาวชน ต่อไป

กรมกิจการเด็กและเยาวชน

สิงหาคม ๒๕๖๖

สารบัญ

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและทางไซเบอร์

บทนำ

ในปัจจุบันความก้าวหน้าของเทคโนโลยีสารสนเทศมีบทบาทอย่างมากในการขับเคลื่อนภารกิจของภาครัฐ ในขณะเดียวกันความซับซ้อนและขยายตัวทางด้านเทคโนโลยีสารสนเทศอย่างรวดเร็วทำให้ส่งผลในการอาจจะเกิดความเสี่ยงต่าง ๆ ในหลายมิติมากขึ้น ได้แก่ ความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ซึ่งหมายถึง ความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนิน และความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ ทั้งนี้ความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเดิม ถือเป็นส่วนหนึ่งของความเสี่ยงด้านปฏิบัติการ แต่ในปัจจุบันความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ เป็นความเสี่ยงที่มีความสำคัญมากขึ้น แนวทางการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและทางไซเบอร์ฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายของหน่วยงาน ในการส่งเสริมและยกระดับการให้บริการและการปฏิบัติงาน โดยการให้ความสำคัญด้านการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตั้งแต่การวางกรอบนโยบายที่ชัดเจน การระบุความเสี่ยง การประเมินความเสี่ยง รวมถึงการบริหารและจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่องค์กรยอมรับได้ รวมทั้งเพื่อสร้างความน่าเชื่อมั่นในการให้บริการภาครัฐด้วยระบบเทคโนโลยีสารสนเทศและทางไซเบอร์อย่างมีมาตรฐาน

ปัญหาทั่วไปที่สังเกตได้

กรมกิจการเด็กและเยาวชน มีภารกิจเกี่ยวกับการส่งเสริมและพัฒนาศักยภาพของเด็กและเยาวชน การคุ้มครองและพิทักษ์สิทธิเด็กและเยาวชน การส่งเสริมสวัสดิการเด็กและครอบครัว โดยการกำหนดนโยบาย มาตรการ กลไก ส่งเสริมและสนับสนุนภาครัฐและภาคเอกชน ติดตามและประเมินผลการดำเนินการตามนโยบายและมาตรการที่กำหนด เพื่อให้เด็กและเยาวชน มีคุณภาพชีวิตที่ดี และมีความมั่นคงในการดำรงชีวิต จากการดำเนินงานดังกล่าว จะต้องให้ความสำคัญในการป้องกันและควบคุมไม่ให้มีความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด หรืออาจจะเกิดจากข้อผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัยอุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึง

ประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใด ๆ รวมทั้งอาจจะเกิดความเสี่ยงจากข้อผิดพลาดการทำงานระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ฐานข้อมูลด้านเด็กและเยาวชน ฐานข้อมูลบุคลากร ฐานข้อมูลสนับสนุนการปฏิบัติงานตามภารกิจของหน่วยงาน ระบบฐานข้อมูลบริหารงานภายใน (Back Office) ระบบการให้บริการบนเครือข่ายคอมพิวเตอร์ ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Anti-Virus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) และโปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์ (Web Application Program) เป็นต้น อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์ต่อพ่วง อุปกรณ์ที่ใช้จัดเก็บและสำรองข้อมูล อุปกรณ์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องคอมพิวเตอร์ชนิดพกพา เครื่องสแกนเนอร์ เครื่องพิมพ์ อุปกรณ์สำรองไฟฟ้า อุปกรณ์กระจายสัญญาณเครือข่าย และอุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย เป็นต้น

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและ
สารสนเทศทางไซเบอร์

2. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบ
เทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

3. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่าง
ทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร และการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการ
ดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม 5 ขั้นตอน ประกอบด้วย 1) การระบุความเสี่ยง 2) การวิเคราะห์ความเสี่ยง 3) การกำหนดมาตรการ 4) การติดตามรายงานประเมินผล และ 5) การทบทวนระบุกรอบเวลา ดังรูป

รูปที่ 1 แสดงกระบวนการบริหารความเสี่ยง

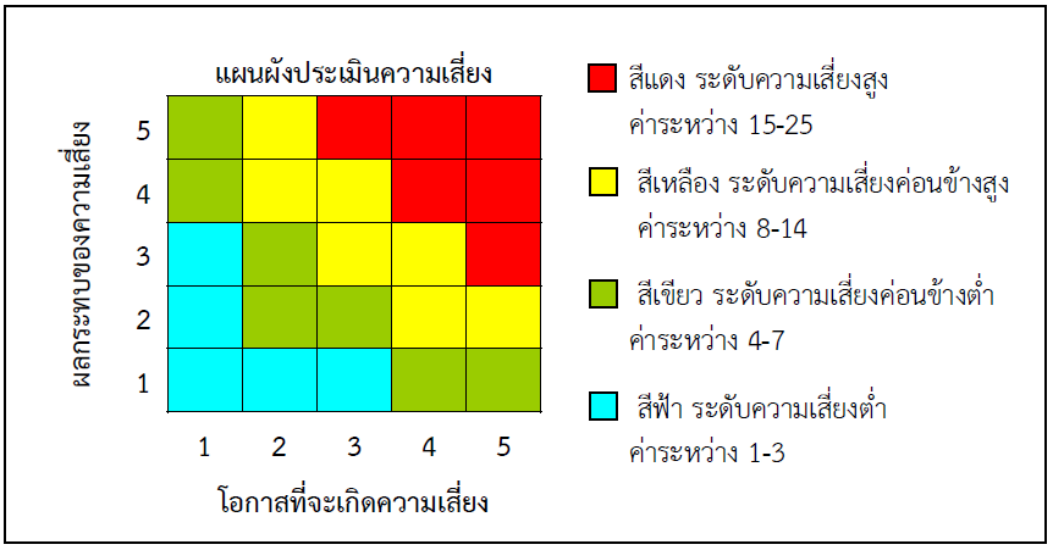
1. <u>การระบุความเสี่ยง</u> เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร โดยมีวิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย การใช้ Checklist การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน เป็นต้น ซึ่งในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีต ทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

2. <u>การวิเคราะห์ความเสี่ยงและประเมินความเสี่ยง</u> การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วย การวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

2.1 การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิญปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ 4 ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

2.2 การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยง ก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

2.3 การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน



2.4 การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่ผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้แล้ว เลือกความเสี่ยงที่มีระดับสูงมากหรือสูง มาจัดทำแผนการบริหารความเสี่ยงก่อน

ตอบสนองต่อความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) โดยมีหลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

1. การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้น จึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้
คิดทบทวนถึงผลที่จะได้รับ อาจนำมาซึ่งการเสียโอกาสของหน่วยงานได้

2. การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัย ที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด user/password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้ user/password ที่กำหนดให้แล้ว อาจจะบอก user/password ของตนให้ผู้ใต้บังคับบัญชาทราบ และเมื่อผู้ใต้บังคับบัญชาทราบ user/password ของหัวหน้างาน อาจจะเก็บไว้คนเดียวหรือนำไปบอกให้

บุคคลอื่นทราบต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย และหน่วยงานที่รับผิดชอบต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น แล้วจึงแก้ไขโดยการกำหนด user/password ใหม่ ให้กับหัวหน้างาน เป็นต้น

3. การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิดหาก เราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดย มีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า

4. การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะเวลาในการรับประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่ อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขายให้ทันก่อน ระยะเวลาในการรับประกันจะสิ้นสุด

ขั้นตอนและวิธีการดำเนินงาน

1. <u>ขั้นตอนที่ 1</u> เริ่มต้นโดยการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและทางไซเบอร์ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and assessment) อย่างน้อยปีละ 1 ครั้ง โดยมีวิธีการปฏิบัติดังนี้

1.1 มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ

1.2 มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

1.3 มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ

1.4 มีการตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations) อย่างน้อย 1 ครั้งต่อปี เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพและผลการตรวจสอบเป็นที่น่าเชื่อถือได้

2. <u>ขั้นตอนที่ 2</u> ดำเนินการตรวจสอบและประเมินความเสี่ยง จะต้องดำเนินการโดยผู้ตรวจสอบระบบสารสนเทศและทางไซเบอร์ของ ดย. (Internal IT Auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของ ดย. โดยมีวิธีการปฏิบัติ ดังนี้

2.1 กำหนดให้หน่วยตรวจสอบภายใน ของ ดย. เป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ ดย. และให้ตรวจสอบและประเมินความเสี่ยงอย่างน้อย 1 ครั้งต่อปี

2.2 มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบ ระหว่างผู้ตรวจสอบกับผู้รับการตรวจ

2.3 มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ ในลักษณะที่อ่านได้เพียงอย่างเดียว

2.4 มีวิธีการที่ปลอดภัยสำหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูล ชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้

2.5 ต้องสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา

2.6 ต้องทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

2.7 ต้องมีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ

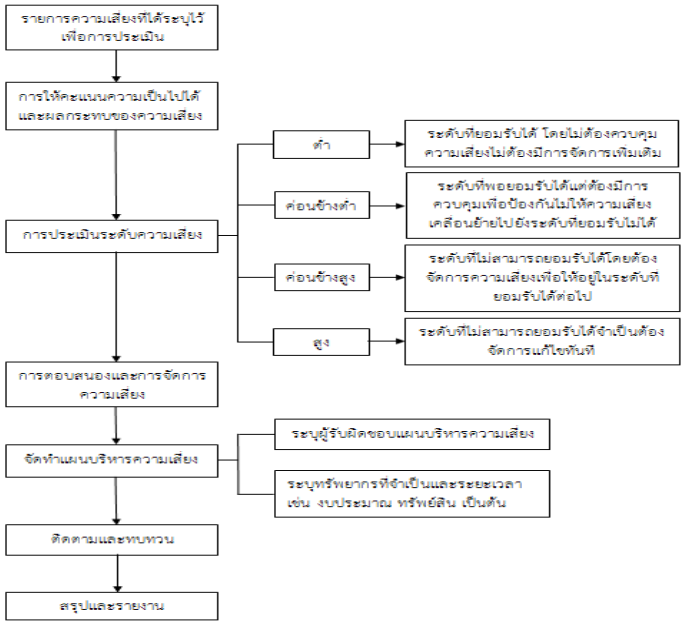
2.8 ต้องกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ

2.9 ต้องกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศ จากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแลหรือรับผิดชอบ)

3. ขั้นตอนที่ 3 ติดตามผลการดำเนินงาน เพื่อให้ทราบว่าผลการดำเนินงานการตรวจสอบและประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและทางไซเบอร์พบความเสี่ยงหรือไม่ หากพบว่ามีความเสี่ยงแล้ว อยู่ในระดับใด เกิดผลกระทบมากน้องเพียงใด

4. ขั้นตอนที่ 4 สรุปผลการดำเนินงาน เพื่อเป็นการรายงานความก้าวหน้าในการดำเนินงานวิเคราะห์และประเมินความเสี่ยง เพื่อให้ผู้บริหารทราบ และกำหนดเป็นแผนในการดำเนินงานในอนาคต

โดยมีรายละเอียดตามรูปขั้นตอนและวิธีการดำเนินงาน ดังนี้



รูปที่ 2 ขั้นตอนและวิธีการดำเนินงาน

ประโยชน์ที่คาดว่าจะได้รับ

1. มีความพร้อมในการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศและทางไซเบอร์

2. มีแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูล ระบบเทคโนโลยีสารสนเทศ และทางไซเบอร์ให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

ระยะเวลาดำเนินการ

ที่	กิจกรรม	ปี 2566				ผู้รับผิดชอบ
		ไตรมาส 1	ไตรมาส 2	ไตรมาส 3	ไตรมาส 4	
1	ศึกษาข้อมูลในการจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและทางไซเบอร์	═══				กยผ.
2	วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและทางไซเบอร์		═══			กยผ.
3	ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและทางไซเบอร์		═══	═══		กยผ.
4	ติดตามประเมินผล				═══	กยผ.

ผู้รับผิดชอบ

1. นางสาวดรุณี พจนานุกูลกิจ ผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยี
2. นางเรณู บุญวัฒน์พุฒิ นักสังคมสงเคราะห์ชำนาญการพิเศษ
3. นายนิรุตต์ รุ่งแจ้ง นักพัฒนาสังคมชำนาญการ
4. นางสาวจุไรรัตน์ รุ่งเรือง นักวิเคราะห์นโยบายและแผนปฏิบัติการ
5. นายสุธี วังเกล็ดแก้ว นักวิชาการคอมพิวเตอร์

กรมกิจการเด็กและเยาวชน
Department of Children and Youth