ประกาศกรมการจัดหางาน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามที่กรมการจัดหางานเป็นหน่วยงานของรัฐตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งมีภารกิจในการให้บริการประชาชนผ่านระบบเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินภารกิจของกรมการจัดหางานในการให้บริการประชาชนผ่านระบบเทคโนโลยีสารสนเทศเป็นไปอย่างมั่นคงปลอดภัย และน่าเชื่อถือตลอดจนสอดคล้องกับกฎหมายและมาตรฐานสากล กรมการจัดหางานจึงกำหนดนโยบายและแนวปฏิบัติไว้ ดังนี้

๑. กรมการจัดหางานยึดถือกรอบแนวคิดพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security) ประกอบด้วย ๓ องค์ประกอบหลัก เพื่อป้องกันข้อมูลและระบบสารสนเทศ ประกอบด้วย ความลับ (Confidentiality) การเข้าถึงข้อมูลต้องได้รับอนุญาตเท่านั้น ความถูกต้องครบถ้วน (Integrity) ข้อมูลต้องไม่มีการแก้ไขโดยมิชอบ และความพร้อมใช้งาน (Availability) ระบบสามารถให้บริการได้อย่างต่อเนื่องแม้ในสภาวะวิกฤตโดยให้ความสำคัญกับการป้องกันเชิงรุกต่อภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยของประชาชน

๒. กรมการจัดหางานปฏิบัติตามฐานอำนาจและข้อกฎหมายที่เกี่ยวข้อง ประกาศฉบับนี้จัดทำขึ้นโดยอ้างอิงตามกฎหมายและระเบียบ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยเฉพาะมาตรา ๔๔ ที่กำหนดให้หน่วยงานต้องมีประมวลแนวทางปฏิบัติ (Code of Practice) และมาตรา ๕๔ เรื่องการประเมินความเสี่ยง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) เพื่อปกป้องข้อมูลส่วนบุคคลของประชาชนผู้มาติดต่อราชการ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องมีนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศที่เป็นลายลักษณ์อักษร

๓. กรมการจัดหางานปฏิบัติตามกรอบมาตรฐานสากลที่ประยุกต์ใช้ เพื่อให้มีมาตรฐานทัดเทียมระดับสากล กรมฯ ได้บูรณาการกรอบงาน ISO/IEC 27001:2022 ใช้เป็นโครงสร้างหลักในการบริหารจัดการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) และการนำมาตรการควบคุม (Annex A) มาใช้งาน NIST Cybersecurity Framework (CSF) 2.0 ใช้ฟังก์ชันหลัก ๖ ด้าน (Govern, Identify, Protect, Detect, Respond, Recover) ในการกำกับดูแลและตอบสนองภัยคุกคาม

๔. กรมการจัดหางานปฏิบัติตามมาตรการและการดำเนินงานที่สำคัญการบริหารความเสี่ยงและการตรวจสอบ กรมฯ ต้องมีการประเมินความเสี่ยงและตรวจสอบความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบที่มีความเป็นกลาง อย่างน้อยปีละ ๑ ครั้ง การเฝ้าระวังและรับมือภัยคุกคาม โดยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ที่ทำหน้าที่ตรวจจับและตอบสนองต่อภัยคุกคามทางเครือข่ายขององค์กร (SOC) ตลอด ๒๔ ชั่วโมง เพื่อตรวจจับเหตุการณ์ผิดปกติ และปฏิบัติตามแผนรับมือภัยคุกคาม (IRP) รวมถึง

การแจ้งเหตุ...

การแจ้งเหตุตามกระบวนการแจ้งเหตุฉุกเฉิน (Call Tree) เมื่อเกิดเหตุร้ายแรง อีกทั้งการบริหารความต่อเนื่องทางธุรกิจ กรณีเกิดสภาวะวิกฤต กรมฯ จะดำเนินการกู้คืนระบบและฐานข้อมูลสำคัญจาก ระบบคลาวด์กลางภาครัฐ (GDCC) ตามลำดับความสำคัญเพื่อให้สามารถกลับมาให้บริการได้ภายในระยะเวลาเป้าหมาย (RTO)

๕. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์มีผลบังคับใช้กับบุคลากรทุกคนและบุคคลภายนอกที่เกี่ยวข้อง โดยผู้ที่ฝ่าฝืนหรือละเลยการปฏิบัติตามอาจได้รับโทษทางวินัยหรือโทษตามที่กฎหมายกำหนด

จึงประกาศให้ทราบโดยทั่วกัน ทั้งนี้ ให้มีผลนับตั้งแต่บัดนี้เป็นต้นไป จนกว่าจะมีประกาศเปลี่ยนแปลง

ประกาศ ณ วันที่ ๑๔ พฤษภาคม พ.ศ. ๒๕๖๙

(นายสมชาย มรกตศรีวรรณ)
อธิบดีกรมการจัดหางาน

นโยบายและแนวปฏิบัติ
ด้านความมั่นคงปลอดภัยไซเบอร์

คำนำ

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารเป็นเครื่องมือสำคัญที่กรมการจัดหางานนำมาใช้ในการขับเคลื่อนภารกิจหลักเพื่อให้บริการประชาชนและภาคธุรกิจอย่างกว้างขวาง โดยเฉพาะการให้บริการผ่านระบบอิเล็กทรอนิกส์ (e-Services) เช่น ระบบไทยมีงานทำ ระบบการออกใบอนุญาตจัดหางานอิเล็กทรอนิกส์ (DOE e-License) และระบบบริหารแรงงานต่างด้าว อย่างไรก็ตาม ท่ามกลางการเปลี่ยนแปลงที่รวดเร็วของโลกไซเบอร์ กรมการจัดหางานต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีรูปแบบหลากหลายและทวีความรุนแรงเพิ่มขึ้น ตลอดจนภัยพิบัติทางธรรมชาติและเหตุการณ์ฉุกเฉินที่ไม่คาดคิด ซึ่งอาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยของประชาชน

เพื่อให้การดำเนินงานของกรมการจัดหางานเป็นไปอย่างต่อเนื่อง มีประสิทธิภาพ และสอดคล้องกับมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กรมการจัดหางานจึงได้จัดทำนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ขึ้น โดยบูรณาการกรอบมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๒๒ และ NIST Cybersecurity Framework (CSF) ๒.๐ เอกสารฉบับนี้มุ่งเน้นการรักษาความมั่นคงปลอดภัยตามหลักการ CIA อันประกอบด้วย ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลและระบบสารสนเทศ

นอกจากนโยบายเชิงป้องกันแล้ว กรมการจัดหางานได้จัดทำแผนบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Plan: BCP) และแผนกู้คืนระบบสารสนเทศจากภัยพิบัติ (Disaster Recovery Plan: DRP) แยกส่วนอย่างชัดเจน เพื่อเป็นแนวทางปฏิบัติในการตอบสนองและฟื้นฟูการดำเนินงานเมื่อเกิดสถานการณ์วิกฤต แผนดังกล่าวมีวัตถุประสงค์เพื่อปกป้องบุคลากร ทรัพย์สิน และข้อมูลสำคัญของกรมฯ เพื่อให้สามารถให้บริการประชาชนได้อย่างต่อเนื่องและมีประสิทธิภาพสูงสุด แม้ในยามที่เกิดสภาวะไม่ปกติ

กรมการจัดหางานหวังเป็นอย่างยิ่งว่า นโยบายและแผนการดำเนินงานฉบับนี้จะเป็นเครื่องมือสำคัญในการสร้างความเชื่อมั่นให้กับประชาชนและผู้มีส่วนได้ส่วนเสียทุกภาคส่วน และเป็นบรรทัดฐานให้บุคลากรทุกคนนำไปปฏิบัติอย่างเคร่งครัด เพื่อสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ที่ยั่งยืนให้กับองค์กรสืบไป

กรมการจัดหางาน พฤษภาคม ๒๕๖๙

สารบัญ

บทที่ ๑
นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Policy)

ในปัจจุบัน การเปลี่ยนผ่านสู่รัฐบาลดิจิทัลทำให้เทคโนโลยีสารสนเทศและการสื่อสารกลายเป็นกลไกหลักในการขับเคลื่อนภารกิจของกรมการจัดหางาน กรมฯ ได้พัฒนาระบบบริการอิเล็กทรอนิกส์ (e-Services) จำนวนมากเพื่ออำนวยความสะดวกแก่ประชาชน เช่น ระบบไทยมีงานทำ ระบบการออกใบอนุญาตจัดหางานอิเล็กทรอนิกส์ (DOE e-License) และระบบบริหารจัดการแรงงานต่างด้าว, ซึ่งระบบเหล่านี้มีการจัดเก็บและประมวลผลข้อมูลที่มีความสำคัญต่อความมั่นคงทางเศรษฐกิจและสังคมของประเทศ อย่างไรก็ตาม ท่ามกลางความก้าวหน้าทางเทคโนโลยี กรมการจัดหางานต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีรูปแบบหลากหลายและรุนแรงขึ้น รวมถึงภัยพิบัติทางธรรมชาติและเหตุการณ์ฉุกเฉินต่าง ๆ, ซึ่งอาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลและระบบสารสนเทศ, หากระบบสำคัญหยุดชะงัก ย่อมส่งผลกระทบอย่างมีนัยสำคัญต่อการให้บริการประชาชนและชื่อเสียงของหน่วยงาน

เพื่อให้การดำเนินงานเป็นไปอย่างมั่นคงปลอดภัยและสอดคล้องกับระเบียบข้อบังคับ กรมการจัดหางานจึงได้จัดทำนโยบายฉบับนี้โดยมีหลักการและเหตุผลอ้างอิง ดังนี้

๑. ด้านกฎหมาย: เพื่อปฏิบัติตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งกำหนดให้หน่วยงานของรัฐต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้ง, และสอดคล้องกับพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

๒. ด้านมาตรฐานสากล: เพื่อยกระดับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ ซึ่งเป็นกรอบการบริหารจัดการที่เน้นการประเมินและจัดการความเสี่ยงอย่างเป็นระบบ , และการนำ NIST Cybersecurity Framework (CSF) ๒.๐ มาใช้เป็นแนวทางในปฏิบัติครอบคลุมทั้งการกำกับดูแล (Govern) การป้องกัน (Protect) และการกู้คืน (Recover)

๓. ด้านความต่อเนื่องทางธุรกิจ: เพื่อสร้างความพร้อมในการรับมือกับสภาวะวิกฤต กรมฯ จึงได้บูรณาการแผนบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Plan: BCP) และแผนกู้คืนระบบสารสนเทศจากภัยพิบัติ (Disaster Recovery Plan: DRP), เพื่อเป็นกลยุทธ์ในการรักษากระบวนงานที่สำคัญ (Critical Business Processes) และฟื้นฟูระบบไอทีให้กลับมาใช้งานได้ตามระยะเวลาเป้าหมาย (RTO) ที่กำหนดไว้

การกำหนดนโยบายและแนวปฏิบัติที่ชัดเจนนี้ จะช่วยสร้างบรรทัดฐานให้บุคลากรทุกระดับปฏิบัติงานด้วยความตระหนักรู้, และสร้างความเชื่อมั่นให้แก่ประชาชนและผู้มีส่วนได้ส่วนเสียว่า กรมการจัดหางานมีความพร้อมในการคุ้มครองข้อมูลและให้บริการได้อย่างต่อเนื่องในทุกสถานการณ์

เพื่อให้การปฏิบัติตามนโยบายและแนวทางปฏิบัติฉบับนี้เป็นไปอย่างถูกต้องและเข้าใจตรงกัน จึงกำหนดคำนิยามสำคัญไว้ดังนี้:

๑. คำนิยามด้านหน่วยงานและบุคลากร

- กรม: หมายถึง กรมการจัดหางาน
- ผู้บริหารระดับสูง (CEO): หมายถึง อธิบดีกรมการจัดหางาน หรือผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการของกรมการจัดหางาน
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO): หมายถึง ผู้บริหารที่ได้รับมอบหมายให้รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมการจัดหางาน
- ผู้ดูแลระบบ (System Administrator): หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย
- ผู้ใช้งาน (User): หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าใช้งานระบบสารสนเทศของกรมฯ

๒. คำนิยามด้านความมั่นคงปลอดภัยไซเบอร์

- ไซเบอร์ (Cyber): ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม
- การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity): มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้ของข้อมูล
- ภัยคุกคามทางไซเบอร์ (Cyber Threat): การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ มุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์หรือข้อมูล
- เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident): เหตุการณ์ที่เกิดจากการโจมตีหรือการดำเนินการที่มิชอบ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อความมั่นคงปลอดภัยของคอมพิวเตอร์หรือข้อมูล
- โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure - CII): ระบบคอมพิวเตอร์หรือเครือข่ายที่ใช้ในกิจการที่เกี่ยวข้องกับการรักษาความมั่นคงของรัฐ ความปลอดภัยสาธารณะ หรือบริการภาครัฐที่สำคัญ

๓. นิยามหลักด้าน ISMS

- ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS): ส่วนหนึ่งของระบบการบริหารจัดการโดยรวมของกรมฯ ที่มุ่งเน้นการจัดทำ นำไปปฏิบัติ ดำเนินการ ติดตาม ทบทวน บำรุงรักษา และปรับปรุงความมั่นคงปลอดภัยสารสนเทศ โดยใช้กระบวนการบริหารจัดการความเสี่ยงเป็นหลัก

- ความมั่นคงปลอดภัยสารสนเทศ (Information Security): การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมถึงคุณสมบัติอื่น ๆ เช่น ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) และความน่าเชื่อถือ (Reliability)
- ความลับ (Confidentiality): การรับรองว่าสารสนเทศจะไม่ถูกเปิดเผยหรือเปิดเผยต่อบุคคล กระบวนการหรือตัวตนที่ไม่ได้รับอนุญาต
- ความถูกต้องครบถ้วน (Integrity): การรักษาความถูกต้องและสมบูรณ์ของสารสนเทศและวิธีการประมวลผล
- ความพร้อมใช้งาน (Availability): การรับรองว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงและใช้งานสารสนเทศหรือระบบงานได้เมื่อต้องการ

๔. คำนิยามด้านความต่อเนื่องทางธุรกิจ (BCP & DRP)

- แผนบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Plan - BCP): แนวทางในการตอบสนองต่อสภาวะวิกฤตเพื่อให้กระบวนงานที่สำคัญ (Critical Business Process) สามารถกลับมาดำเนินการได้อย่างปกติภายในระยะเวลาที่เหมาะสม
- แผนกู้คืนระบบสารสนเทศจากภัยพิบัติ (Disaster Recovery Plan - DRP): แผนปฏิบัติการที่เน้นการกู้คืนโครงสร้างพื้นฐานด้านไอที ข้อมูล และระบบสารสนเทศที่ได้รับผลกระทบจากภัยพิบัติให้กลับมาใช้งานได้ตามปกติ
- ระยะเวลาเป้าหมายการฟื้นคืนสภาพ (Recovery Time Objective - RTO): ระยะเวลาที่กำหนดไว้เพื่อให้กระบวนงานหรือระบบสารสนเทศต้องได้รับการกู้คืนกลับมาให้บริการได้อีกครั้งหลังจากเกิดเหตุหยุดชะงัก
- คลาวด์กลางภาครัฐ (Government Data Center and Cloud Service - GDCC): โครงสร้างพื้นฐานคลาวด์สำหรับการจัดเก็บฐานข้อมูลและระบบงานสำคัญของกรมการจัดหางาน ซึ่งมีมาตรฐานความปลอดภัยระดับสากล

๑.๑ วัตถุประสงค์และขอบเขตการบังคับใช้

๑.๑.๑ วัตถุประสงค์ (Objectives)

การจัดทำนโยบายและแนวปฏิบัติฉบับนี้มีวัตถุประสงค์หลักเพื่อ:

- เพื่อธำรงไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศตามหลักการ CIA Triad อันประกอบด้วย ความลับ (Confidentiality) ข้อมูลต้องเข้าถึงได้เฉพาะผู้มีสิทธิ์, ความถูกต้องครบถ้วน (Integrity) ข้อมูลต้องมีความสมบูรณ์ไม่ถูกแก้ไขโดยมิชอบ และ ความพร้อมใช้ (Availability) ระบบต้องสามารถให้บริการได้อย่างต่อเนื่อง

- เพื่อให้สอดคล้องกับกฎหมายและมาตรฐานสากล โดยเฉพาะมาตรา ๔๔ แห่ง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานรัฐต้องมีประมวลแนวทางปฏิบัติและกรอบมาตรฐานขั้นต่ำ รวมถึงให้สอดคล้องกับมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ และกรอบ NIST Cybersecurity Framework (CSF) ๒.๐
- เพื่อบริหารจัดการและลดระดับความเสี่ยง จากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อภารกิจหลักและการให้บริการประชาชน เช่น ภัยจากโปรแกรมไม่ประสงค์ดี (Malware) หรือการโจมตีระบบคอมพิวเตอร์
- เพื่อสร้างบรรทัดฐานและวัฒนธรรมความปลอดภัย ให้บุคลากรทุกระดับมีความตระหนักและเข้าใจหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินสารสนเทศของกรมฯ
- เพื่อสร้างความเชื่อมั่น ให้แก่ประชาชน ผู้ประกันตน นายจ้าง และผู้มีส่วนได้ส่วนเสีย (Stakeholders) ว่าข้อมูลและระบบบริการอิเล็กทรอนิกส์ของกรมการจัดหางานมีความมั่นคงปลอดภัยและน่าเชื่อถือ

๑.๑.๒ ขอบเขตการบังคับใช้ (Scope of Application)

นโยบายและแนวปฏิบัติฉบับนี้มีขอบเขตครอบคลุมองค์ประกอบต่าง ๆ ดังนี้:

- ด้านทรัพย์สินสารสนเทศ (Asset Scope): ครอบคลุมข้อมูลสารสนเทศ (Data) ทั้งในรูปแบบเอกสารและอิเล็กทรอนิกส์, ระบบเครือข่ายคอมพิวเตอร์, ระบบฐานข้อมูล, ซอฟต์แวร์ประยุกต์, และอุปกรณ์ฮาร์ดแวร์ทั้งหมดของกรมฯ
- ด้านระบบงานสำคัญ (System Scope): มุ่งเน้นการคุ้มครองระบบบริการประชาชนและระบบบริหารจัดการภายในที่สำคัญ เช่น:
    - ระบบไทยมีงานทำ
    - ระบบการออกใบอนุญาตจัดหางานอิเล็กทรอนิกส์ (DOE e-License)
    - ระบบบริหารจัดการการทำงานของคนต่างด้าว (e-WorkPermit)
    - ระบบเครือข่ายสื่อสารข้อมูลที่เชื่อมโยงหน่วยงานส่วนกลางและส่วนภูมิภาค
- ด้านบุคลากร (Personnel Scope): บังคับใช้กับบุคลากรทุกคนที่ปฏิบัติงานให้กับกรมการจัดหางาน ได้แก่ ข้าราชการ, พนักงานราชการ, ลูกจ้างประจำ, ลูกจ้างชั่วคราว รวมถึงบุคคลภายนอก (Third Parties) เช่น ที่ปรึกษา, ผู้รับจ้างเหมาบริการ (Outsource), และผู้ปฏิบัติงานตามสัญญาจ้างที่ได้รับอนุญาตให้เข้าถึงระบบ
- ด้านสถานที่ (Physical Scope): ครอบคลุมพื้นที่ปฏิบัติงานหลัก (อาคารกรมการจัดหางาน เขตดินแดง), สำนักงานจัดหางานกรุงเทพมหานครพื้นที่ ๑-๑๐, ศูนย์ข้อมูลและเครือข่าย (Data Center), รวมถึงสถานที่ปฏิบัติงานสำรองตามแผน BCP และการปฏิบัติงานระยะไกล (Work From Home)
- ด้านการกำกับดูแล (Governance Scope): ครอบคลุมกระบวนการตั้งแต่การระบุทรัพย์สิน, การป้องกัน, การตรวจจับ, การตอบสนองต่อเหตุการณ์, และการกู้คืนระบบตามวงจรชีวิตของ NIST CSF

๑.๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้สอดคล้องกับภารกิจของกรมการจัดหางานและมาตรฐานสากล กรมฯ ได้บูรณาการกรอบมาตรฐานสำคัญ ๓ ส่วนหลัก ดังนี้

๑.๒.๑ มาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๒๒

กรมการจัดหางานยึดถือมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ เป็นกรอบพื้นฐานหลักในการจัดทำ ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของหน่วยงานเป็นไปอย่างมีระบบ มีประสิทธิภาพ และสอดคล้องกับมาตรฐานสากล, โดยมีองค์ประกอบสำคัญที่กรมฯ นำมาประยุกต์ใช้ดังนี้

- โครงสร้างข้อกำหนดหลัก : กรมฯ ดำเนินการตามข้อกำหนดเพื่อสร้างระบบ ISMS ที่สมบูรณ์ เริ่มจากการทำความเข้าใจบริบทองค์กรและกลุ่มผู้มีส่วนได้ส่วนเสีย, การแสดงภาวะผู้นำของผู้บริหารระดับสูงในการกำหนดนโยบายและบทบาทความรับผิดชอบ, การวางแผนเพื่อจัดการความเสี่ยงและโอกาส การสนับสนุนด้านทรัพยากรและสมรรถนะของบุคลากร การปฏิบัติงานตามแผนที่วางไว้ ไปจนถึงการประเมินประสิทธิภาพผ่าน การตรวจประเมินภายใน (Internal Audit) และการทบทวนโดยผู้บริหาร, เพื่อนำไปสู่การปรับปรุงระบบอย่างต่อเนื่อง
- มาตรการควบคุมความมั่นคงปลอดภัย (Annex A): กรมฯ ได้ดำเนินการระบุมาตรการควบคุมที่เลือกใช้งานและจัดเตรียมเอกสาร แสดงการใช้มาตรการ (Statement of Applicability: SoA) เพื่อใช้เป็นแนวทางในการป้องกันความเสี่ยง, โดยครอบคลุมมาตรการ ๔ ด้านหลัก ได้แก่
    - มาตรการด้านองค์กร (Organizational Controls): เช่น การกำหนดนโยบายเฉพาะเรื่อง การบริหารจัดการทรัพย์สิน และความสัมพันธ์กับผู้ให้บริการภายนอก
    - มาตรการด้านบุคลากร (People Controls): เช่น การตรวจสอบภูมิหลังก่อนเริ่มงาน การสร้างความตระหนักรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์
    - มาตรการด้านกายภาพ (Physical Controls): เช่น การรักษาความมั่นคงปลอดภัยพื้นที่ศูนย์ข้อมูล (Data Center) การป้องกันอุปกรณ์ และการรักษาความสะอาดโต๊ะทำงานและหน้าจอ (Clear Desk and Clear Screen)
    - มาตรการด้านเทคโนโลยี (Technological Controls): เช่น การควบคุมการเข้าถึงสิทธิพิเศษ การป้องกันมัลแวร์ การสำรองข้อมูล และการเฝ้าระวังผ่านข้อมูลล็อก

การปฏิบัติตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ นี้ มีวัตถุประสงค์หลักเพื่อธำรงไว้ซึ่งหลักการ CIA คือ ความลับ (Confidentiality) ข้อมูลเข้าถึงได้โดยผู้มีสิทธิ์เท่านั้น, ความถูกต้อง (Integrity) ข้อมูลมีความครบถ้วนถูกต้อง และ ความพร้อมใช้ (Availability) ระบบสามารถให้บริการได้อย่างต่อเนื่องแม้ในสภาวะวิกฤต

๑.๒.๒ กรอบงาน NIST Cybersecurity Framework (CSF) ๒.๐

กรมการจัดหางานได้นำกรอบงาน NIST CSF ๒.๐ มาใช้เป็นแนวทางหลักในการบริหารจัดการความเสี่ยงและบูรณาการเข้ากับระบบนิเวศด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน โดยกรอบงานนี้ทำหน้าที่เป็นสื่อกลางในการเชื่อมโยงเป้าหมายเชิงกลยุทธ์เข้ากับการปฏิบัติงานทางเทคนิค ซึ่งประกอบด้วย ๖ ฟังก์ชันหลัก (Core Functions) ดังนี้

๑.๒.๒.๑ การกำกับดูแล (Govern - GV): มุ่งเน้นการกำหนดกลยุทธ์ ลำดับความสำคัญ และความรับผิดชอบในการบริหารความเสี่ยงทางไซเบอร์ให้สอดคล้องกับภารกิจของกรมฯ

- บริบทองค์กร: ทำความเข้าใจความคาดหวังของผู้มีส่วนได้ส่วนเสียและข้อกำหนดทางกฎหมาย เช่น พรบ. ไซเบอร์ฯ ๒๕๖๒ และ PDPA
- กลยุทธ์การบริหารความเสี่ยง: กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และแนวทางการสื่อสารความเสี่ยงทั่วทั้งองค์กร
- บทบาทและความรับผิดชอบ: ผู้บริหารระดับสูง (อธิบดี) แสดงภาวะผู้นำและรับผิดชอบในการกำกับดูแล โดยมีคณะบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team) สนับสนุนด้านทรัพยากร

๑.๒.๒.๒ การระบุ (Identify - ID): การทำความเข้าใจความเสี่ยงที่มีต่อสินทรัพย์และบุคลากรของกรมฯ

- การบริหารจัดการทรัพย์สิน: จัดทำบัญชีรายการทรัพย์สิน (Asset Inventory) ทั้งฮาร์ดแวร์ ซอฟต์แวร์ และระบบสำคัญ เช่น ระบบไทยมีงานทำ, ระบบ DOE e-License และระบบบริหารแรงงานไทยไปต่างประเทศ
- การประเมินความเสี่ยง: ระบุภัยคุกคาม จุดอ่อน และช่องโหว่ โดยใช้วิธีสร้างสถานการณ์สมมติ (Scenario Based Approach) เพื่อวิเคราะห์ผลกระทบต่อภารกิจ

๑.๒.๒.๓. การป้องกัน (Protect - PR): การนำมาตรการควบคุมมาใช้งานเพื่อจำกัดผลกระทบจากภัยคุกคาม

- การควบคุมการเข้าถึง: การพิสูจน์ตัวตนและการบริหารจัดการสิทธิเข้าถึงข้อมูล (Identity Management) โดยยึดหลักการให้สิทธิเท่าที่จำเป็น
- ความตระหนักรู้และฝึกอบรม: สร้างความตระหนักรู้ด้านไซเบอร์ (Awareness) ให้กับบุคลากรของกรมฯ อย่างน้อยปีละ ๑ ครั้ง
- ความปลอดภัยของข้อมูล: ป้องกันความลับและความถูกต้องของข้อมูลผ่านการเข้ารหัส และดำเนินการสำรองข้อมูลสำคัญบน ระบบคลาวด์กลางภาครัฐ (GDCC)

๑.๒.๒.๔. การตรวจจับ (Detect - DE): การเฝ้าสังเกตและวิเคราะห์เหตุการณ์ผิดปกติเพื่อตรวจพบอุบัติการณ์ไซเบอร์โดยเร็ว

- การเฝ้าระวังต่อเนื่อง: ใช้ระบบ SOC (Security Operation Center) และ EDR ตรวจสอบพฤติกรรมที่น่าสงสัยและตัวบ่งชี้การบุกรุก (IoC) บนเครือข่ายและเครื่องลูกข่ายตลอด ๒๔ ชั่วโมง
- การวิเคราะห์เหตุการณ์ผิดปกติ: วิเคราะห์ความสัมพันธ์ของข้อมูลจากหลายแหล่งเพื่อระบุขอบเขตของเหตุการณ์ที่เกิดขึ้น

๑.๒.๒.๕. การตอบสนอง (Respond - RS): การดำเนินการทันทีเมื่อตรวจพบอุบัติการณ์ไซเบอร์

- การบริหารจัดการเหตุการณ์: ปฏิบัติตามแผนรับมือภัยคุกคาม (IRP) และ Playbook ที่กำหนดไว้เพื่อระงับเหตุและจำกัดขอบเขตความเสียหายไม่ให้กระจายตัว (Containment)
- การรายงานและการสื่อสาร: รายงานสรุปสถานการณ์ต่ออธิบดี และแจ้งเหตุต่อ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ตามกฎหมาย

๑.๒.๒.๖. การกู้คืน (Recover - RC): การดำเนินกิจกรรมเพื่อคืนสภาพระบบและบริการที่ได้รับผลกระทบ

- การปฏิบัติแผนกู้คืน: กู้คืนระบบสารสนเทศและฐานข้อมูลจาก GDCC ตามลำดับความสำคัญ โดยมีระยะเวลาเป้าหมาย (RTO) ภายใน ๑ วัน สำหรับระบบให้บริการประชาชน
- การสื่อสารการกู้คืน: ประสานงานกับผู้ให้บริการ ISP และหน่วยงานกำกับดูแล รวมถึงอัปเดตข้อมูลสถานะการให้บริการแก่สาธารณะ

การประยุกต์ใช้กรอบงาน NIST CSF ๒.๐ ช่วยให้กรมการจัดหางานสามารถบริหารจัดการความปลอดภัยไซเบอร์ได้อย่างเป็นระบบ มีความยืดหยุ่น (Resilience) และสร้างความเชื่อมั่นในศักยภาพของหน่วยงานต่อประชาชนผู้ใช้บริการ

๑.๒.๓ ประมวลแนวทางปฏิบัติ (Code of Practice) ตามกฎหมายไทย

กรมการจัดหางานในฐานะหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII), ดำเนินการจัดทำนโยบายและแนวปฏิบัติฉบับนี้ให้สอดคล้องกับ "ประมวลแนวทางปฏิบัติ (Code of Practice)" ซึ่งหมายถึง ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนดขึ้น ตามมาตรา ๔๔ แห่ง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยมีสาระสำคัญดังนี้:

- ข้อกำหนดขั้นต่ำตามกฎหมาย: ประมวลแนวทางปฏิบัตินี้เป็นข้อกำหนดขั้นต่ำเพื่อให้กรมฯ มีมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่รวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกันกับระดับประเทศ โดยครอบคลุมมาตรการสำคัญ ๕ ด้าน ได้แก่ การระบุความเสี่ยง, มาตรการป้องกัน, มาตรการตรวจสอบและเฝ้าระวัง, มาตรการเผชิญเหตุ และมาตรการรักษาฟื้นฟูความเสียหาย
- องค์ประกอบสำคัญที่ต้องมี: ตามมาตรา ๔๔ (๑) และ (๒) ประมวลแนวทางปฏิบัติของกรมฯ ต้องประกอบด้วยส่วนสำคัญอย่างน้อย ๒ ส่วนหลัก
    ๑. แผนการตรวจสอบและประเมินความเสี่ยง: ต้องจัดให้มีการตรวจสอบโดยผู้ตรวจประเมินภายในหรือภายนอก อย่างน้อยปีละ ๑ ครั้ง

๒. แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan): เพื่อเตรียมความพร้อมในการเผชิญเหตุและระงับความเสียหายอย่างทันท่วงที

- ความสอดคล้องเชิงบูรณาการ: แนวทางปฏิบัตินี้ถูกร่างขึ้นให้มีความสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม รวมถึงต้องมีความเกี่ยวเนื่องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) เพื่อป้องกันการรั่วไหลของข้อมูลประชาชนที่มาใช้บริการในระบบสำคัญ เช่น ระบบไทยมีงานทำ หรือ ระบบ DOE e-License
- การกำกับดูแลและรายงาน: กรมฯ มีหน้าที่ต้องปฏิบัติตามประมวลแนวทางปฏิบัตินี้อย่างเคร่งครัด และจัดส่งผลสรุปรายงานการดำเนินงานตามรอบปีต่อ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จ

การยึดถือประมวลแนวทางปฏิบัติตามกฎหมายไทยนี้ จะช่วยสร้างศักยภาพในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยของประชาชนตามภารกิจหลักของกรมการจัดหางาน

๑.๓ โครงสร้างการกำกับดูแลและภาวะผู้นำ (Governance & Leadership)

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของกรมการจัดหางานเป็นไปอย่างมีประสิทธิภาพและยั่งยืน กรมฯ กำหนดโครงสร้างการกำกับดูแลและบทบาทความรับผิดชอบตามหลักการภาวะผู้นำและการให้ความสำคัญ (Leadership and Commitment) ดังนี้:

๑.๓.๑ บทบาทของผู้บริหารระดับสูง (Top Management - CEO)

อธิบดีกรมการจัดหางาน ในฐานะผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบสูงสุดต่อความเสี่ยงและความเสียหายที่อาจเกิดขึ้น โดยมีหน้าที่และอำนาจหน้าที่ดังนี้:

- การกำหนดทิศทาง: มั่นใจว่ามีการจัดทำนโยบายและวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับทิศทางเชิงกลยุทธ์ของกรมฯ
- การสนับสนุนทรัพยากร: มั่นใจว่าองค์กรจัดสรรทรัพยากรที่จำเป็น ทั้งด้านงบประมาณ บุคลากร และเทคโนโลยี เพื่อนำนโยบายไปสู่การปฏิบัติอย่างสัมฤทธิผล
- การสร้างวัฒนธรรมความปลอดภัย: สนับสนุนและส่งเสริมวัฒนธรรมองค์กรที่ตระหนักถึงความเสี่ยง จริยธรรม และการปรับปรุงความมั่นคงปลอดภัยอย่างต่อเนื่อง
- การตัดสินใจในภาวะวิกฤต: ทำหน้าที่เป็นหัวหน้าคณะบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team) เพื่อประเมินสถานการณ์และประกาศใช้แผนบริหารความต่อเนื่อง

๑.๓.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

ผู้บริหารที่ได้รับมอบหมายให้รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมฯ (Chief Information Officer: CIO) มีหน้าที่หลักดังนี้

๑. การกำกับนโยบาย: รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ และคำปรึกษาด้านเทคนิคเพื่อให้สอดคล้องกับมาตรฐานสากล

๒. การติดตามตรวจสอบ: ควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตามนโยบายและแนวปฏิบัติอย่างเคร่งครัด

๓. การรายงานผล: รายงานประสิทธิภาพและประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง

๑.๓.๓ คณะกรรมการบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team) ประกอบด้วยผู้บริหารระดับสำนัก/กอง/ศูนย์/กลุ่ม มีโครงสร้างและหน้าที่ดังนี้

- หัวหน้าทีม (ผู้อำนวยการสำนัก/กอง): สนับสนุนการปฏิบัติงานตามแผนต่อเนื่อง และสรรหาทรัพยากรในส่วนงานของตนเมื่อเกิดเหตุวิกฤต
- ผู้ประสานงาน (เลขานุการกรม): ทำหน้าที่ติดต่อประสานงานภายในและภายนอกหน่วยงาน รวมถึงอำนวยความสะดวกในการสื่อสารตามผังการแจ้งเหตุ (Call Tree)
- ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร: รับผิดชอบการบริหารจัดการระบบเครือข่าย ฐานข้อมูล และการสำรองข้อมูลบนระบบคลาวด์กลางภาครัฐ (GDCC)

๑.๓.๔ การแบ่งแยกหน้าที่ (Segregation of Duties)

กรมการจัดหางานกำหนดให้มีการแยกหน้าที่ความรับผิดชอบที่อาจก่อให้เกิดการขัดกันของผลประโยชน์ออกจากกัน เพื่อป้องกันการทุจริตหรือความผิดพลาดที่มีนัยสำคัญ

- แยกส่วนงานปฏิบัติการและงานตรวจสอบ: บุคลากรที่ทำหน้าที่ดูแลระบบ (System Administrator) ต้องไม่ใช่บุคคลเดียวกับผู้ตรวจสอบระบบ (Internal Auditor)
- การควบคุมสิทธิเข้าถึง: การมอบหมายอำนาจหน้าที่ต้องเป็นไปตามหลักการสิทธิขั้นต่ำที่จำเป็น (Least Privilege) และมีการทบทวนสิทธิโดยผู้บริหารที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง

๑.๓.๕ การติดตามและการกำกับดูแล (Oversight)

กรมฯ ต้องจัดให้มีการประเมินผลการดำเนินงานและการบริหารจัดการความเสี่ยงเป็นระยะ เพื่อให้มั่นใจว่ามาตรการที่กำหนดมีความครอบคลุมและเพียงพอต่อภัยคุกคามปัจจุบัน:

- การทบทวนของฝ่ายบริหาร: ผู้บริหารระดับสูงต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนด
- การรายงานเหตุการณ์: กำหนดหน้าที่ให้เจ้าหน้าที่ทุกคนต้องรายงานเหตุการณ์ผิดปกติหรือจุดอ่อนที่พบผ่านช่องทางการรายงานที่กำหนดทันที

๑.๔ การบริหารจัดการทรัพย์สินสารสนเทศและข้อมูล (Asset Management)

เพื่อให้กรมการจัดหางานสามารถระบุและบริหารจัดการทรัพย์สินที่จำเป็นต่อการดำเนินภารกิจให้บรรลุวัตถุประสงค์ทางธุรกิจได้อย่างมั่นคงปลอดภัย กรมฯ จึงกำหนดแนวทางปฏิบัติดังนี้

๑.๔.๑ การระบุและจัดทำบัญชีทรัพย์สิน (Asset Identification and Inventory)

- การระบุทรัพย์สิน: กรมฯ ต้องระบุทรัพย์สินสารสนเทศทั้งหมดที่ช่วยให้องค์กรบรรลุวัตถุประสงค์ทางธุรกิจและพันธกิจ
- ประเภททรัพย์สิน: ทรัพย์สินในขอบเขตการกำกับดูแลครอบคลุมถึง:
    - ข้อมูล (Data): ข้อมูลสารสนเทศในรูปแบบเอกสารและอิเล็กทรอนิกส์ ข้อมูลจราจรคอมพิวเตอร์ และชุดข้อมูลสำคัญด้านแรงงาน
    - ซอฟต์แวร์และบริการ (Software and Services): ระบบงานสำคัญ เช่น ระบบ DOE e-License, ระบบไทยมีงานทำ, และระบบบริหารจัดการแรงงานต่างด้าว (e-WorkPermit)
    - ฮาร์ดแวร์ (Hardware): เครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่าย อุปกรณ์สนับสนุนในห้อง Data Center และอุปกรณ์ปลายทางของผู้ใช้งาน
    - บุคลากร (Personnel): ข้าราชการ ลูกจ้าง และบุคคลภายนอกที่ปฏิบัติงานในหน้าที่ด้านไอที
- บัญชีทรัพย์สิน: ต้องจัดทำและปรับปรุงบัญชีทรัพย์สิน (Asset Inventory) ให้เป็นปัจจุบันและถูกต้องเสมอ โดยครอบคลุมทั้งฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล รวมถึงบริการที่ใช้จากผู้ให้บริการภายนอก
- แผนผังเครือข่าย: ต้องจัดทำแผนผังแสดงการไหลของข้อมูล (Data Flow) และแผนผังการสื่อสารผ่านเครือข่ายที่ได้รับอนุญาตทั้งภายในและภายนอก และต้องทบทวนอย่างสม่ำเสมอ

๑.๔.๒ การกำหนดเจ้าของทรัพย์สิน (Asset Ownership)

- ทรัพย์สินสารสนเทศทุกรายการต้องระบุ เจ้าของทรัพย์สิน (Owner) ที่ชัดเจน เพื่อรับผิดชอบในการจัดลำดับความสำคัญและควบคุมการเข้าถึง
- เจ้าของทรัพย์สินต้องเป็นบุคคลซึ่งรับผิดชอบในการบริหารงานหรือดูแลระบบนั้น ๆ และมีหน้าที่ทบทวนสิทธิการใช้งานอย่างน้อยปีละ ๑ ครั้ง

๑.๔.๓ การจัดชั้นความลับและการบ่งชี้ข้อมูล (Information Classification and Labeling)

- การแยกหมวดหมู่: ข้อมูลต้องได้รับการแยกหมวดหมู่ตามความสำคัญต่อพันธกิจ โดยพิจารณาจากความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability)
- ระดับชั้นความลับ: กรมฯ กำหนดระดับความสำคัญเป็น ๓ ระดับ และจัดแบ่งลำดับชั้นความลับตามระเบียบว่าด้วยการรักษาความลับของทางราชการ ได้แก่ "ลับที่สุด", "ลับมาก", "ลับ", และ "ทั่วไป"
- การบ่งชี้ข้อมูล: ต้องกำหนดขั้นตอนการบ่งชี้ข้อมูล (Labeling) ให้สอดคล้องกับลำดับชั้นความลับที่กำหนดไว้ เพื่อให้ผู้ใช้งานทราบถึงมาตรการการดูแลรักษาที่เหมาะสม

๑.๔.๔ การใช้งานทรัพย์สินอย่างเหมาะสมและการส่งคืน (Acceptable Use and Return of Assets)

- กฎเกณฑ์การใช้งาน: กรมฯ ต้องจัดทำกฎเกณฑ์การใช้งานที่ยอมรับได้ (Acceptable Use Policy: AUP) และขั้นตอนปฏิบัติสำหรับการจัดการข้อมูลและทรัพย์สินเป็นลายลักษณ์อักษร

- ความรับผิดชอบผู้ใช้งาน: ผู้ใช้งานมีหน้าที่ดูแลรักษาอุปกรณ์และข้อมูลที่ได้รับมอบหมายเสมือนเป็นทรัพย์สินของตนเอง และห้ามนำไปใช้เพื่อประโยชน์ทางการค้าส่วนตน
- การส่งคืนทรัพย์สิน: บุคลากรและผู้รับจ้างภายนอกต้องคืนทรัพย์สินสารสนเทศทั้งหมดของกรมฯ เมื่อสิ้นสุดสัญญาจ้างหรือพ้นสภาพการปฏิบัติงาน

๑.๔.๕ การบริหารจัดการทรัพย์สินตลอดวงจรชีวิต (Life Cycle Management)

- ต้องบริหารจัดการระบบ ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล ตลอดวงจรชีวิต ตั้งแต่การจัดหา การใช้งาน การบำรุงรักษา จนถึงการทำลาย
- การทำลายข้อมูล: อุปกรณ์ที่มีสื่อบันทึกข้อมูลต้องได้รับการตรวจสอบและลบข้อมูลสำคัญทิ้งอย่างมั่นคงปลอดภัย (Secure Disposal) ก่อนการจำหน่ายออกหรือนำไปใช้งานอย่างอื่น
- การสำรองข้อมูล: ข้อมูลสำคัญต้องมีการสำรอง (Backup) และทดสอบการกู้คืนอย่างสม่ำเสมอตามนโยบายที่กำหนด โดยจัดเก็บไว้ในสถานที่ที่ปลอดภัยและห่างจากสถานที่ปฏิบัติงานหลัก

๑.๕ การบริหารจัดการความเสี่ยง (Risk Management)

เพื่อให้กรมการจัดหางานสามารถระบุ ประเมิน และจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบและต่อเนื่อง กรมฯ จึงกำหนดแนวทางปฏิบัติดังนี้

๑.๕.๑ วัตถุประสงค์ของการบริหารความเสี่ยง

- เพื่อระบุภัยคุกคามและจุดอ่อนที่อาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของระบบสารสนเทศสำคัญ เช่น ระบบ DOE e-License และ ระบบไทยมีงานทำ
- เพื่อช่วยในการตัดสินใจเลือกมาตรการควบคุมที่เหมาะสมและคุ้มค่าที่สุดในการลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Risk Appetite)
- เพื่อให้สอดคล้องกับมาตรา ๔๔ และ ๕๔ ของ พรบ. ไซเบอร์ฯ ที่กำหนดให้หน่วยงานรัฐต้องประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๑.๕.๒ กระบวนการประเมินความเสี่ยง (Risk Assessment)

กรมฯ ต้องดำเนินการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยครอบคลุมขั้นตอนดังนี้

- การระบุความเสี่ยง (Risk Identification): ระบุทรัพย์สินสารสนเทศ เจ้าของความเสี่ยง ภัยคุกคาม (เช่น อุทกภัย, การจู่โจมทางคอมพิวเตอร์) และจุดอ่อนของระบบ
- การวิเคราะห์ความเสี่ยง (Risk Analysis): ประเมินระดับความรุนแรงของผลกระทบ (Impact) และโอกาสที่จะเกิดเหตุการณ์ (Likelihood)
- การประเมินระดับความเสี่ยง (Risk Evaluation): เปรียบเทียบผลการวิเคราะห์ความเสี่ยงกับเกณฑ์ที่กำหนดไว้ เพื่อจัดลำดับความสำคัญของความเสี่ยงที่ต้องเร่งจัดการ

๑.๕.๓ กลยุทธ์การจัดการความเสี่ยง (Risk Treatment)

เมื่อทราบระดับความเสี่ยงแล้ว กรมฯ ต้องกำหนดทางเลือกในการจัดการความเสี่ยงที่เหมาะสม

- การลดความเสี่ยง (Risk Mitigation): การนำมาตรการควบคุมทั้งทางเทคนิคและกายภาพมาใช้งานเพื่อลดโอกาสหรือผลกระทบ
- การยอมรับความเสี่ยง (Risk Acceptance): ในกรณีที่ระดับความเสี่ยงอยู่ในเกณฑ์ที่ยอมรับได้ หรือมีค่าใช้จ่ายในการป้องกันสูงเกินความจำเป็น โดยต้องได้รับการอนุมัติจากผู้บริหารสูงสุด
- การโอนย้ายความเสี่ยง (Risk Transfer): เช่น การใช้บริการคลาวด์กลางภาครัฐ (GDCC) เพื่อเพิ่มความยืดหยุ่นและการสำรองข้อมูล
- การหลีกเลี่ยงความเสี่ยง (Risk Avoidance): ยกเลิกกิจกรรมหรือกระบวนงานที่มีความเสี่ยงสูงเกินกว่าที่จะจัดการได้

๑.๕.๔ การติดตามและทบทวน (Monitoring and Oversight)

- การเฝ้าระวังอย่างต่อเนื่อง: ต้องมีการตรวจสอบความเปลี่ยนแปลงของบริบทองค์กรและภัยคุกคามใหม่ ๆ อย่างสม่ำเสมอ
- การรายงานผล: ผลการประเมินความเสี่ยงและสถานะของแผนจัดการความเสี่ยงต้องถูกรายงานต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) และอธิบดีกรมการจัดหางาน (CEO) เพื่อทบทวนประสิทธิภาพ
- การซักซ้อมแผน: บูรณาการผลการประเมินความเสี่ยงเข้ากับ แผนบริหารความพร้อมต่อสภาวะวิกฤต (BCP) โดยต้องมีการซักซ้อมอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่ามาตรการที่มีอยู่สามารถรับมือภัยคุกคามได้จริง

๑.๕.๕ การจัดทำเอกสารหลักฐาน

กรมฯ ต้องจัดเก็บผลการประเมินความเสี่ยง แผนจัดการความเสี่ยง และเอกสารแสดงการใช้มาตรการควบคุม (Statement of Applicability - SoA) ไว้เป็นลายลักษณ์อักษร เพื่อใช้เป็นหลักฐานในการตรวจสอบและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ต่อไป

๑.๖ มาตรการควบคุมการเข้าถึงและการพิสูจน์ตัวตน (Access Control)

เพื่อให้การเข้าถึงข้อมูลและทรัพย์สินสารสนเทศของกรมการจัดหางานเป็นไปอย่างมั่นคงปลอดภัย ป้องกันการเข้าถึงโดยมิชอบ และมั่นใจได้ว่าเฉพาะผู้ที่มีสิทธิเท่านั้นที่สามารถเข้าถึงระบบได้ กรมฯ จึงกำหนดแนวปฏิบัติไว้ดังนี้

๑.๖.๑ หลักการทั่วไปในการควบคุมการเข้าถึง (Access Control Principles)

- การอนุญาตสิทธิตามความจำเป็น (Business Requirement): การกำหนดสิทธิเข้าถึงข้อมูลและระบบต้องขึ้นอยู่กับความต้องการทางธุรกิจ หน้าที่ความรับผิดชอบ และนโยบายความมั่นคงปลอดภัยสารสนเทศ

- หลักการสิทธิขั้นต่ำที่จำเป็น (Least Privilege): ผู้ใช้งานจะได้รับสิทธิเข้าถึงเฉพาะข้อมูลและระบบที่จำเป็นต่อการปฏิบัติงานตามหน้าที่เท่านั้น
- การแบ่งแยกหน้าที่ (Segregation of Duties): ต้องแยกหน้าที่การอนุมัติ การปฏิบัติงาน และการตรวจสอบออกจากกัน เพื่อป้องกันการทุจริตหรือความผิดพลาดที่ตรวจไม่พบ

๑.๖.๒ การบริหารจัดการอัตลักษณ์ (Identity Management)

- การระบุตัวตน (Identification): ผู้ใช้งานทุกคนต้องมีชื่อบัญชีผู้ใช้งาน (Username) เฉพาะตัว ห้ามใช้บัญชีร่วมกัน (Shared Account) เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- วงจรชีวิตอัตลักษณ์ (Identity Lifecycle): กรมฯ ต้องบริหารจัดการข้อมูลอัตลักษณ์ตั้งแต่การเริ่มสร้าง การปรับปรุง จนถึงการยกเลิกเมื่อพ้นสภาพการปฏิบัติงาน
- การลงทะเบียน: ผู้ใช้งานต้องลงทะเบียนและผ่านการตรวจสอบตัวตนก่อนได้รับสิทธิเข้าสู่ระบบเครือข่ายและระบบงานสำคัญ เช่น ระบบ DOE e-License

๑.๖.๓ การพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย (Authentication)

- วิธีการพิสูจน์ตัวตน: ต้องมีการยืนยันตัวตน (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงก่อนเข้าถึงระบบ
- มาตรฐานรหัสผ่าน (Password Management)
    - รหัสผ่านต้องมีความยาวไม่น้อยกว่า ๑๒ ตัวอักษร และประกอบด้วยตัวอักษรใหญ่ เล็ก ตัวเลข และสัญลักษณ์พิเศษ
    - ห้ามใช้ข้อมูลส่วนบุคคลที่คาดเดาง่ายเป็นรหัสผ่าน (เช่น วันเกิด หรือชื่อนามสกุล)
    - ต้องเปลี่ยนรหัสผ่านทุก ๆ ๑๘๐ วัน หรือตามที่ระบบกำหนด
- การพิสูจน์ตัวตนหลายปัจจัย (MFA): สำหรับการเข้าถึงระบบจากภายนอก (Remote Access) หรือการเข้าถึงระบบที่มีความสำคัญสูง ต้องใช้การพิสูจน์ตัวตนหลายปัจจัยร่วมกับการเข้ารหัสช่องทางสื่อสาร (เช่น VPN)

๑.๖.๔ การบริหารจัดการสิทธิการเข้าถึง (Access Rights Management)

- สิทธิการเข้าถึงระดับพิเศษ (Privileged Access Rights): การให้สิทธิระดับผู้ดูแลระบบ (Admin) ต้องมีการจำกัดจำนวนผู้ใช้งานอย่างเคร่งครัดและต้องมีการทบทวนสิทธิอย่างสม่ำเสมอ
- การทบทวนสิทธิ (Access Rights Review): ผู้ดูแลระบบร่วมกับหัวหน้าหน่วยงานต้นสังกัดต้องทบทวนสิทธิการเข้าใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าสิทธิที่ได้รับยังคงสอดคล้องกับหน้าที่ปัจจุบัน
- การยกเลิกสิทธิ: ต้องดำเนินการยกเลิกหรือถอดถอนสิทธิการเข้าถึงทันที (ภายใน ๓ วัน) เมื่อบุคลากรลาออก หรือเปลี่ยนแปลงหน้าที่งาน

๑.๖.๕ มาตรการควบคุมการเข้าถึงตามระดับความสำคัญ (Specific Access Controls)

- การควบคุมระดับเครือข่าย: ต้องมีการแบ่งแยกเครือข่าย (Network Segregation) ระหว่างเครือข่ายภายใน (Intranet) และภายนอก (Internet) เพื่อป้องกันการเข้าถึงข้อมูลสำคัญ
- การตัดการเชื่อมต่ออัตโนมัติ (Session Time-out): ระบบต้องกำหนดให้มีการหยุดพักการทำงานและต้องการการพิสูจน์ตัวตนใหม่ หากไม่มีกิจกรรมการใช้งานเกินกว่า ๓๐ นาที (หรือ ๑๕ นาที สำหรับระบบที่มีความเสี่ยงสูง)
- โต๊ะทำงานปลอดเอกสารและหน้าจอ (Clear Desk and Clear Screen): ผู้ใช้งานต้องล็อกหน้าจอคอมพิวเตอร์ทุกครั้งเมื่อไม่ได้อยู่ที่โต๊ะทำงาน และจัดเก็บเอกสารที่มีข้อมูลลับไว้ในตู้ที่ล็อกมิดชิด

๑.๗ ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

เพื่อให้ทรัพย์สินสารสนเทศและระบบงานสำคัญของกรมการจัดหางานได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต ความเสียหายจากภัยพิบัติทางธรรมชาติ หรืออุบัติภัยต่าง ๆ กรมฯ จึงกำหนดแนวปฏิบัติไว้ดังนี้

๑.๗.๑ การกำหนดขอบเขตและการควบคุมการเข้าออก (Physical Security Perimeter and Entry)

- การกำหนดพื้นที่ควบคุม: กรมฯ ต้องกำหนดพื้นที่ปฏิบัติงานและพื้นที่ควบคุมเฉพาะให้ชัดเจน โดยเฉพาะพื้นที่ที่มีข้อมูลสำคัญและทรัพย์สินที่เกี่ยวข้องตั้งอยู่
- มาตรการควบคุมการเข้า-ออก: พื้นที่ควบคุมเฉพาะ เช่น ศูนย์ข้อมูล (Data Center) และห้องเครือข่าย ต้องมีการควบคุมจุดเข้า-ออกอย่างเหมาะสม
    - ต้องใช้ระบบการพิสูจน์ตัวตนทางกายภาพ เช่น การพิมพ์ลายนิ้วมือ (Finger Scan)
    - ต้องติดตั้งกล้องวงจรปิด (CCTV) เพื่อเฝ้าระวังและบันทึกภาพการเข้า-ออกตลอด ๒๔ ชั่วโมง
    - บุคคลภายนอกที่ต้องเข้าพื้นที่ควบคุมต้องลงบันทึกในแบบฟอร์มขออนุญาตและมีเจ้าหน้าที่กำกับดูแลตลอดเวลา

๑.๗.๒ ความมั่นคงปลอดภัยของศูนย์ข้อมูลและสิ่งอำนวยความสะดวก (Data Center and Facilities)

- การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม: ต้องมีการออกแบบมาตรการป้องกันภัยพิบัติทางธรรมชาติและอุบัติภัย (เช่น อัคคีภัย หรือน้ำท่วม) อย่างเป็นรูปธรรม
- ระบบสนับสนุน (Supporting Utilities): ระบบประมวลผลข้อมูลต้องได้รับการป้องกันจากการหยุดชะงักของระบบสาธารณูปโภค โดยต้องมีระบบสนับสนุนที่เพียงพอดังนี้:
    - เครื่องกำเนิดไฟฟ้าสำรอง และระบบสำรองไฟฟ้า (UPS)
    - ระบบระงับเพลิง อัตโนมัติที่เหมาะสมกับอุปกรณ์อิเล็กทรอนิกส์
    - ระบบควบคุมอุณหภูมิและความชื้น พร้อมระบบแจ้งเตือนเมื่อทำงานผิดปกติ

๑.๗.๓ ความมั่นคงปลอดภัยของสายสัญญาณและอุปกรณ์ (Cabling and Equipment Security)

- การเดินสายสัญญาณ (Cabling Security): สายสัญญาณไฟฟ้าและสายสื่อสารต้องได้รับการป้องกันจากการแทรกแซงหรือการทำให้เสียหาย โดยควรเดินสายแยกจากกันและร้อยท่อเพื่อป้องกันการดักจับสัญญาณ
- การบำรุงรักษาอุปกรณ์: อุปกรณ์ต้องได้รับการบำรุงรักษาตามรอบระยะเวลาเพื่อให้พร้อมใช้งานและรักษาความถูกต้องของข้อมูลเสมอ โดยต้องมีการบันทึกกิจกรรมการบำรุงรักษาไว้เป็นหลักฐาน
- ความมั่นคงปลอดภัยเมื่อใช้งานนอกสถานที่: ทรัพย์สินที่นำไปใช้งานนอกองค์กร (เช่น Notebook) ต้องได้รับการป้องกันความเสี่ยงจากการสูญหายหรืออุบัติเหตุ และต้องขออนุญาตผู้บริหารก่อนนำออกนอกหน่วยงาน

๑.๗.๔ การปฏิบัติงานในพื้นที่ปลอดภัย (Secure Areas and Working Habits)

- นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและหน้าจอ (Clear Desk and Clear Screen):
    - ผู้ใช้งานต้องล็อกหน้าจอคอมพิวเตอร์ทุกครั้งเมื่อไม่ได้ปฏิบัติงาน ณ โต๊ะทำงาน (แนะนำให้ตั้งระบบล็อกอัตโนมัติภายใน ๑๕-๓๐ นาที)
    - ต้องจัดเก็บเอกสารสำคัญและสื่อบันทึกข้อมูล (เช่น Flash Drive) ไว้ในตู้ที่ล็อกมิดชิดเมื่อไม่ใช้งาน
- การทำลายข้อมูลและอุปกรณ์อย่างมั่นคงปลอดภัย: อุปกรณ์ที่มีสื่อบันทึกข้อมูลต้องได้รับการลบข้อมูลทิ้งอย่างมั่นคงปลอดภัย (เช่น การเขียนทับหลายรอบหรือทุบทำลาย) ก่อนการจำหน่ายออกหรือนำไปใช้งานอย่างอื่น เพื่อให้มั่นใจว่าข้อมูลจะไม่สามารถกู้คืนมาได้

๑.๗.๕ การเฝ้าระวังทางกายภาพอย่างต่อเนื่อง (Physical Security Monitoring)

กรมฯ ต้องจัดให้มีการเฝ้าระวังและติดตามพื้นที่ อาคาร หรือสถานที่ขององค์กรอย่างต่อเนื่อง เพื่อตรวจหาพฤติกรรมผิดปกติหรือตัวบ่งชี้การบุกรุกทางกายภาพ

๑.๘ การสร้างความตระหนักและการฝึกอบรม (Awareness and Training)

เพื่อให้บุคลากรของกรมการจัดหางานมีความรู้ ความเข้าใจ และทักษะที่จำเป็นในการปฏิบัติงานให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ และสามารถตอบสนองต่อภัยคุกคามได้อย่างถูกต้อง กรมฯ จึงกำหนดแนวทางปฏิบัติดังนี้

๑.๘.๑ วัตถุประสงค์ของการสร้างความตระหนักและฝึกอบรม

- เพื่อให้บุคลากรตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศและผลกระทบที่อาจเกิดขึ้นจากการใช้งานระบบอย่างไม่ระมัดระวัง
- เพื่อให้บุคลากรมีทักษะเพียงพอในการปฏิบัติหน้าที่ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- เพื่อให้บุคลากรรับทราบถึงหน้าที่ความรับผิดชอบและบทลงโทษหากมีการละเมิดนโยบาย

๑.๘.๒ การฝึกอบรมสำหรับบุคลากรทั่วไป (General Training)

- ความถี่ในการอบรม: กรมฯ ต้องจัดให้มีการอบรมเพื่อสร้างความรู้และความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรทุกคนอย่างน้อยปีละ ๑ ครั้ง
- บุคลากรใหม่และบุคคลภายนอก: เจ้าหน้าที่ที่เข้าปฏิบัติงานใหม่ หรือบุคคลภายนอก (Third Parties) ที่ได้รับสิทธิ์เข้าใช้งานระบบ ต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติต่าง ๆ ทันทีเมื่อได้รับสิทธิ์
- เนื้อหาหลัก: ครอบคลุมถึงภัยคุกคามไซเบอร์ในปัจจุบัน (เช่น Phishing, Malware), วิธีการใช้งานรหัสผ่านที่ปลอดภัย, และวิธีการรายงานเหตุการณ์ผิดปกติ

๑.๘.๓ การฝึกอบรมสำหรับบุคลากรที่มีบทบาทเฉพาะ (Specialized Training)

- บุคลากรที่มีหน้าที่รับผิดชอบด้านเทคนิคหรือการกำดูแลระบบที่มีความเสี่ยงสูง (เช่น ผู้ดูแลระบบ, ผู้พัฒนาระบบ) ต้องได้รับการฝึกอบรมเชิงลึกเพื่อเพิ่มพูนทักษะที่จำเป็นต่อบทบาทหน้าที่นั้น ๆ
- ต้องมีการทบทวนทักษะเฉพาะด้านเมื่อมีการเปลี่ยนแปลงเทคโนโลยีหรือกระบวนงานที่สำคัญเพื่อให้มั่นใจในความต่อเนื่องและความปลอดภัย

๑.๘.๔ ประเด็นการสร้างความตระหนัก (Awareness Topics)

บุคลากรทุกคนที่ปฏิบัติงานภายใต้การควบคุมของกรมฯ ต้องได้รับการสื่อสารให้ตระหนักถึงประเด็นดังต่อไปนี้

- นโยบายความมั่นคงปลอดภัยสารสนเทศ: เนื้อหาและแนวทางที่เกี่ยวข้องกับงานของตน
- การมีส่วนร่วม: การที่ตนเองมีส่วนช่วยให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสัมฤทธิ์ผล
- ผลที่ตามมา: หากไม่ปฏิบัติตามนโยบายหรือข้อกำหนดด้านความปลอดภัย จะส่งผลกระทบต่อทั้งส่วนตัวและองค์กร รวมถึงโทษทางวินัยและกฎหมาย

๑.๘.๕ หน้าที่ความรับผิดชอบและการรายงาน (Responsibility and Reporting)

- การรายงานเหตุการณ์: บุคลากรมีหน้าที่รายงานเหตุการณ์ที่ตนสังเกตพบหรือสงสัยว่าเกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ผ่านช่องทางที่กำหนดโดยทันที
- การติดตามผล: กรมฯ ต้องประเมินความสัมฤทธิ์ผลของการฝึกอบรมและการสร้างความตระหนักเพื่อนำมาปรับปรุงโปรแกรมการอบรมในอนาคต

๑.๙ การเฝ้าระวังและการตรวจจับภัยคุกคาม (Detection & Monitoring)

เพื่อให้กรมการจัดหางานสามารถตรวจพบพฤติกรรมที่ผิดปกติหรือเหตุการณ์ภัยคุกคามไซเบอร์ได้อย่างทันท่วงที ก่อนที่จะส่งผลกระทบต่อระบบงานสำคัญ เช่น **ระบบ DOE e-License** หรือ **ระบบไทยมีงานทำ** กรมฯ จึงกำหนดแนวปฏิบัติไว้ดังนี้

๑.๙.๑ การเฝ้าระวังอย่างต่อเนื่อง (Continuous Monitoring)

- การเฝ้าระวังเครือข่ายและระบบ: กรมฯ ต้องจัดให้มีการเฝ้าระวังระบบเครือข่าย บริสารด้านเครือข่าย และระบบสารสนเทศทั้งหมดอย่างต่อเนื่อง เพื่อตรวจหาพฤติกรรมที่ผิดปกติหรือตัวบ่งชี้การบุกรุก (Indicators of Compromise: IoC)
- ขอบเขตการเฝ้าระวัง: ครอบคลุมถึงกิจกรรมของบุคลากร การใช้งานเทคโนโลยีจากภายนอก และสภาพแวดล้อมทางกายภาพ รวมถึงการเฝ้าระวังบริการที่ใช้บน ระบบคลาวด์กลางภาครัฐ (GDCC)
- เครื่องมือตรวจจับ: ต้องมีการติดตั้งและดูแลรักษาเครื่องมือตรวจจับการบุกรุก (เช่น IDS/IPS) และระบบป้องกันไวรัส (Anti-malware) ให้มีความเป็นปัจจุบันและพร้อมใช้งานเสมอ

๑.๙.๒ การบันทึกและบริหารจัดการข้อมูลล็อก (Logging)

- การบันทึกเหตุการณ์: ต้องจัดให้มีการบันทึกข้อมูลจราจรและเหตุการณ์สำคัญ (Audit Logging) เช่น ข้อมูลการเข้าและออกจากระบบ (Log in/out) ทั้งที่สำเร็จและไม่สำเร็จ, การแก้ไขสิทธิ์ผู้ใช้งาน, และการเปลี่ยนการตั้งค่าระบบ (Configuration)
- การป้องกันข้อมูลล็อก: ข้อมูลล็อกต้องได้รับการจัดเก็บไว้อย่างมั่นคงปลอดภัย เพื่อป้องกันการถูกลบหรือแก้ไขโดยมิชอบ และต้องสามารถนำมาวิเคราะห์ย้อนหลังได้เมื่อเกิดเหตุการณ์
- การซิงโครไนซ์เวลา: นาฬิกาของระบบสารสนเทศทั้งหมดต้องได้รับการตั้งค่าให้เที่ยงตรงตรงกันโดยอ้างอิงจากแหล่งเทียบเวลาที่ได้รับการรับรอง เพื่อประโยชน์ในการตรวจสอบความสัมพันธ์ของเหตุการณ์ (Correlation)

๑.๙.๓ การวิเคราะห์เหตุการณ์ผิดปกติ (Adverse Event Analysis)

- กระบวนการวิเคราะห์: เมื่อตรวจพบความผิดปกติหรือเหตุการณ์ที่น่าสงสัย ต้องมีการนำข้อมูลจากหลายแหล่งมาวิเคราะห์เพื่อหาความสัมพันธ์และกำหนดคุณลักษณะของเหตุการณ์
- การประเมินผลกระทบ: ต้องประเมินขอบเขตและระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นต่อพันธกิจของกรมฯ เพื่อประกอบการตัดสินใจประกาศเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
- ข้อมูลข่าวสารด้านภัยคุกคาม (Threat Intelligence): กรมฯ ต้องมีการเก็บรวบรวมและวิเคราะห์ข้อมูลข่าวสารด้านภัยคุกคามจากแหล่งที่เชื่อถือได้ เพื่อนำมาปรับปรุงมาตรการตรวจจับให้มีประสิทธิภาพ

๑.๙.๔ หน้าหน้าที่และความรับผิดชอบในการตรวจจับ

- ผู้ดูแลระบบและศูนย์ไอที: มีหน้าที่รับผิดชอบในการติดตามเฝ้าระวังหน้าจอระบบ (Monitoring Activities) และรายงานสถานะความผิดปกติต่อผู้บริหารตามสายงาน
- การรายงานโดยบุคลากร: เจ้าหน้าที่ทุกคนมีหน้าที่รายงานพฤติกรรมที่ผิดปกติหรือจุดอ่อนด้านความปลอดภัยที่พบเห็นผ่านช่องทางที่กำหนดโดยทันที

๑.๙.๕ การประสานงานและการรายงานเหตุการณ์ภายนอก

- การรายงานตามกฎหมาย: เมื่อเกิดเหตุภัยคุกคามไซเบอร์ที่มีนัยสำคัญ กรมฯ ต้องรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และหน่วยงานกำกับดูแลที่เกี่ยวข้องโดยเร็ว ตามมาตรา ๕๗ แห่ง พรบ. ไซเบอร์ฯ
- การแจ้งเตือน: ในกรณีที่มีความเสี่ยงสูง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ต้องพิจารณาแจ้งเตือนไปยังหน่วยงานภายในและคู่ค้าที่เกี่ยวข้องตามผังการแจ้งเหตุ (Call Tree) เพื่อเตรียมการรับมือ

บทที่ ๒

แผนบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Plan - BCP)

๒.๑ บทนำ

ในสภาวะปัจจุบันที่โลกมีการเปลี่ยนแปลงอย่างรวดเร็ว กรมการจัดหางานในฐานะหน่วยงานที่มีภารกิจหลักในการให้บริการประชาชนและภาคธุรกิจด้านแรงงาน จำเป็นต้องเตรียมความพร้อมเพื่อรับมือกับสถานการณ์วิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ ที่อาจเกิดขึ้นโดยไม่คาดคิด แผนบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Plan: BCP) ฉบับนี้จึงถูกจัดทำขึ้นเพื่อใช้เป็นแนวทางปฏิบัติในการตอบสนองต่อเหตุการณ์ที่ส่งผลให้การดำเนินงานปกติหยุดชะงัก ไม่ว่าเหตุการณ์นั้นจะเกิดจากภัยธรรมชาติ (เช่น อุทกภัย อัคคีภัย แผ่นดินไหว) หรือภัยที่มนุษย์สร้างขึ้น (เช่น การชุมนุมประท้วง การจลาจล การจู่โจมทางคอมพิวเตอร์ หรือโรคระบาดร้ายแรง)

๒.๑.๒ ความสำคัญของการบริหารความต่อเนื่อง (Importance) การบริหารความพร้อมต่อสภาวะวิกฤตมีความสำคัญยิ่งต่อกรมการจัดหางานในมิติต่าง ๆ ดังนี้

- การรักษากระบวนงานที่สำคัญ (Critical Business Process): เพื่อให้กรมฯ สามารถดำเนินภารกิจหลักและให้บริการประชาชนได้อย่างต่อเนื่องและเป็นระบบ แม้ในยามที่เกิดสภาวะไม่ปกติ โดยมุ่งเน้นการปกป้องบุคลากร ทรัพย์สิน และข้อมูลสำคัญขององค์กร
- การลดและบรรเทาความเสียหาย: หากหน่วยงานไม่มีแผนรองรับภายใต้สภาวะวิกฤต อาจก่อให้เกิดผลกระทบรุนแรงในหลายด้าน ทั้งด้านเศรษฐกิจ การเงิน สังคม ตลอดจนความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชนและเจ้าหน้าที่ แผน BCP จะช่วยลดระดับความรุนแรงของผลกระทบให้กลับคืนสู่สภาวะปกติภายในระยะเวลาที่เหมาะสม
- การรักษาความพร้อมใช้ของระบบบริการ (Availability): เพื่อให้ระบบบริการอิเล็กทรอนิกส์ (e-Services) เช่น ระบบไทยมีงานทำ หรือระบบ DOE e-License สามารถให้บริการประชาชนได้ทุกที่ทุกเวลา ลดความจำเป็นในการติดต่อ ณ สำนักงาน ซึ่งเป็นการลดความเสี่ยงจากเหตุการณ์ฉุกเฉินต่าง ๆ ไปในตัว
- การสร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย: เพื่อให้ประชาชน นายจ้าง และผู้มีส่วนได้ส่วนเสีย (Stakeholders) ทุกภาคส่วน มีความเชื่อมั่นในศักยภาพของกรมการจัดหางาน ว่าจะสามารถกอบกู้สถานการณ์และให้บริการได้อย่างต่อเนื่องแม้ต้องเผชิญกับสถานการณ์ร้ายแรง

ดังนั้น การกำหนดแผนบริหารความต่อเนื่องจึงเป็นเครื่องมือทางกลยุทธ์ที่ช่วยยกระดับความมั่นคงปลอดภัยไซเบอร์และความพร้อมทางโครงสร้างพื้นฐานของกรมฯ ให้สอดคล้องกับมาตรฐานสากลและบทบัญญัติแห่งกฎหมาย

๒.๒ สมมติฐานและขอบเขตของแผน BCP

เพื่อให้แผนบริหารความพร้อมต่อสภาวะวิกฤต (BCP) ของกรมการจัดหางานสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและตั้งอยู่บนพื้นฐานของความเป็นจริง กรมฯ จึงได้กำหนดสมมติฐานและขอบเขตของแผนไว้ดังนี้

๒.๒.๑ สมมติฐานของแผน BCP (BCP Assumptions) การจัดทำแผนฉบับนี้ตั้งอยู่บนสมมติฐานสำคัญ ๓ ประการ เพื่อให้การจัดเตรียมทรัพยากรสำรองมีความชัดเจน

- สถานที่ปฏิบัติงานสำรองไม่ได้รับผลกระทบ: สมมติว่าเหตุการณ์ฉุกเฉินที่เกิดขึ้น ณ สถานที่ปฏิบัติงานหลัก (อาคารกรมการจัดหางาน ดินแดง) ในช่วงเวลาต่าง ๆ นั้น มิได้ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองที่ได้มีการจัดเตรียมไว้ (เช่น ศูนย์ Smart Job Center หรืออาคารสำนักงานประกันสังคม เขตพื้นที่ ๓)
- ระบบไอทีสำรองมีความพร้อม: หน่วยงานเทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) รับผิดชอบในการสำรองระบบสารสนเทศและข้อมูลสำคัญ โดยระบบสารสนเทศสำรองนั้นต้องตั้งอยู่ในสภาพแวดล้อมที่ไม่ได้รับผลกระทบจากเหตุการณ์ฉุกเฉินเดียวกันกับระบบสารสนเทศหลัก
- การครอบคลุมบุคลากร: คำว่า “บุคลากร” ในแผนนี้ หมายถึง บุคลากรทั้งหมดของหน่วยงานในส่วนกลาง ได้แก่ สำนัก/กอง และสำนักงานจัดหางานกรุงเทพมหานครพื้นที่ ๑ - ๑๐

๒.๒.๒ ขอบเขตของแผน BCP (Scope of BCP)

แผนฉบับนี้ใช้รองรับกรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินภายในสำนักงานหรือบริเวณใกล้เคียง ซึ่งส่งผลกระทบต่อทรัพยากรหลัก ๕ ประเภท (อาคาร, วัสดุอุปกรณ์, เทคโนโลยี, บุคลากร และคู่ค้า) โดยครอบคลุมเหตุการณ์ดังต่อไปนี้

- เหตุการณ์ภัยธรรมชาติ: ได้แก่ อุทกภัย (น้ำท่วม), อัคคีภัย (ไฟไหม้) และแผ่นดินไหว
- เหตุการณ์ภัยจากมนุษย์: ได้แก่ การชุมนุมประท้วง หรือการจลาจลที่ส่งผลต่อการเข้าปฏิบัติงานในอาคาร
- เหตุการณ์ด้านสาธารณสุข: ได้แก่ โรคระบาดหรือการแพร่ระบาดของโรคติดเชื้อไวรัสที่ทำให้ไม่สามารถรวมตัวกันปฏิบัติงานในสถานที่ปกติได้
- เหตุการณ์ภัยคุกคามไซเบอร์: ครอบคลุมถึงการจู่โจมทางคอมพิวเตอร์ที่ส่งผลให้ระบบงานสำคัญ (เช่น ระบบ DOE e-License หรือระบบไทยมีงานทำ) หยุดชะงัก

๒.๒.๓ ข้อยกเว้นของแผน (Exclusions) แผน BCP ฉบับนี้ ไม่รองรับ กรณีดังต่อไปนี้

- เหตุขัดข้องที่เกิดขึ้นจากการปฏิบัติภารกิจตามปกติ (Normal Operations)
- เหตุการณ์ที่ไม่มีผลกระทบระดับสูงต่อการดำเนินงานหรือการให้บริการประชาชน

- เหตุการณ์ที่หน่วยงานยังสามารถจัดการหรือปรับปรุงแก้ไขได้ภายในระยะเวลาที่เหมาะสมโดยผู้บริหารกลุ่มงานหรือฝ่ายงานตามขั้นตอนปกติ

๒.๓ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis - BIA)

การวิเคราะห์ผลกระทบทางธุรกิจ (BIA) เป็นกระบวนการระบุและประเมินผลกระทบที่อาจเกิดขึ้นต่อการดำเนินภารกิจของกรมการจัดหางานเมื่อเกิดเหตุหยุดชะงัก เพื่อจัดลำดับความสำคัญของกระบวนงานและกำหนดระยะเวลาในการกู้คืนระบบ

๒.๓.๑ เกณฑ์การพิจารณาระดับผลกระทบ (Impact Criteria) กรมฯ กำหนดเกณฑ์ความเสียหายหรือความรุนแรงของเหตุการณ์ที่ส่งผลต่อขีดความสามารถในการให้บริการประชาชนและชื่อเสียงขององค์กรเป็น ๕ ระดับ ดังนี้

- ระดับสูงมาก: ขีดความสามารถในการให้บริการลดลงมากกว่า ๕๐% หรือมีการสูญเสียชีวิต
- ระดับสูง: ขีดความสามารถลดลง ๒๕ - ๕๐% และต้องการการบริหารจัดการอย่างเร่งด่วน
- ระดับปานกลาง: ขีดความสามารถลดลง ๑๐ - ๒๕% และมีผลกระทบชัดเจนต่อการดำเนินงาน
- ระดับต่ำ: ขีดความสามารถลดลง ๕ - ๑๐% และส่งผลเล็กน้อยต่อบางหน่วยงาน
- ระดับต่ำมาก: ขีดความสามารถลดลงน้อยกว่า ๕% และไม่กระทบต่อบริการประชาชน

๒.๓.๒ ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective - RTO) เพื่อให้การฟื้นฟูกระบวนงานเป็นไปอย่างเป็นระบบ กรมฯ ได้จัดแบ่งกระบวนงานสำคัญตามระยะเวลาที่ต้องกู้คืนกลับมาให้บริการได้อีกครั้ง ดังนี้

- RTO ๑ วัน (วิกฤต): ระบบสารสนเทศสำหรับให้บริการประชาชน (เช่น ระบบไทยมีงานทำ), ระบบสารบรรณอิเล็กทรอนิกส์, และงานรับคำขอใบอนุญาตภายใต้ระบบ DOE e-License
- RTO ๓ วัน (เร่งด่วน): ระบบเครือข่ายสื่อสารข้อมูล, ระบบการเงินและบัญชี, การเบิกจ่ายเงินและการรับ-ส่งเงิน,
- RTO ๗ วัน (สำคัญ): งานสารบรรณและธุรการ, งานอาคารสถานที่, และงานจัดซื้อจัดจ้าง

๒.๓.๓ การประเมินผลกระทบต่อทรัพยากร (Resource Impact) กรมฯ ประเมินภัยคุกคามโดยพิจารณาถึงผลกระทบต่อทรัพยากรสำคัญ ๕ ประเภท ได้แก่

- ด้านอาคาร/สถานที่: หากอาคารดินแดงเสียหาย ต้องอพยพไปปฏิบัติงาน ณ สถานที่สำรอง
- ด้านวัสดุอุปกรณ์: หากคอมพิวเตอร์หรือเครื่องใช้สำนักงานหลักเสียหาย ต้องมีการจัดหาทดแทนหรือเช่าใช้,
- ด้านเทคโนโลยีและข้อมูล: หากระบบล่ม ข้อมูลสำคัญต้องได้รับการกู้คืนจากระบบคลาวด์ GDCC หรือข้อมูลสำรองนอกสถานที่,

- ด้านบุคลากร: หากบุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ ต้องมีบุคลากรสำรองในกลุ่มงานเดียวกันทำหน้าที่แทน,
- ด้านคู่ค้า/ผู้ให้บริการ: เช่น ผู้ให้บริการอินเทอร์เน็ตหรือระบบเครือข่าย หากขัดข้องต้องมีแผนรองรับการเชื่อมต่อผ่าน Hotspot หรือเครือข่ายสำรอง,

๒.๓.๔ สรุปกระบวนงานที่ต้องให้ความสำคัญลำดับแรก จากการวิเคราะห์ พบว่ากระบวนงานที่มีผลกระทบระดับ "สูงมาก" และ "สูง" ซึ่งต้องเร่งดำเนินการกู้คืนโดยเร็วที่สุด ได้แก่

- การให้บริการผ่านระบบอิเล็กทรอนิกส์ทั้งหมดต่อประชาชนและนายจ้าง
- กระบวนงานที่เกี่ยวข้องกับกองทุนเพื่อช่วยเหลือคนหางานไปทำงานต่างประเทศ
- งานตรวจสอบและพิจารณาใบอนุญาตทำงานคนต่างด้าว
- การบริหารจัดการงบประมาณและการเบิกจ่ายเพื่อให้การดำเนินงานต่อเนื่อง

๒.๔ กลยุทธ์การบริหารความต่อเนื่องและสถานที่ปฏิบัติงานสำรอง

กรมการจัดหางานกำหนดกลยุทธ์เพื่อเป็นแนวทางในการรักษากระบวนงานที่สำคัญให้ดำเนินต่อไปได้ในสภาวะวิกฤต โดยมุ่งเน้นการจัดเตรียมทรัพยากรสำรองในด้านต่าง ๆ ดังนี้

๒.๔.๑ กลยุทธ์การบริหารความต่อเนื่องรายด้าน (Resource-based Strategies)

- กลยุทธ์ด้านอาคารและสถานที่
  - กำหนดให้ใช้สถานที่ปฏิบัติงานสำรองภายนอกหน่วยงาน หรือการปฏิบัติงาน ณ ที่พักอาศัย (Work From Home) สำหรับภารกิจที่สามารถดำเนินการได้ผ่านระบบเครือข่าย
  - มุ่งเน้นการให้บริการประชาชนผ่านระบบ e-Service และระบบอิเล็กทรอนิกส์ เพื่อลดการติดต่อ ณ สำนักงาน ซึ่งช่วยลดความเสี่ยงจากเหตุการณ์ฉุกเฉินได้โดยตรง
- กลยุทธ์ด้านวัสดุอุปกรณ์
  - ในกรณีอุปกรณ์หลักเสียหาย ให้สรรหาอุปกรณ์ที่เหลืออยู่ในหน่วยงานมาใช้งานก่อน หากไม่เพียงพอให้ดำเนินการจัดหาคอมพิวเตอร์สำรอง หรือขอความร่วมมือเจ้าหน้าที่ให้นำคอมพิวเตอร์พกพา (Notebook) ส่วนตัวมาใช้ชั่วคราว
  - สำหรับการป้องกันโรคระบาด ให้จัดตั้งจุดคัดกรองและเตรียมวัสดุอุปกรณ์ด้านสุขอนามัย (หน้ากาก, เจลแอลกอฮอล์) ให้เพียงพอทั้งต่อเจ้าหน้าที่และผู้มารับบริการ
- กลยุทธ์ด้านเทคโนโลยีสารสนเทศและข้อมูล
  - ใช้บริการระบบคลาวด์กลางภาครัฐ (GDCC) เป็นที่ตั้งฐานข้อมูลและระบบงานหลัก เพื่อความปลอดภัยและความพร้อมใช้ระดับสากล
  - จัดทำ Backup ระบบงานและฐานข้อมูลไว้บน GDCC และให้บุคลากรสำรองข้อมูลสำคัญในอุปกรณ์พกพา (External Hard disk/Flash Drive) อย่างสม่ำเสมอ

- ติดตั้งเครื่องกำเนิดไฟฟ้าสำรองสำหรับห้อง Data Center เพื่อป้องกันความเสียหายต่อระบบเมื่อไฟฟ้าขัดข้อง

- กลยุทธ์ด้านบุคลากร
  - กำหนดบุคลากรสำรองทดแทนภายในกลุ่มงานหรือฝ่ายเดียวกันเพื่อให้สามารถปฏิบัติหน้าที่แทนกันได้ทันที
  - ใช้ช่องทางการติดต่อสื่อสารผ่านระบบออนไลน์ (Line, Facebook, Zoom) เพื่อประสานงานในภาวะวิกฤต
- กลยุทธ์ด้านคู่ค้าและผู้ให้บริการ
  - ประสานผู้ให้บริการโครงข่าย (ISP) และผู้ดูแลระบบ GDCC เพื่อทดสอบและเชื่อมต่อการใช้งานระบบสารสนเทศ ณ สถานที่สำรอง
  - ในกรณีอินเทอร์เน็ตหลักขัดข้อง ให้ใช้ระบบสำรองผ่าน Pocket Wi-Fi หรือการแชร์ Hotspot จากโทรศัพท์เคลื่อนที่

๒.๔.๒ สถานที่ปฏิบัติงานสำรอง (Alternate Work Sites)

กรมการจัดหางานได้จัดเตรียมสถานที่ปฏิบัติงานสำรองที่มีความพร้อมด้านสาธารณูปโภค (ไฟฟ้า, ประปา, ระบบปรับอากาศ) ดังนี้

- สำหรับหน่วยงานส่วนกลาง
  - ศูนย์บริการจัดหางานเพื่อคนไทย (Smart Job Center) บริเวณกระทรวงแรงงาน.
  - ศูนย์อบรมคนหางานก่อนไปทำงานต่างประเทศ (ชั้น ๑ อาคารสำนักงานประกันสังคม กทม. พื้นที่ ๓)
  - สนามกีฬาไทย-ญี่ปุ่น, โรงเรียนพิบูลประชาสรรค์ หรือสำนักงานจัดหางานจังหวัดปทุมธานี.
- สำหรับสำนักงานจัดหางานกรุงเทพมหานครพื้นที่ ๑ - ๑๐ (สจก.)
  - ให้ใช้สถานที่ของ สจก. พื้นที่ใกล้เคียง ที่ไม่ได้รับผลกระทบ หรือย้ายเข้าปฏิบัติงาน ณ หน่วยงานส่วนกลางตามความเหมาะสม

๒.๕ โครงสร้างทีมงาน BCP และระบบการแจ้งเหตุฉุกเฉิน (Call Tree)

เพื่อให้แผนบริหารความพร้อมต่อสภาวะวิกฤต (BCP) สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ กรมการจัดหางานจึงได้จัดตั้งคณะบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team) และกำหนดระบบการสื่อสารในภาวะฉุกเฉินดังนี้

๒.๕.๑ โครงสร้างคณะบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team)

คณะบริหารความพร้อมต่อสภาวะวิกฤตของกรมการจัดหางาน มีโครงสร้างที่ครอบคลุมผู้บริหารทุกระดับ เพื่อให้สามารถสั่งการและประสานงานได้อย่างรวดเร็ว

- หัวหน้าคณะบริหารความพร้อมต่อสภาวะวิกฤต: คือ อธิบดีกรมการจัดหางาน

- รองหัวหน้าคณะบริหารความพร้อมต่อสภาวะวิกฤต: คือ รองอธิบดีกรมการจัดหางาน
- ผู้ประสานงานคณะบริหารความพร้อมต่อสภาวะวิกฤต: คือ เลขานุการกรม
- หัวหน้าทีมบริหารความพร้อมต่อสภาวะวิกฤต: ประกอบด้วยผู้บริหารระดับสำนัก/กอง/ศูนย์/กลุ่ม ทั้งในส่วนกลางและสำนักงานจัดหางานกรุงเทพมหานครพื้นที่ ๑ - ๑๐

๒.๕.๒ บทบาทและหน้าที่ความรับผิดชอบ

- หัวหน้าคณะบริหารความพร้อมฯ (อธิบดี): มีหน้าที่ประเมินลักษณะ ขอบเขต และแนวโน้มของสถานการณ์เพื่อตัดสินใจประกาศใช้แผน BCP สั่งการตามขั้นตอนการบริหารความต่อเนื่อง และอนุมัติการสรรหาทรัพยากรที่จำเป็น
- ผู้ประสานงานคณะบริหารความพร้อมฯ (เลขานุการกรม): มีหน้าที่ติดต่อประสานงานทั้งภายในและภายนอกหน่วยงาน สนับสนุนการสื่อสารกับฝ่ายงานต่างๆ และดำเนินการตามขั้นตอนที่กำหนดในแผน
- หัวหน้าทีมบริหารความพร้อมฯ (ผู้บริหารสำนัก/กอง): มีหน้าที่สนับสนุนการปฏิบัติงานของคณะบริหารความต่อเนื่องภายในส่วนงานของตน ดำเนินการกอบกู้กระบวนงาน และจัดหาทรัพยากรตามที่ระบุไว้ในแผน BCP ของแต่ละหน่วยงาน

๒.๕.๓ ระบบการแจ้งเหตุฉุกเฉิน (Call Tree)

กระบวนการ Call Tree คือ ขั้นตอนการแจ้งเหตุฉุกเฉินผ่านผังรายชื่อทางโทรศัพท์เพื่อให้บุคลากรรับทราบสถานการณ์และการประกาศใช้แผน BCP อย่างทั่วถึง

- ลำดับการแจ้งเหตุ: เริ่มจากหัวหน้าคณะบริหารความพร้อมฯ (อธิบดี) แจ้งไปยังผู้ประสานงาน (เลขานุการกรม) จากนั้นผู้ประสานงานจะแจ้งไปยังหัวหน้าทีม (ผู้อำนวยการสำนัก/กอง) และหัวหน้าทีมจะแจ้งต่อไปยังบุคลากรภายใต้บังคับบัญชาตามลำดับ
- ช่องทางการติดต่อ
    - หากเกิดเหตุในเวลาทำการ ให้ใช้เบอร์โทรศัพท์ของหน่วยงานเป็นอันดับแรก
    - หากเกิดเหตุนอกเวลาทำการหรือสถานที่ปฏิบัติงานหลักได้รับผลกระทบ ให้ใช้เบอร์โทรศัพท์มือถือเป็นอันดับแรก
- ข้อมูลที่ต้องแจ้ง: ประกอบด้วยสรุปสถานการณ์ฉุกเฉิน การประกาศใช้แผน BCP เวลานัดประชุมเร่งด่วน และสถานที่รวมพลหรือสถานที่ปฏิบัติงานสำรอง
- การรายงานผล: หัวหน้าหน่วยงานมีหน้าที่โทรกลับมาแจ้งผู้ประสานงานเมื่อติดต่อบุคลากรหลักได้ครบถ้วน เพื่อรายงานสรุปความพร้อมและความปลอดภัยของเจ้าหน้าที่ต่อหัวหน้าคณะบริหารความพร้อมฯ ต่อไป
- การปรับปรุงข้อมูล: ทีมบริหารความพร้อมฯ ต้องปรับปรุงข้อมูลติดต่อให้เป็นปัจจุบันอยู่เสมอ เพื่อให้กระบวนการแจ้งเหตุสัมฤทธิผลภายในระยะเวลาที่คาดหวัง

๒.๖ แนวปฏิบัติกรณีเกิดสภาวะวิกฤตรายเหตุการณ์

เพื่อให้กรมการจัดหางานสามารถตอบสนองต่อสภาวะวิกฤตแต่ละประเภทได้อย่างรวดเร็วและมีประสิทธิภาพ จึงกำหนดแนวทางปฏิบัติเฉพาะกรณีไว้ดังนี้

๒.๖.๑ เหตุการณ์อุทกภัย (Flood)

- การเตรียมพร้อม: เมื่อมีการประกาศใช้แผนอุทกภัย ให้ทีม BCP ติดตามข่าวสารอย่างต่อเนื่อง สำรวจจุดเสี่ยงไฟฟ้ารั่ว และจัดเตรียมอุปกรณ์จำเป็น เช่น ไฟสำรอง เวชภัณฑ์ และเครื่องสูบน้ำ
- การป้องกันทรัพย์สิน: ดำเนินการกั้นกระสอบทรายรอบอาคาร ย้ายทรัพย์สินและเอกสารสำคัญขึ้นพื้นที่สูงเพื่อป้องกันความเสียหาย
- กรณีรุนแรง: ประสานสถานที่ปฏิบัติงานสำรอง และแจ้งช่องทางติดต่อสื่อสารใหม่ให้ประชาชนและหน่วยงานภายนอกทราบทันที
- การจัดการข้อมูล: ให้บุคลากรสำรองข้อมูลที่จำเป็นลงในอุปกรณ์พกพา (External Hard Disk/Flash Drive) และ IT ดำเนินการย้ายระบบงานหลักไปยังคลาวด์หรือสถานที่สำรอง
- การกู้คืน: หลังน้ำลด ให้ตรวจสอบความเสียหายของระบบ Server และอุปกรณ์คอมพิวเตอร์ก่อนนำกลับมาใช้งาน

๒.๖.๒ เหตุการณ์อัคคีภัย (Fire)

- การซักซ้อม: ต้องจัดให้มีการฝึกซ้อมอพยพหนีไฟและตรวจสอบอุปกรณ์ดับเพลิงให้พร้อมใช้งานได้ทันที
- การเผชิญเหตุ: เมื่อพบเพลิงไหม้ลุกลาม ให้เปิดสัญญาณเตือนภัย ตัดกระแสไฟฟ้าในบริเวณที่เกิดเหตุ และแจ้งสถานีดับเพลิงใกล้เคียง
- การอพยพ: บุคลากรต้องออกจากอาคารทางบันไดหนีไฟไปยังจุดรวมพลที่กำหนด ห้ามใช้ลิฟต์โดยเด็ดขาด และหากมีกลุ่มควันให้ใช้วิธีการคลานต่ำ
- การตรวจสอบ: ผู้รับผิดชอบต้องตรวจสอบรายชื่อบุคลากร ณ จุดรวมพล หากพบว่ามีผู้สูญหายให้รีบแจ้งเจ้าหน้าที่กู้ภัยเพื่อช่วยเหลือทันที
- การกู้คืนระบบ: IT ต้องตรวจสอบสถานะของศูนย์ข้อมูล (Data Center) และเครื่องแม่ข่าย หากเสียหายจนใช้งานไม่ได้ให้ประกาศใช้แผนกู้คืนระบบ (DRP) ทันที

๒.๖.๓ เหตุการณ์โรคระบาด (Epidemic/Pandemic)

- มาตรการทางกายภาพ: เพิ่มความถี่ในการทำความสะอาดจุดสัมผัสสาธารณะด้วยน้ำยาฆ่าเชื้อ เช่น ปุ่มกดลิฟต์ ราวบันได และจัดตั้งจุดคัดกรองอุณหภูมิก่อนเข้าอาคาร
- ระยะห่างทางสังคม: จัดที่นั่งในสถานที่ทำงานและห้องประชุมให้เว้นระยะห่าง ๑-๒ เมตร และส่งเสริมให้บุคลากรใส่หน้ากากอนามัยตลอดเวลา

- การปฏิบัติงานระยะไกล: IT ต้องเตรียมความพร้อมของระบบสารสนเทศและระบบประชุมทางไกล (Video Conference) เพื่อรองรับการทำงาน ณ ที่พักอาศัย (Work From Home) ตามมาตรการที่กำหนด
- การเฝ้าระวังบุคลากร: เจ้าหน้าที่ที่มีอาการเสี่ยงหรือประวัติสัมผัสเชื้อต้องรายงานผู้บังคับบัญชาทันที และให้เริ่มปฏิบัติงานที่บ้านพร้อมรายงานผลสุขภาพต่อเนื่องจนกว่าจะปลอดภัย

๒.๖.๔ เหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Attack)

- การตรวจจับ (Detect): เมื่อพบตัวบ่งชี้การบุกรุก (IoC) หรือพฤติกรรมผิดปกติในระบบ เช่น ระบบ DOE e-License หรือ ระบบไทยมีงานทำ ให้ทีม IT วิเคราะห์ระดับความรุนแรงทันที
- การระงับเหตุ (Respond): ดำเนินการจำกัดขอบเขตความเสียหายไม่ให้กระจายตัว (Containment) เช่น ตัดการเชื่อมต่อระบบที่ถูกจู่โจมออกจากเครือข่ายหลัก และระบุสาเหตุพื้นฐานของเหตุการณ์
- การรายงาน: หากเป็นภัยคุกคามที่มีนัยสำคัญ กรมฯ ต้องรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช) ตามมาตรา ๕๗ แห่ง พรบ. ไซเบอร์ฯ พ.ศ. ๒๕๖๒
- การกู้คืน (Recover): ดำเนินการกู้คืนข้อมูลจาก ระบบคลาวด์กลางภาครัฐ (GDCC) ที่มีการสำรองไว้ และตรวจสอบความถูกต้องครบถ้วนของข้อมูลก่อนเปิดให้บริการตามปกติ
- การเรียนรู้: หลังสถานการณ์คลี่คลาย ต้องนำข้อมูลเหตุการณ์มาวิเคราะห์เพื่อเสริมสร้างมาตรการป้องกันและอุดช่องโหว่ทางเทคนิคไม่ให้เกิดเหตุซ้ำ

๒.๗ แนวทางในการเตรียมความพร้อมบุคลากร

เพื่อกอบกู้กระบวนงานของกรมการจัดหางานตามแผนบริหารความพร้อมต่อสภาวะวิกฤต (BCP) มุ่งเน้นทั้งการเตรียมการล่วงหน้าและการบริหารจัดการในช่วงที่เกิดเหตุ โดยมีรายละเอียดดังนี้

ขั้นตอนที่ ๑. การเตรียมความพร้อมล่วงหน้า (Pre-Crisis Preparation)

- การกำหนดบทบาทและหน้าที่ความรับผิดชอบ: จัดตั้งคณะบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team) ที่ประกอบด้วยหัวหน้าคณะ (อธิบดี), ผู้ประสานงาน (เลขานุการกรม) และหัวหน้าทีมงานระดับสำนัก/กอง เพื่อให้บุคลากรทราบสายการบังคับบัญชาในภาวะวิกฤต

- การสร้างความตระหนักและการฝึกอบรม: ต้องจัดให้มีการอบรมบุคลากรเพื่อให้มีความรู้และรู้เท่าทันต่อภัยคุกคาม รวมถึงแนวทางปฏิบัติเมื่อเกิดเหตุฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง
- การกำหนดบุคลากรสำรอง: กำหนดรายชื่อบุคลากรหลักและบุคลากรสำรองในแต่ละหน่วยงานที่สามารถปฏิบัติหน้าที่แทนกันได้ภายในกลุ่มงานหรือฝ่ายเดียวกันทันที

ขั้นตอนที่ ๒. กลยุทธ์การบริหารบุคลากรในช่วงเกิดวิกฤต (Business Continuity Strategy)

- การสื่อสารในภาวะฉุกเฉิน: ใช้กระบวนการ Call Tree เพื่อแจ้งเหตุฉุกเฉินและการประกาศใช้แผน BCP ผ่านโทรศัพท์หน่วยงานหรือโทรศัพท์มือถือ เพื่อให้บุคลากรรับทราบสถานการณ์และสถานที่นัดหมายประชุมเร่งด่วน
- ช่องทางติดต่อสื่อสารสำรอง: ในภาวะวิกฤตที่สถานที่ปฏิบัติงานหลักเสียหาย ให้บุคลากรใช้ช่องทางออนไลน์ เช่น Facebook, Line, Zoom หรือสื่อโซเชียลอื่นๆ ในการประสานงานและปฏิบัติงาน
- การปฏิบัติงานนอกสถานที่ (WFH): สำหรับภารกิจที่ทำผ่านระบบเครือข่ายได้ ให้บุคลากรปฏิบัติงาน ณ ที่พักอาศัย (Work From Home) โดยต้องปฏิบัติตามมาตรการการลงชื่อเข้า-ออกงานเสมือนเวลาราชการปกติ

ขั้นตอนที่ ๓. แนวทางปฏิบัติรายระยะสำหรับการกอบกู้งาน (Recovery Execution)

- ระยะตอบสนองทันที (ภายใน ๒๔ ชั่วโมง)
  - ระบุและสรุปรายชื่อบุคลากรที่ได้รับบาดเจ็บหรือเสียชีวิตเพื่อความปลอดภัย
  - มอบหมายบุคลากรหลักประมาณร้อยละ ๑๐ ของแต่ละหน่วยงานเพื่อเริ่มดำเนินกระบวนงานที่เร่งด่วน
  - หากระบบไอทียังไม่พร้อม ให้บุคลากรปฏิบัติงานด้วยมือ (Manual Processing) ไปพลางก่อน
- ระยะสั้น (ภายใน ๗ วัน)
  - ดำเนินการจัดหาบุคลากรหลักเพิ่มเติมเพื่อรองรับการทำงานต่อเนื่อง
  - ติดตามสถานะสุขภาพบุคลากร โดยเฉพาะในกรณีเกิดโรคระบาด หากมีความเสี่ยงให้แยกไปปฏิบัติงานที่บ้าน
- ระยะปานกลาง (ภายหลัง ๗ วัน)
  - สรุปความพร้อมด้านทรัพยากรและแจ้งให้บุคลากรเตรียมพร้อมกลับเข้าดำเนินงานและให้บริการตามปกติ

๒.๘ แผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan)

แผนฉบับนี้มีวัตถุประสงค์เพื่อให้กรมการจัดหางานมีขั้นตอนการปฏิบัติที่ชัดเจนในการเฝ้าระวัง ตรวจจับ ระงับเหตุ และฟื้นฟูระบบสารสนเทศจากภัยคุกคามทางไซเบอร์ เพื่อลดผลกระทบต่อภารกิจหลักและข้อมูลของประชาชน

๒.๘.๑ โครงสร้างทีมตอบสนองอุบัติการณ์ (Cyber CSIRT) เพื่อให้การตอบสนองเป็นไปอย่างรวดเร็ว กรม ฯ กำหนดบทบาทหน้าที่ดังนี้

- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.): ทำหน้าที่เป็นผู้บัญชาการเหตุการณ์ (Incident Commander)
- เจ้าหน้าที่วิเคราะห์ภัยคุกคามไซเบอร์ (Cyber Security Analyst): จำนวน ๒ คน ทำหน้าที่เฝ้าระวังและวิเคราะห์เหตุการณ์ผ่านระบบ SOC ตลอด ๒๔ ชั่วโมง
- ทีมสนับสนุนเทคนิค: เจ้าหน้าที่ดูแลระบบเครือข่าย เครื่องแม่ข่าย และระบบ GDCC

๒.๘.๒ กระบวนการตอบสนองภัยคุกคามไซเบอร์ (Incident Response Workflow) กระบวนการแบ่งออกเป็น ๖ ขั้นตอนหลักตามมาตรฐานสากล

๑. การเตรียมความพร้อม (Preparation)
- จัดเตรียมระบบเฝ้าระวัง SOC (Security Operation Center) และเครื่องมือตอบโต้ EDR/SOAR
- จัดทำ Playbook สำหรับภัยคุกคามรูปแบบต่างๆ (เช่น Ransomware, Web Shell) อย่างน้อย ๑๐ รูปแบบ

๒. การตรวจจับและวิเคราะห์ (Detection & Analysis)
- ระบบ SOC ตรวจสอบ Log และตัวบ่งชี้การบุกรุก (IoC) ตลอดเวลา
- การคัดแยกประเภท (Triage): ประเมินว่าเป็นเหตุการณ์จริงหรือไม่ และระบุระดับความรุนแรงตามมาตรา ๖๐ พรบ. ไซเบอร์ฯ (ไม่ร้ายแรง, ร้ายแรง, วิกฤต)

๓. การจำกัดขอบเขต (Containment)
- มาตรการระยะสั้น: ใช้ระบบ EDR ในการตัดการเชื่อมต่อเครือข่ายของเครื่องที่ถูกโจมตี (Isolate) ทันที
- การรักษาหลักฐาน: ปิดช่องทางการเข้าถึงที่ผิดปกติแต่รักษาข้อมูลในหน่วยความจำเพื่อการวิเคราะห์ทางนิติวิทยาศาสตร์ (Forensics)

๔. การขจัดภัยคุกคาม (Eradication)

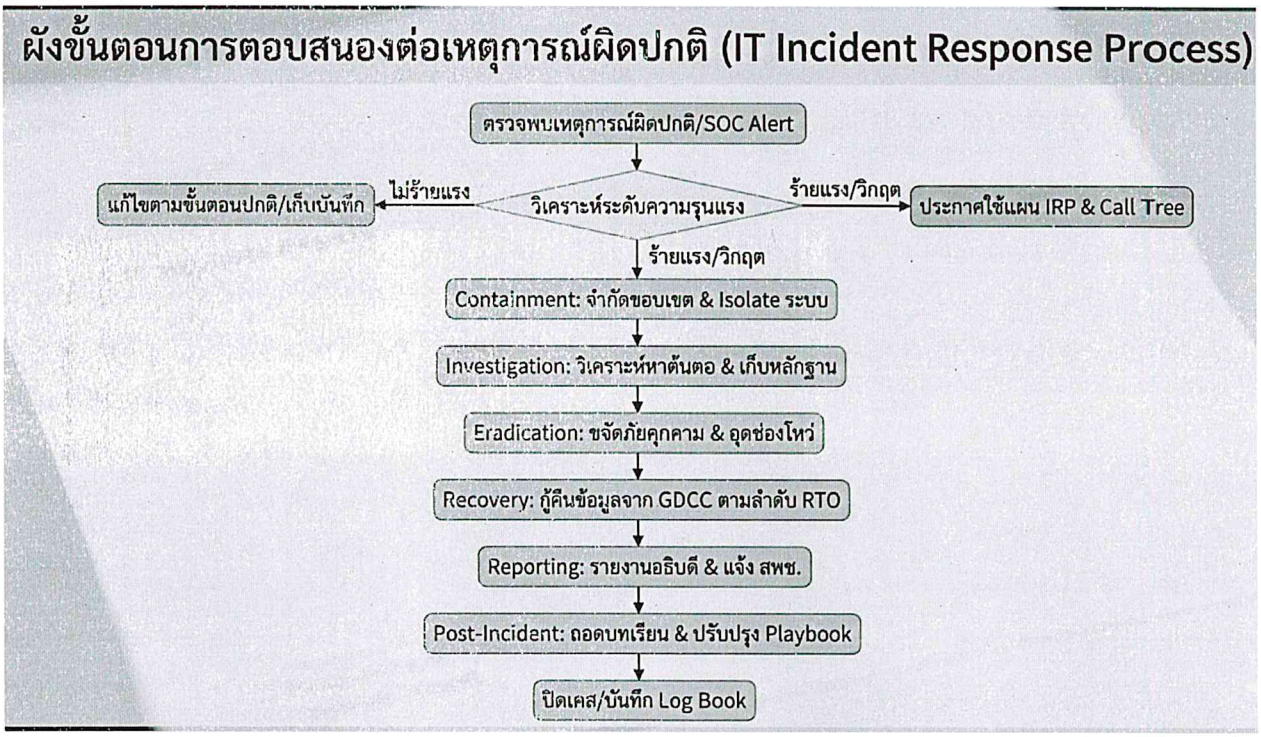
- ลบโปรแกรมไม่พึงประสงค์ (Malware) และอุดช่องโหว่ (Patching) ที่ถูกใช้ในการโจมตี
- ตรวจสอบบัญชีผู้ใช้งานและเปลี่ยนรหัสผ่านหากพบความเสี่ยง

๕. การกู้คืนระบบ (Recovery)

- นำข้อมูลสำรองจาก ระบบคลาวด์กลางภาครัฐ (GDCC) มาใช้กู้คืนระบบตามลำดับความสำคัญ (RTO ภายใน ๑ วัน สำหรับระบบให้บริการประชาชน)
- ทดสอบระบบก่อนเปิดให้บริการจริงเพื่อให้มั่นใจว่าปลอดภัย ๑๐๐%

๖. กิจกรรมหลังเกิดเหตุ (Post-Incident Activity)

- ประชุมถอดบทเรียน (Lesson Learned) เพื่อวิเคราะห์สาเหตุที่แท้จริง (Root Cause)
- จัดทำรายงานสรุปเสนออธิบดีและแจ้งหน่วยงานกำกับดูแล (สกมช.) ตามกฎหมาย



รูปที่ ๑ แสดงขั้นตอนการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response Process)

คำอธิบายกระบวนการ (Process Description)

- ตรวจพบเหตุการณ์ผิดปกติ (Detection): ระบบ SOC และ EDR ตรวจพบพฤติกรรมที่น่าสงสัย หรือตัวบ่งชี้การบุกรุก (IoC) เช่น การพยายามบุกรุกระบบ DOE e-License หรือพบมัลแวร์ในเครื่องลูกข่าย

- วิเคราะห์ระดับความรุนแรง (Severity Analysis): เจ้าหน้าที่วิเคราะห์ภัยคุกคามประเมินระดับความรุนแรงตามมาตรา ๖๐ ของ พรบ. ไซเบอร์ฯ
    - ระดับไม่ร้ายแรง: ระบบด้อยประสิทธิภาพลงแต่ยังทำงานได้ ให้ดำเนินการตามขั้นตอนปกติ
    - ระดับร้ายแรง/วิกฤต: ระบบสำคัญเสียหายหรือส่งผลกระทบต่อประชาชนวงกว้าง ให้ยกระดับการตอบสนอง
- ประกาศใช้แผน IRP & Call Tree: อธิบดีในฐานะหัวหน้าคณะบริหารความพร้อมฯ ประกาศใช้แผนรับมือและเริ่มการแจ้งเหตุตามลำดับสายบังคับบัญชา (Call Tree) เพื่อระดมเจ้าหน้าที่ ศทส. และผู้เกี่ยวข้อง
- การจำกัดขอบเขต (Containment): ใช้ระบบ EDR หรือ SOAR ดำเนินการ Isolate ตัดเครื่องที่ติดเชื้อออกจากเครือข่ายทันที เพื่อป้องกันไม่ให้มัลแวร์หรือการโจมตีกระจายตัวไปยังส่วนอื่น
- การสืบสวนและเก็บหลักฐาน (Investigation): วิเคราะห์หาสาเหตุพื้นฐาน (Root Cause) และรักษาสถานะข้อมูลคอมพิวเตอร์เพื่อใช้ในการพิสูจน์หลักฐานดิจิทัล (Forensics) ตามกฎหมาย
- การขจัดภัยคุกคาม (Eradication): ลบโปรแกรมไม่พึงประสงค์ (Malware) ปิดบัญชีผู้ใช้งานที่ถูกเจาะ และดำเนินการลงโปรแกรมแก้ไขช่องโหว่ (Patching) เพื่อกำจัดต้นตอของการโจมตี
- การกู้คืนระบบ (Recovery): ดำเนินการ Restore ฐานข้อมูลและระบบงานจาก ระบบคลาวด์กลางภาครัฐ (GDCC) โดยยึดตามลำดับความสำคัญ (RTO ภายใน ๑ วัน สำหรับระบบบริการประชาชน)
- การรายงานผล (Reporting): สรุปเหตุการณ์รายงานต่ออธิบดี และแจ้งไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายในระยะเวลาที่กฎหมายกำหนด
- กิจกรรมหลังเกิดเหตุ (Post-Incident): ประชุมทีมงานเพื่อถอดบทเรียน (Lesson Learned) จากเหตุการณ์ที่เกิดขึ้น และนำมาปรับปรุงขั้นตอนการปฏิบัติงาน (Playbook) ให้ทันสมัย
- การปิดเคส (Post-Action): บันทึกรายละเอียดการดำเนินการทั้งหมดลงใน Log Book เพื่อเป็นหลักฐานสำหรับการตรวจประเมินความมั่นคงปลอดภัยประจำปี

๒.๘.๓ การสื่อสารในภาวะวิกฤตไซเบอร์

- ภายใน: แจ้งเหตุตามผัง Call Tree เริ่มจากอธิบดีไปยังเลขานุการกรม และหัวหน้าทีมส่วนงานที่ได้รับผลกระทบ
- ภายนอก
    - รายงานเหตุภัยคุกคามที่มีนัยสำคัญต่อ สกมช. ทันที
    - ประสานผู้ให้บริการ GDCC/ISP เพื่อสนับสนุนด้านเทคนิค

- ประชาสัมพันธ์แจ้งประชาชนผ่านหน้าเว็บไซต์หน่วยงานในกรณีระบบขัดข้อง

การดำเนินการทั้งหมดต้องมีการบันทึกกิจกรรมลงใน Log Book อย่างสม่ำเสมอ เพื่อใช้เป็นหลักฐานประกอบการประเมินประสิทธิภาพตามมาตรา ๕๔ ของ พรบ. ไซเบอร์ฯ

บทที่ ๓

แผนกู้คืนระบบสารสนเทศจากภัยพิบัติ (Disaster Recovery Plan - DRP)

แผนกู้คืนระบบสารสนเทศจากภัยพิบัติ (DRP) ฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางสำหรับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ในการกู้คืนโครงสร้างพื้นฐานด้านไอที ระบบเครือข่าย และฐานข้อมูลสำคัญให้กลับมาใช้งานได้ตามปกติเมื่อเกิดเหตุการณ์ภัยพิบัติ

๓.๑ กลยุทธ์การกู้คืนโครงสร้างพื้นฐานสารสนเทศและระบบเครือข่าย

เพื่อให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) สามารถกู้คืนระบบโครงสร้างพื้นฐานและเครือข่ายของกรมการจัดหางานให้กลับมาทำงานได้อย่างต่อเนื่องตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ และฟังก์ชัน Recover (RC.RP) ของ NIST CSF ๒.๐ กรมฯ จึงกำหนดกลยุทธ์การดำเนินงานดังนี้

๓.๑.๑ กลยุทธ์การกู้คืนระบบเครือข่ายและการสื่อสาร (Network Recovery Strategy)

- การจัดเตรียมโครงข่ายสื่อสารสำรอง: กรมฯ กำหนดให้มีการประสานงานกับผู้ให้บริการโครงข่าย (ISP) เพื่อติดตั้งระบบให้สามารถปฏิบัติงานได้ ณ สถานที่ปฏิบัติงานสำรองที่กำหนดไว้ทันทีเมื่อเกิดเหตุวิกฤต.
- มาตรการเชื่อมต่อฉุกเฉิน: ในกรณีที่ระบบเครือข่ายสื่อสารข้อมูลหลักของกรมฯ ขัดข้องนานกว่า ๑ ชั่วโมง ให้เจ้าหน้าที่ใช้เครื่องมือเชื่อมโยงอินเทอร์เน็ตพกพา (Pocket Wi-Fi) หรือแชร์สัญญาณอินเทอร์เน็ต (Hotspot) จากโทรศัพท์เคลื่อนที่ส่วนตัว เพื่อรักษาการเข้าถึงระบบสารสนเทศและฐานข้อมูลที่สำคัญเป็นการชั่วคราว.
- การกู้คืนช่องทางติดต่อประชาชน: ประสานผู้ให้บริการระบบ Call Center ให้ปรับเปลี่ยนรูปแบบการรับสาย เพื่อให้เจ้าหน้าที่สามารถปฏิบัติงาน ณ ที่พักอาศัยหรือสถานที่อื่นได้ตามความเหมาะสม.

๓.๑.๒ กลยุทธ์ด้านโครงสร้างพื้นฐานและการประมวลผล (Infrastructure & Processing Strategy)

- การใช้งานระบบคลาวด์กลางภาครัฐ (GDCC): กรมฯ มุ่งเน้นการใช้ฐานข้อมูลและระบบงานสำคัญบน ระบบคลาวด์กลางภาครัฐ (GDCC) ซึ่งมีมาตรการรักษาความมั่นคงปลอดภัยและความยืดหยุ่นสูงตามมาตรฐานสากล.
- การสำรองข้อมูลและระบบงาน (Backup): ต้องจัดทำข้อมูลสำรอง (Backup) ของระบบงานหลักและฐานข้อมูลสำหรับให้บริการประชาชนไว้บน GDCC อย่างสม่ำเสมอ เพื่อรองรับการกู้คืนในกรณีที่ระบบ ณ อาคารกรมฯ เกิดความเสียหาย.

- ความพร้อมใช้ของอุปกรณ์ประมวลผล (Redundancy): ต้องมีการเตรียมการสำรองอุปกรณ์ประมวลผลข้อมูลและฮาร์ดแวร์ที่สำคัญให้เพียงพอ เพื่อให้ระบบมีความพร้อมใช้งาน (Availability) ตามระยะเวลาเป้าหมาย (RTO) ที่กำหนดไว้.
- ระบบไฟฟ้าสำรองฉุกเฉิน: ต้องติดตั้งและบำรุงรักษาเครื่องกำเนิดไฟฟ้าสำรองสำหรับห้อง Data Center เพื่อป้องกันความเสียหายต่อระบบคอมพิวเตอร์และฐานข้อมูลเมื่อเกิดไฟฟ้าขัดข้อง.

๓.๑.๓ การบริหารจัดการในช่วงรอยต่อการกู้คืน (Interim Recovery Measures)

- การปฏิบัติงานด้วยมือ (Manual Processing): ในระหว่างที่ระบบเครือข่ายยังไม่สามารถกู้คืนได้สมบูรณ์ ให้เจ้าหน้าที่ดำเนินการบันทึกข้อมูลสำคัญด้วยโปรแกรมจัดการสำนักงานทั่วไป เช่น Excel หรือ Word ไปพลางก่อน และให้นำข้อมูลดังกล่าวบันทึกเข้าระบบสารสนเทศหลักทันทีเมื่อระบบกลับมาใช้งานได้ตามปกติ.
- การสำรองข้อมูลระดับบุคคล: บุคลากรทุกคนมีหน้าที่สำรองข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของตนลงในอุปกรณ์พกพา เช่น Flash Drive หรือ External Hard Disk อย่างสม่ำเสมอ เพื่อให้สามารถทำงานได้อย่างต่อเนื่องในสภาวะวิกฤต.

๓.๑.๔ การตรวจสอบและความมั่นคงปลอดภัยหลังการกู้คืน (Post-Recovery Verification)

- การยืนยันสถานะระบบ: หลังการกู้คืนระบบเครือข่ายและฮาร์ดแวร์ ศทส. ต้องตรวจสอบความถูกต้องครบถ้วนของทรัพยากรที่ได้รับการกู้คืน และยืนยันว่าระบบสามารถให้บริการได้ตามเกณฑ์มาตรฐานก่อนประกาศสิ้นสุดกิจกรรมกู้คืน.
- การปฏิบัติตามแผนไอทีสำรอง (ICP): การดำเนินการกู้คืนทั้งหมดต้องเป็นไปตาม แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติด้านไอที (IT Contingency Plan : ICP) ของกรมฯ เพื่อความปลอดภัยและเป็นระบบ

๓.๒ การใช้งานระบบคลาวด์กลางภาครัฐ (GDCC) ในการสำรองข้อมูล

เพื่อให้การบริหารจัดการข้อมูลและระบบงานสำคัญของกรมการจัดหางานมีความยืดหยุ่นและมั่นคงปลอดภัยตามมาตรฐานสากล กรมฯ จึงกำหนดแนวปฏิบัติในการใช้งานระบบคลาวด์กลางภาครัฐ (Government Data Center and Cloud Service: GDCC) สำหรับการสำรองข้อมูลและการกู้คืนระบบดังนี้

๓.๒.๑ นโยบายการใช้บริการคลาวด์ (Cloud Service Policy)

- การเลือกใช้บริการ: กรมฯ กำหนดให้ใช้บริการ GDCC เป็นโครงสร้างพื้นฐานหลักสำหรับจัดเก็บฐานข้อมูลและระบบงานที่ให้บริการประชาชน เนื่องจากเป็นระบบที่มีมาตรการรักษาความมั่นคงปลอดภัย ความน่าเชื่อถือ และมีการบริหารความพร้อมต่อสภาวะวิกฤตที่เป็นมาตรฐานสากล

- การกำกับดูแลผู้ให้บริการ: การจัดหา การใช้งาน และการบริหารจัดการบริการคลาวด์ต้องสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของกรมฯ และต้องมีการกำหนดบทบาทความรับผิดชอบที่ชัดเจนระหว่างกรมฯ กับผู้ให้บริการ (สพธอ./DGA)

๓.๒.๒ มาตรการสำรองข้อมูลบนระบบคลาวด์ (Cloud Backup Measures)

- ขอบเขตการสำรองข้อมูล: ต้องจัดทำข้อมูลสำรอง (Backup) ของระบบงานและฐานข้อมูลสำคัญทั้งหมดสำหรับให้บริการประชาชนไว้ที่ระบบ GDCC อย่างสม่ำเสมอ
- ความถี่และรูปแบบ: การสำรองข้อมูลต้องพิจารณาจากความสำคัญและความถี่ในการเปลี่ยนแปลงของข้อมูล โดยมุ่งเน้นการรักษาข้อมูลให้มีความทันสมัยล่าสุด (Latest Update) เพื่อรองรับการกู้คืนระบบได้อย่างมีประสิทธิภาพ
- การทดสอบการกู้คืน: ข้อมูลสำรองบนคลาวด์ต้องได้รับการทดสอบการกู้คืน (Restore Test) อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถนำกลับมาใช้งานได้จริงเมื่อเกิดเหตุวิกฤต ตามหลักการของมาตรฐาน ISO/IEC ๒๗๐๐๑ และ NIST CSF

๓.๒.๓ การเชื่อมต่อและการเข้าถึงในภาวะวิกฤต (Crisis Connectivity)

- การประสานงาน: ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) มีหน้าที่ประสานงานกับผู้ดูแลระบบ GDCC เพื่อทดสอบและเชื่อมต่อการใช้งานระบบสารสนเทศและฐานข้อมูลจากสถานที่ปฏิบัติงานสำรองทันทีที่มีการประกาศใช้แผน BCP
- ความต่อเนื่องของระบบเครือข่าย: ในกรณีที่ระบบเครือข่ายหลักของกรมฯ ขัดข้อง ให้ใช้ช่องทางการเชื่อมต่อผ่านอินเทอร์เน็ตที่ปลอดภัยเพื่อเข้าถึงทรัพยากรบน GDCC ตามที่ได้กำหนดไว้ในกลยุทธ์ด้านเทคโนโลยีสารสนเทศ

๓.๒.๔ ความมั่นคงปลอดภัยของข้อมูลบนคลาวด์ (Cloud Data Security)

- การรักษาความลับและความถูกต้อง: ข้อมูลที่จัดเก็บและสำรองไว้บน GDCC ต้องได้รับการคุ้มครองตามหลักการ CIA (Confidentiality, Integrity, Availability) เพื่อป้องกันการเข้าถึง การแก้ไข หรือการสูญหายโดยมิชอบ
- การควบคุมสิทธิการเข้าถึง: การเข้าถึงระบบจัดการคลาวด์ (Cloud Management Console) ต้องจำกัดเฉพาะเจ้าหน้าที่ ศทส. ที่ได้รับมอบหมาย และต้องใช้การพิสูจน์ตัวตนที่มั่นคงปลอดภัย

๓.๓ ลำดับความสำคัญในการกู้คืนระบบสารสนเทศและฐานข้อมูลสำคัญ

เพื่อให้การฟื้นฟูระบบสารสนเทศของกรมการจัดหางานภายหลังเกิดภัยพิบัติเป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับความจำเป็นของภารกิจหลัก กรมฯ จึงกำหนดลำดับความสำคัญในการกู้คืนระบบสารสนเทศและฐานข้อมูล (System Recovery Priority) โดยแบ่งตามระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO) ดังนี้

๓.๓.๑ ระบบงานที่มีความสำคัญสูงสุด (Critical - RTO ภายใน ๑ วัน)

เป็นระบบสารสนเทศที่ให้บริการประชาชนและนายจ้างโดยตรง หรือเป็นโครงสร้างพื้นฐานที่จำเป็นต่อการปฏิบัติงานในภาวะวิกฤต ซึ่งต้องได้รับการกู้คืนให้พร้อมใช้งานภายใน ๒๔ ชั่วโมง ได้แก่

- ระบบโครงสร้างพื้นฐานและช่องทางการสื่อสาร
    - ระบบอินเทอร์เน็ต, ระบบ Air card และ Wi-Fi สำหรับการเชื่อมต่อฉุกเฉิน
    - Website ของหน่วยงาน เพื่อใช้สื่อสารข้อมูลข่าวสารต่อประชาชน
    - ระบบ Call Center เพื่อรองรับการสอบถามข้อมูล
- ระบบบริการประชาชนและธุรกิจแรงงาน
    - ระบบไทยมีงานทำ และ แพลตฟอร์มคนทำงาน (Khon Tham Ngan)
    - ระบบบริการออกใบอนุญาตจัดหางานอิเล็กทรอนิกส์ (DOE e-License)
    - ระบบอนุญาตทำงานของคนต่างด้าวทางอิเล็กทรอนิกส์ และ ระบบ Single Window For Visa and Work Permit
    - ระบบอิเล็กทรอนิกส์การบริหารแรงงานไทยไปต่างประเทศ
    - ระบบการให้สิทธิและขอรับสิทธิผู้พิการตามมาตรา ๓๕
- ระบบสนับสนุนการทำงานภายใน
    - ระบบสารบรรณอิเล็กทรอนิกส์ (e-Saraban) เพื่อการลงทะเบียนรับ-ส่งหนังสือ
    - ระบบ Smart Office และ ระบบประชุมทางไกล (VDO Conference) เพื่อประสานงานภาวะวิกฤต

๓.๓.๒ ระบบงานที่มีความเร่งด่วน (Urgent - RTO ภายใน ๓ วัน)

เป็นระบบงานสนับสนุนภารกิจภายในที่ต้องรีบดำเนินการกู้คืนเพื่อให้การบริหารงานราชการไม่หยุดชะงักนานเกินควร ได้แก่

- ระบบบริหารทรัพยากรบุคคล (HR System) เพื่อการจัดระบบงานและพัฒนาบุคลากร
- ฐานข้อมูลงานการเงินและบัญชี สำหรับการรับ-นำส่งเงิน และการคุมยอดขออนุมัติเบิกจ่ายงบประมาณ

๓.๓.๓ ระบบงานสำคัญ (Important - RTO ภายใน ๗ วัน)

เป็นระบบงานที่มีความสำคัญรองลงมา ซึ่งสามารถหยุดชะงักได้ชั่วคราวแต่ต้องกู้คืนภายใน ๑ สัปดาห์ ได้แก่:

- ระบบเครือข่ายสื่อสารข้อมูล ที่เชื่อมโยงระหว่างหน่วยงานภายในและภายนอก (ในส่วนงานปกติที่ไม่เร่งด่วน)
- ระบบฐานข้อมูลวิชาการและสถิติ: เช่น ระบบข้อมูลข่าวสารตลาดแรงงาน และฐานข้อมูลงานวิจัย/วิเคราะห์นโยบาย

๓.๓.๔ ระบบงานสนับสนุนอื่นๆ (Normal - RTO ๑๕ วันขึ้นไป)

- ระบบงานสารสนเทศเพื่อการตรวจสอบภายในและการประเมินส่วนราชการ
- ระบบฐานข้อมูลห้องสมุดกรมการจัดหางาน

๓.๔ ขั้นตอนการปฏิบัติการกู้คืนระบบ (Recovery Plan Execution)

เพื่อให้การกู้คืนระบบสารสนเทศและฐานข้อมูลสำคัญของกรมการจัดหางาน ภายหลังการเกิดภัยพิบัติหรือภัยคุกคามไซเบอร์เป็นไปอย่างมีประสิทธิภาพ และสามารถกลับมาให้บริการประชาชนได้ตามระยะเวลาเป้าหมาย (RTO) ที่กำหนด กรมฯ จึงกำหนดขั้นตอนการปฏิบัติไว้ดังนี้

๓.๔.๑ การประกาศใช้แผนกู้คืนระบบ (Execution based on Incident Response)

- ศทส. ต้องดำเนินการกู้คืนระบบทันทีเมื่อกระบวนการตอบสนองต่อเหตุการณ์ (Incident Response) ระบุว่าระบบสารสนเทศได้รับความเสียหายจนไม่สามารถให้บริการได้ตามปกติ หรือเมื่อมีการประกาศใช้แผน BCP โดยหัวหน้าคณะบริหารความพร้อมต่อสภาวะวิกฤต

๓.๔.๒ การกำหนดขอบเขตและลำดับความสำคัญ (Scoping and Prioritization)

- ศทส. ต้องระบุทรัพยากรที่ได้รับผลกระทบ และจัดลำดับความสำคัญในการกู้คืนตามภารกิจสำคัญของกรมฯ
  - ลำดับที่ ๑ (ภายใน ๑ วัน): ระบบให้บริการประชาชน เช่น ระบบไทยมีงานทำ, ระบบ DOE e-License และเว็บไซต์หน่วยงาน
  - ลำดับที่ ๒ (ภายใน ๓ วัน): ระบบเครือข่ายสื่อสาร, ระบบงานการเงินและบัญชี
  - ลำดับที่ ๓ (ภายใน ๗ วัน): ระบบบริหารทรัพยากรบุคคล และฐานข้อมูลวิชาการ

๓.๔.๓ การตรวจสอบความถูกต้องของข้อมูลสำรอง (Backup Data Verification)

- ก่อนเริ่มการกู้คืน ต้องดำเนินการประเมินและตรวจสอบความถูกต้องครบถ้วน (Integrity and Completeness) ของข้อมูลสำรองที่จัดเก็บไว้บน ระบบคลาวด์กลางภาครัฐ (GDCC) หรือสื่อบันทึกข้อมูลนอกสถานที่ เพื่อให้มั่นใจว่าข้อมูลที่จะนำมาใช้กู้คืนไม่ได้รับความเสียหายหรือถูกแก้ไขโดยมิชอบ

๓.๔.๔ การดำเนินการกู้คืนและมาตรการระยะชั่วคราว (Recovery Operations)

- ดำเนินการกู้คืนระบบตามขั้นตอนทางเทคนิค (Manual/Scripted Restore) โดยมุ่งเน้นการรักษาความปลอดภัยของระบบในระดับขั้นต่ำที่ยอมรับได้ (Minimum Operational Standard)
- ในระหว่างที่ระบบยังกู้คืนไม่แล้วเสร็จ ให้หน่วยงานพิจารณา ปฏิบัติงานด้วยมือ (Manual Processing) หรือใช้โปรแกรมจัดการสำนักงานทั่วไป (Excel, Word) ไปพลางก่อนตามความเหมาะสมของสถานการณ์

๓.๔.๕ การตรวจสอบและยืนยันสถานะหลังการกู้คืน (Verification and Validation)

- เมื่อกู้คืนระบบสำเร็จ ศทส. ต้องตรวจสอบความถูกต้องของทรัพยากรและทดสอบการทำงานของระบบ (System Testing) เพื่อยืนยันว่าบริการต่างๆ กลับมาทำงานได้ตามเกณฑ์มาตรฐานความปลอดภัยก่อนเปิดให้บริการแก่ประชาชน

๓.๔.๖ การปิดกิจกรรมการกู้คืนและจัดทำเอกสาร (Conclusion and Documentation)

- ประกาศสิ้นสุดกิจกรรมการกู้คืนเมื่อระบบกลับสู่สภาวะปกติ
- ศทส. และทีมงานบริหารความพร้อมต่อสภาวะวิกฤตของสำนัก/กอง ต้องจัดทำ บันทึกกิจกรรม (Log Book) และสรุปผลการกู้คืน รวมถึงระบุปัญหาและอุปสรรคที่พบเพื่อใช้เป็นแนวทางในการปรับปรุงแผนในอนาคต

แนวทางการกอบกู้กระบวนการปฏิบัติงานของกรมการจัดหางานแบ่งออกเป็น ๓ ระยะ ตามกรอบเวลาเพื่อให้การตอบสนองต่อสภาวะวิกฤตเป็นไปอย่างมีระบบ ดังนี้

ระยะที่ ๑ ตอบสนองต่อสถานการณ์ทันที (ภายใน ๒๔ ชั่วโมง) ระยะนี้มุ่งเน้นการรักษาความปลอดภัยของบุคลากรและการประเมินความเสียหายเบื้องต้น

- การแจ้งเหตุและสื่อสาร: แจ้งเหตุฉุกเฉินตามกระบวนการ Call Tree และสื่อสารสถานการณ์ให้บุคลากรทราบตามเนื้อหาที่คณะบริหารความพร้อมฯ เห็นชอบ
- การประเมินผลกระทบ: ประชุมทีมงานเพื่อประเมินความเสียหายต่อการดำเนินงาน ทรัพยากร และระบุรายชื่อผู้ได้รับบาดเจ็บหรือเสียชีวิต
- การบริหารกระบวนงานเร่งด่วน: ทบทวนงานที่ต้องทำให้เสร็จภายใน ๑-๕ วัน และขออนุมัติปฏิบัติงานด้วยมือ (Manual Processing) หากระบบไอทียังไม่พร้อม
- การจัดหาทรัพยากร: ประสานงานจัดหาทรัพยากรที่จำเป็น เช่น สถานที่ปฏิบัติงานสำรอง วัสดุอุปกรณ์ และคู่ค้า/ผู้ให้บริการ
- การบันทึกและรายงาน: บันทึกกิจกรรมใน Log Book และรายงานความคืบหน้าต่อหัวหน้าคณะบริหารความพร้อมฯ (อธิบดี)

ระยะที่ ๒ ตอบสนองต่อสถานการณ์ในระยะสั้น (ภายใน ๗ วัน) ระยะนี้เน้นการจัดหาทรัพยากรทดแทนและเริ่มกอบกู้ข้อมูล

- การติดตามสถานะ: ติดตามการกอบกู้ทรัพยากรที่ได้รับผลกระทบ และประเมินระยะเวลาที่ต้องใช้ในการกู้คืน
- การจัดซื้อจัดสรร: ตรวจสอบข้อจำกัดและดำเนินการจัดหาวัสดุอุปกรณ์ ระบบเทคโนโลยี และบุคลากรหลัก เพื่อรองรับการทำงานต่อเนื่อง
- การกู้คืนข้อมูล: ดำเนินการกอบกู้ข้อมูลและจัดทำรายงานต่าง ๆ ที่จำเป็นต่อการให้บริการประชาชน

- การประสานภายนอก: ประชาสัมพันธ์แจ้งสถานการณ์และแนวทางปฏิบัติให้คู่ค้าและผู้ให้บริการทราบ
- บันทึกและรายงาน: บันทึกกิจกรรมลงใน Log Book และรายงานความคืบหน้าตามเวลาที่กำหนด

ระยะที่ ๓ ตอบสนองต่อสถานการณ์ในระยะปานกลาง (ภายหลัง ๗ วัน) ระยะนี้มุ่งเน้นการกลับเข้าสู่สภาวะปกติ

- การประเมินขั้นสุดท้าย: ติดตามและรายงานสถานภาพการกอบกู้คืนมาของทรัพยากรทั้งหมดว่าพร้อมใช้งานเพียงใด
- การเตรียมกลับสู่ภาวะปกติ: แจ้งสรุปสถานการณ์และความพร้อมด้านทรัพยากรต่าง ๆ เพื่อให้บุคลากรเตรียมดำเนินงานและให้บริการตามปกติ
- การสรุปผล: บันทึกกิจกรรมและรายงานความคืบหน้าขั้นสุดท้ายต่อหัวหน้าคณะบริหารความพร้อมฯ เพื่อปิดสถานการณ์วิกฤต

ในทุกขั้นตอน บุคลากรต้องคำนึงถึงความปลอดภัยในชีวิตเป็นอันดับแรกและปฏิบัติตามแผนเผชิญเหตุอย่างเคร่งครัด

๓.๕ การทดสอบและการซักซ้อมแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan Testing)

เพื่อให้มั่นใจว่าแผนกู้คืนระบบสารสนเทศ (DRP) และมาตรการความพร้อมด้าน ICT ของกรมการจัดหางาน สามารถนำไปปฏิบัติได้จริงและมีประสิทธิภาพเมื่อเกิดเหตุวิกฤต กรมฯ จึงกำหนดแนวทางปฏิบัติในการทดสอบและซักซ้อมดังนี้

๓.๕.๑ วัตถุประสงค์ของการซักซ้อม

- เพื่อประเมินความพร้อมของบุคลากร เทคโนโลยี และกระบวนการในการกู้คืนระบบสารสนเทศสำคัญ
- เพื่อให้บุคลากรที่มีบทบาทหน้าที่รับผิดชอบตามแผน BCP/DRP ทราบขั้นตอนการปฏิบัติงานและเกิดความชำนาญเมื่อต้องเผชิญสถานการณ์จริง
- เพื่อระบุจุดบกพร่องหรือช่องว่างของแผนและดำเนินการปรับปรุงให้มีความทันสมัยอยู่เสมอ

๓.๕.๒ ความถี่และขอบเขตการทดสอบ

- รอบระยะเวลา: กรมฯ กำหนดให้มีการทบทวนและซักซ้อมแผนบริหารความพร้อมต่อสภาวะวิกฤตและการกู้คืนระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบงานที่สำคัญอย่างมีนัยสำคัญ

- ขอบเขต: ครอบคลุมการทดสอบกู้คืนระบบสารสนเทศสำหรับให้บริการประชาชน (เช่น ระบบไทยมีงานทำ, ระบบ DOE e-License) และฐานข้อมูลสำคัญที่สำรองไว้บน ระบบคลาวด์กลางภาครัฐ (GDCC)

๓.๕.๓ รูปแบบการซักซ้อม (Testing Methods) กรมฯ เลือกใช้รูปแบบการทดสอบตามความเหมาะสมของทรัพยากรและระดับความเสี่ยง ดังนี้

- การซักซ้อมเชิงอภิปราย (Tabletop Exercise): การจำลองสถานการณ์และให้ทีมงานร่วมวิเคราะห์ขั้นตอนการตอบสนองตามแผน
- การซักซ้อมเสมือนจริง (Simulation Exercise): การทดสอบกู้คืนระบบในสภาพแวดล้อมจำลองเพื่อตรวจสอบความถูกต้องของข้อมูลสำรองและเวลาที่ใช้ (RTO)
- การทดสอบสถานะความพร้อมภายนอก: เข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามไซเบอร์ที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จัดขึ้นตามที่กฎหมายกำหนด

๓.๕.๔ การประเมินผลและการปรับปรุง (Evaluation and Improvement)

- การบันทึกผล: หลังเสร็จสิ้นการซักซ้อม ทีมงานต้องบันทึกกิจกรรมและผลการทดสอบลงใน Log Book เพื่อเปรียบเทียบผลลัพธ์กับเป้าหมายที่กำหนดไว้
- การวิเคราะห์จุดบกพร่อง: นำปัญหาและอุปสรรคที่พบจากการซักซ้อมมาวิเคราะห์เพื่อหาแนวทางแก้ไข
- การปรับปรุงแผน: ปรับปรุงแผน DRP และขั้นตอนการปฏิบัติงานให้สอดคล้องกับผลการทดสอบและสภาพแวดล้อมทางเทคโนโลยีที่เปลี่ยนแปลงไป เพื่อสร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย

๓.๕.๕ หน้าที่ความรับผิดชอบ

- ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.): รับผิดชอบในการวางแผนและดำเนินการทดสอบความพร้อมด้าน ICT และระบบสำรอง
- คณะบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team): รับผิดชอบในการกำกับการซักซ้อมภาพรวมของกรมฯ และให้ความเห็นชอบต่อรายงานผลการซักซ้อม

บทที่ ๔

การปฏิบัติตามกฎหมายและบทลงโทษ (Compliance & Enforcement)

เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการบริหารความต่อเนื่องทางธุรกิจของกรมการจัดหางานเป็นไปอย่างถูกต้องตามกฎหมาย ระเบียบ และมาตรฐานระดับสากล กรมฯ จึงให้ความสำคัญสูงสุดกับการปฏิบัติตามข้อกำหนด (Compliance) ทั้งจากปัจจัยภายในและภายนอกองค์กร การกำหนดนโยบายในส่วนนี้มีวัตถุประสงค์เพื่อสร้างบรรทัดฐานในการปฏิบัติงานที่มั่นคงปลอดภัย และเป็นหลักประกันว่าภารกิจสำคัญของกรมฯ จะได้รับการคุ้มครองภายใต้กรอบของกฎหมายอย่างเคร่งครัด

การปฏิบัติตามนโยบายและแนวปฏิบัติฉบับนี้ ถือเป็นหน้าที่และความรับผิดชอบของบุคลากรทุกคน รวมถึงบุคคลภายนอกที่เข้ามาปฏิบัติงานร่วมกับกรมฯ เพื่อป้องกันผลกระทบที่อาจเกิดต่อความมั่นคงปลอดภัยของข้อมูลประชาชนและชื่อเสียงของทางราชการ โดยมีหลักการสำคัญดังนี้

- การสอดคล้องกับกฎหมาย (Legal Compliance): การดำเนินกิจกรรมไซเบอร์ทั้งหมดต้องเป็นไปตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้อง เช่น พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เพื่อลดความเสี่ยงทางกฎหมายและรักษาความสงบเรียบร้อยของประเทศ
- การยึดถือมาตรฐานสากล: กรมฯ นำแนวทางจากมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ และกรอบ NIST CSF ๒.๐ มาใช้ในการกำกับดูแล เพื่อให้เกิดความโปร่งใสและสามารถตรวจสอบประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ได้อย่างต่อเนื่อง
- ความรับผิดชอบและการบังคับใช้ (Enforcement): กรมฯ กำหนดให้มีมาตรการบังคับใช้และกระบวนการทางวินัยสำหรับผู้ที่ฝ่าฝืน หรือละเลยไม่ปฏิบัติตามนโยบายที่กำหนดไว้ เพื่อรักษามาตรฐานความปลอดภัยและสร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้ส่วนเสียทุกภาคส่วน

๔.๑ การรายงานเหตุการณ์ตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

เพื่อให้การตอบสนองต่อภัยคุกคามไซเบอร์ของกรมการจัดหางานเป็นไปอย่างถูกต้องตามกฎหมาย และสามารถประสานงานกับหน่วยงานภายนอกได้อย่างทันท่วงที กรมฯ จึงกำหนดแนวทางการรายงานเหตุการณ์ดังนี้

๔.๑.๑ หน้าที่ในการรายงานตามกฎหมาย (Legal Mandatory Reporting)

- การรายงานต่อหน่วยงานกำกับดูแล: เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของกรมฯ (เช่น ระบบไทยมีงานทำ หรือ ระบบ DOE e-License) กรมฯ มีหน้าที่ต้องรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และหน่วยงานควบคุมหรือกำกับดูแลที่เกี่ยวข้องโดยเร็ว

- การประเมินเหตุการณ์: ก่อนการรายงาน ให้หน่วยงานที่รับผิดชอบดำเนินการตรวจสอบข้อมูลคอมพิวเตอร์และพฤติการณ์แวดล้อมเพื่อประเมินว่ามีภัยคุกคามเกิดขึ้นจริงหรือไม่ หากพบว่าเกิดหรือคาดว่าจะเกิดภัยคุกคาม ให้ดำเนินการป้องกันและแจ้งไปยัง สกมช. ทันที

๔.๑.๒ ระดับของภัยคุกคามที่ต้องรายงาน (Cyber Threat Levels) กรมฯ จะอ้างอิงระดับภัยคุกคามตามมาตรา ๖๐ ของ พรบ. ไซเบอร์ฯ เพื่อประกอบการรายงาน ดังนี้

- ระดับไม่ร้ายแรง: ภัยคุกคามที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานหรือการให้บริการของรัฐด้อยประสิทธิภาพลง
- ระดับร้ายแรง: การโจมตีที่มุ่งหมายต่อโครงสร้างพื้นฐานสำคัญ และส่งผลให้ระบบหรือบริการสำคัญเสียหายจนไม่สามารถทำงานหรือให้บริการได้
- ระดับวิกฤต: ภัยคุกคามที่ส่งผลกระทบรุนแรงเป็นวงกว้าง จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ได้ หรืออาจทำให้บุคคลจำนวนมากเสียชีวิต

๔.๑.๓ ขั้นตอนการรายงานภายในและภายนอก (Reporting Workflow)

- การแจ้งเหตุภายใน: บุคลากรที่พบเหตุการณ์ผิดปกติหรือสงสัยว่าเกิดภัยคุกคาม มีหน้าที่รายงานต่อผู้ดูแลระบบหรือผู้บังคับบัญชาตามช่องทางที่กำหนดโดยทันที
- การสื่อสารตามผังการแจ้งเหตุ (Call Tree): เมื่อยืนยันเหตุการณ์แล้ว ให้ดำเนินการแจ้งเหตุตามลำดับขั้น โดยเริ่มจากหัวหน้าคณะบริหารความพร้อมฯ (อธิบดี) แจ้งไปยังผู้ประสานงาน (เลขานุการกรม) และหัวหน้าทีมบริหารความพร้อมฯ ของแต่ละสำนัก/กอง ตามลำดับ
- ข้อมูลที่ต้องรายงาน: รายงานเหตุการณ์ต้องครอบคลุมสรุปสถานการณ์ฉุกเฉิน ความเสียหายที่เกิดขึ้น ผลกระทบต่อการบริการประชาชน และทรัพยากรที่จำเป็นต้องใช้ในการแก้ไข
- การประสานงานภายนอก: กรมฯ ต้องสื่อสารสถานการณ์และแนวทางปฏิบัติให้คู่ค้า ผู้ให้บริการ (เช่น ผู้ดูแลระบบ GDCC) และผู้รับบริการทราบตามความเหมาะสม

๔.๑.๔ บทลงโทษกรณีละเลยการรายงาน (Penalties) ตามมาตรา ๗๓ แห่ง พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หากกรมฯ ในฐานะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่รายงานเหตุภัยคุกคามทางไซเบอร์โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท

๔.๒ บทลงโทษและการบังคับใช้ตามวินัยและกฎหมาย (Penalties & Enforcement)

เพื่อให้มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์และการบริหารความต่อเนื่องทางธุรกิจมีสภาพบังคับใช้อย่างจริงจัง กรมการจัดหางานจึงกำหนดบทลงโทษสำหรับผู้ที่ฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติดังนี้

๔.๒.๑ ความรับผิดชอบส่วนบุคคล (Individual Responsibility)

- การใช้งานบัญชีผู้ใช้: การกระทำใด ๆ ที่เกิดขึ้นจากการใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคลากรรายใด ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลของบุคลากรรายนั้น ซึ่งต้องรับผิดชอบต่อความผิดที่เกิดขึ้นทั้งทางวินัยและทางกฎหมาย
- หน้าที่การปฏิบัติตามนโยบาย: บุคลากรทุกคนและบุคคลภายนอกที่ได้รับอนุญาตเข้าใช้งานระบบมีหน้าที่ต้องยึดมั่นและปฏิบัติตามนโยบายเฉพาะแยกตามเรื่อง และขั้นตอนปฏิบัติที่กรมฯ กำหนดไว้อย่างเคร่งครัด

๔.๒.๒ บทลงโทษทางวินัย (Disciplinary Actions)

- กระบวนการทางวินัย: กรมฯ กำหนดให้มีกระบวนการทางวินัยอย่างเป็นทางการเพื่อดำเนินการต่อบุคลากรที่ละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ ตามความร้ายแรงของพฤติกรรม
- กรณีละเลยหรือฝ่าฝืน: หากเกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศอันเนื่องมาจากความบกพร่อง ละเลย หรือจงใจฝ่าฝืนนโยบาย ผู้กระทำผิดจะถูกดำเนินการทางวินัยตามระเบียบข้าราชการพลเรือนหรือสัญญาจ้างที่เกี่ยวข้อง

๔.๒.๓ บทกำหนดโทษตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ในกรณีที่การฝ่าฝืนส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของประเทศ กรมฯ และผู้ที่เกี่ยวข้องต้องระวางโทษตามกฎหมาย ดังนี้

- การไม่รายงานเหตุภัยคุกคาม: หากหน่วยงานละเลยไม่รายงานเหตุภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญต่อ สกมช. โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท
- การเปิดเผยข้อมูลโดยมิชอบ: เจ้าหน้าที่ผู้ใดเปิดเผยข้อมูลคอมพิวเตอร์ ข้อมูลจราจร หรือข้อมูลผู้ใช้บริการที่ได้มาตามอำนาจหน้าที่ให้แก่บุคคลอื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ
- ความประมาทเลินเล่อของเจ้าหน้าที่: หากเจ้าหน้าที่กระทำการโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลความมั่นคงปลอดภัยที่ได้มาตาม พรบ. นี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ
- การฝ่าฝืนคำสั่งศาลหรือคณะกรรมการ: ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการกากับดูแล (กกม.) หรือคำสั่งศาลในการรับมือภัยคุกคามระดับร้ายแรง (เช่น การเข้าตรวจสอบสถานที่ หรือการยึดอุปกรณ์) ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

๔.๒.๔ ความรับผิดชอบของผู้บริหารและนิติบุคคล

- ความรับผิดชอบระดับสูง: ผู้บริหารระดับสูงสุด (CEO/อธิบดี) เป็นผู้รับผิดชอบต่อความเสี่ยงและความเสียหายที่เกิดขึ้นในภาพรวมหากระบบล้มเหลวเนื่องจากการขาดมาตรการควบคุมที่เหมาะสม

- ความผิดของนิติบุคคล: ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล (เช่น คู่ค้าหรือผู้รับจ้าง) หากการกระทำนั้นเกิดจากการสั่งการหรือละเว้นการสั่งการของผู้จัดการหรือบุคคลผู้รับผิดชอบ ผู้นั้นต้องรับโทษตามที่กฎหมายบัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

๔.๓ การทบทวนและตรวจสอบการปฏิบัติตามนโยบาย (Policy Compliance Review & Audit)

เพื่อให้มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์และแผนบริหารความต่อเนื่องของกรมการจัดหางานมีผลบังคับใช้อย่างยั่งยืนและมีประสิทธิภาพ กรมฯ จึงกำหนดแนวทางในการตรวจสอบและทบทวนการปฏิบัติตามนโยบาย (Compliance) ตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ (ข้อ ๙.๒ และ Annex A ๕.๓๕ - ๕.๓๖) และ พรบ. ไซเบอร์ฯ พ.ศ. ๒๕๖๒ ดังนี้

๔.๓.๑ การตรวจสอบการปฏิบัติตามข้อกำหนด (Internal Monitoring)

- การตรวจสอบภายใน: หัวหน้าหน่วยงานและผู้ดูแลระบบมีหน้าที่ทบทวนการปฏิบัติงานภายในส่วนงานของตนให้เป็นไปตามนโยบาย มาตรฐาน และขั้นตอนปฏิบัติที่กำหนดไว้เป็นลายลักษณ์อักษรอย่างสม่ำเสมอ
- การทบทวนสิทธิการเข้าถึง: ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ต้องดำเนินการทบทวนบัญชีชื่อผู้ใช้งานและสิทธิการเข้าถึงระบบสารสนเทศสำคัญ (เช่น ระบบไทยมีงานทำ หรือระบบ DOE e-License) อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- การเฝ้าระวังผ่านข้อมูลล็อก: ต้องมีการตรวจสอบบันทึกเหตุการณ์ (Log File) อย่างต่อเนื่อง เพื่อตรวจหาพฤติกรรมที่อาจเป็นการฝ่าฝืนนโยบายความมั่นคงปลอดภัยหรือตัวบ่งชี้การบุกรุก

๔.๓.๒ การตรวจประเมินความมั่นคงปลอดภัยประจำปี (Security Audit)

- รอบระยะเวลาการตรวจสอบ: กรมฯ ในฐานะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ต้องจัดให้มีการประเมินความเสี่ยงและตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละ ๑ ครั้ง ตามมาตรา ๕๔ แห่ง พรบ. ไซเบอร์ฯ
- ขอบเขตการตรวจสอบ: ครอบคลุมถึงความมั่นคงปลอดภัยทางกายภาพ, ระบบเครือข่าย, การสำรองข้อมูลบน GDCC, และความพร้อมของบุคลากรตามแผน BCP/DRP
- การรายงานผลต่อหน่วยงานกำกับดูแล: กรมฯ ต้องจัดส่งผลสรุปรายงานการดำเนินการตรวจสอบต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จ

๔.๓.๓ การทบทวนโดยผู้บริหาร (Management Review)

- การประเมินประสิทธิผล: ผู้บริหารระดับสูง (อธิบดี และ CIO) ต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ตามรอบที่กำหนด เพื่อให้มั่นใจว่านโยบายยังคงมีความเหมาะสม เพียงพอ และสอดคล้องกับทิศทางเชิงกลยุทธ์ของกรมฯ
- การพิจารณาผลตอบกลับ: การทบทวนต้องนำข้อมูลจากการตรวจประเมิน, สถานะของการแก้ไขข้อบกพร่อง, และสถานะของแผนจัดการความเสี่ยงมาพิจารณาประกอบการตัดสินใจปรับปรุงระบบ

๔.๓.๔ การทบทวนอย่างเป็นอิสระ (Independent Review)

- ความโปร่งใส: มาตรการบริหารจัดการความมั่นคงปลอดภัยต้องได้รับการทบทวนอย่างเป็นอิสระโดยหน่วยงานที่ไม่ได้มีส่วนเกี่ยวข้องกับการปฏิบัติตามกระบวนการนั้น ๆ เพื่อให้เกิดความโปร่งใสและระบุจุดบกพร่องที่อาจถูกมองข้าม

๔.๓.๕ การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)

- การจัดการความไม่สอดคล้อง: หากพบการปฏิบัติที่ไม่สอดคล้องกับนโยบาย (Non-conformity) กรมฯ ต้องดำเนินการแก้ไข (Corrective Action) เพื่อขจัดสาเหตุและป้องกันการเกิดซ้ำ โดยมีการบันทึกหลักฐานไว้เป็นลายลักษณ์อักษร
- การพัฒนาแผนงาน: ต้องนำผลจากการตรวจสอบและการซักซ้อมแผน BCP/DRP มาใช้ในการปรับปรุงนโยบายและขั้นตอนการปฏิบัติงานให้มีความทันสมัยและพร้อมรับมือกับภัยคุกคามรูปแบบใหม่ ๆ เสมอ

๔.๔ แผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

เพื่อให้ระบบสารสนเทศของกรมการจัดหางานมีความมั่นคงปลอดภัยและสอดคล้องกับมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ และ NIST CSF ๒.๐ (ฟังก์ชัน Govern) กรมฯ จึงกำหนดแผนการตรวจสอบไว้ดังนี้

๔.๔.๑ วัตถุประสงค์ของการตรวจสอบ (Audit Objectives)

- เพื่อประเมินว่ามาตรการควบคุม (Controls) ที่ประกาศใช้มีความสอดคล้องกับนโยบายของกรมฯ และข้อกำหนดของมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒
- เพื่อตรวจสอบการปฏิบัติตามกฎหมายที่เกี่ยวข้อง โดยเฉพาะ พรบ. ไซเบอร์ฯ และ พรบ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)
- เพื่อระบุช่องว่าง (GAP Analysis) และจุดอ่อนของระบบสารสนเทศก่อนที่จะเกิดเหตุภัยคุกคามจริง

๔.๔.๒ รอบระยะเวลาและความถี่ (Audit Frequency)

- การตรวจสอบประจำปี: กรมฯ ในฐานะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ต้องจัดให้มีการตรวจสอบ อย่างน้อยปีละ ๑ ครั้ง
- การตรวจสอบกรณีพิเศษ: ดำเนินการเมื่อมีการเปลี่ยนแปลงระบบงานที่สำคัญอย่างมีนัยสำคัญ หรือเมื่อเกิดเหตุการณ์ภัยคุกคามไซเบอร์ระดับร้ายแรง

๔.๔.๓ ขอบเขตการตรวจสอบ (Audit Scope) ครอบคลุมสินทรัพย์สารสนเทศและกระบวนการที่สำคัญของกรมฯ ได้แก่

- ระบบให้บริการประชาชน: เช่น ระบบไทยมีงานทำ, ระบบ DOE e-License และระบบบริหารแรงงานไทยไปต่างประเทศ
- การควบคุมการเข้าถึง (Access Control): ตรวจสอบการลงทะเบียนผู้ใช้งาน การทบทวนสิทธิ์การเข้าถึง และการบริหารจัดการรหัสผ่าน
- ความมั่นคงปลอดภัยทางกายภาพ: ตรวจสอบศูนย์ข้อมูล (Data Center) ระบบไฟฟ้าสำรอง และระบบระงับเพลิง
- การสำรองและกู้คืนข้อมูล: ตรวจสอบความพร้อมของข้อมูลสำรองบน ระบบคลาวด์กลางภาครัฐ (GDCC) และผลการซักซ้อมแผน DRP
- การบริหารจัดการช่องโหว่: ตรวจสอบผลการใช้เครื่องมือ Vulnerability Assessment (VA) บนระบบเครือข่ายและแอปพลิเคชัน

๔.๔.๔ แนวทางการดำเนินการตรวจสอบ (Audit Methodology)

- ความเป็นอิสระ: ผู้ตรวจสอบ (Auditor) ต้องมีความเป็นกลาง ไม่ตรวจสอบงานที่ตนเองรับผิดชอบ
- การเข้าถึงข้อมูล: ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นได้ในลักษณะ อ่านอย่างเดียว (Read-only) หรือใช้ข้อมูลสำรองในการทดสอบเพื่อไม่ให้กระทบต่อระบบให้บริการจริง
- วิธีการตรวจสอบ: ครอบคลุมการสัมภาษณ์บุคลากร การตรวจสอบเอกสารหลักฐาน และการสังเกตการณ์การปฏิบัติงานจริง
- การใช้เครื่องมือทางเทคนิค: ตรวจสอบผ่านระบบ SOC, SOAR และ EDR เพื่อดูบันทึกเหตุการณ์ (Log) และประสิทธิภาพการตอบสนองต่อภัยคุกคาม

๔.๔.๕ การรายงานผลและการปรับปรุง (Reporting & Improvement)

- การรายงานต่อผู้บริหาร: สรุปผลการตรวจสอบเสนอต่ออธิบดีและคณะกรรมการ ISMS เพื่อพิจารณาสั่งการแก้ไขข้อบกพร่อง (Corrective Action)

- การรายงานต่อหน่วยงานกำกับดูแล: กรมฯ ต้องจัดส่งผลสรุปรายงานการตรวจสอบต่อ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จ ตามมาตรา ๕๔ วรรคสอง
- การปรับปรุงอย่างต่อเนื่อง: นำผลการตรวจสอบมาใช้ในการทบทวนนโยบายและปรับปรุง Playbook ของการรับมือภัยคุกคามให้ทันสมัยอยู่เสมอ

๔.๕ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้สอดคล้องกับมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ และ พรบ. ไซเบอร์ฯ (มาตรา ๕๔) กรมฯ จึงกำหนดแนวทางปฏิบัติในการประเมินความเสี่ยงไว้ดังนี้

๔.๕.๑ วัตถุประสงค์ของการประเมินความเสี่ยง

- เพื่อระบุภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลประชาชน
- เพื่อวิเคราะห์โอกาสที่อาจเกิดเหตุการณ์ (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) ต่อภารกิจของกรมฯ
- เพื่อนำผลการประเมินมาใช้ในการจัดลำดับความสำคัญและเลือกมาตรการควบคุมความปลอดภัยที่เหมาะสม (Risk Treatment)

๔.๕.๒ รอบระยะเวลาการดำเนินงาน

- การประเมินประจำปี: ต้องจัดให้มีการประเมินความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับสภาวะแวดล้อมที่เปลี่ยนแปลง
- การประเมินกรณีพิเศษ: ต้องดำเนินการทันทีเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อระบบงาน เช่น การย้ายระบบไปยัง GDCC หรือการพัฒนาระบบให้บริการใหม่

๔.๕.๓ ขอบเขตและทรัพยากรที่ต้องประเมิน ต้องครอบคลุมสินทรัพย์สารสนเทศสำคัญ (CII) ตามที่ระบุไว้ในแผน BCP ของกรมฯ ได้แก่

- ระบบให้บริการประชาชน: ระบบไทยมีงานทำ, ระบบ DOE e-License และระบบ e-Services ต่างๆ
- ทรัพยากร ๕ ด้าน: อาคารสถานที่, วัสดุอุปกรณ์, เทคโนโลยีสารสนเทศ, บุคลากรหลัก และคู่ค้า/ผู้ให้บริการ

๔.๕.๔ แนวทางและวิธีการประเมิน (Methodology) กรมฯ กำหนดให้ใช้วิธีการประเมินตามมาตรฐานสากล ดังนี้

- การระบุความเสี่ยง: รวบรวมข้อมูลผ่านการสัมภาษณ์บุคลากรและการตรวจสอบขั้นตอนการปฏิบัติงานจริงกรมการจัดหางานกำหนดให้มีการระบุความเสี่ยงอย่างเป็นระบบ เพื่อให้

ครอบคลุมปัจจัยคุกคามที่มีต่อ ความลับ (Confidentiality) ความถูกต้อง (Integrity) และ ความพร้อมใช้ (Availability) ของสารสนเทศภายในขอบเขตระบบ ISMS, โดยมีองค์ประกอบสำคัญดังนี้

๑.การระบุสินทรัพย์สารสนเทศ (Information Asset Identification) ก่อนการระบุความเสี่ยง ต้องมีการจัดทำบัญชีรายการทรัพย์สิน (Asset Inventory) ให้เป็นปัจจุบันเพื่อใช้เป็นฐานข้อมูลในการประเมิน ครอบคลุมทรัพย์สิน ๕ ด้านตามแผน BCP

- ด้านเทคโนโลยีและข้อมูล: เช่น ระบบไทยมีงานทำ, แพลตฟอร์มคนทำงาน, ระบบ DOE e-License และฐานข้อมูลแรงงานต่างด้าว,
- ด้านวัสดุอุปกรณ์: เครื่องคอมพิวเตอร์แม่ข่าย (Server), อุปกรณ์เครือข่าย, และอุปกรณ์พกพา (Notebook/Tablet)
- ด้านอาคารสถานที่: ศูนย์ข้อมูล (Data Center) และพื้นที่ปฏิบัติงานของแต่ละสำนัก/กอง,
- ด้านบุคลากร: บุคลากรหลักที่มีอำนาจหน้าที่สำคัญในกระบวนการทำงาน,
- ด้านคู่ค้าและผู้ให้บริการ: ผู้ให้บริการระบบคลาวด์ (GDCC), ผู้ให้บริการอินเทอร์เน็ต (ISP),

๒. การระบุภัยคุกคาม (Threat Identification) ดำเนินการระบุเหตุการณ์ที่ไม่พึงประสงค์ซึ่งอาจทำให้ภารกิจหยุดชะงัก โดยแบ่งเป็นกลุ่มหลักตามแผน BCP และ พรบ. ไซเบอร์ฯ

- ภัยคุกคามทางไซเบอร์: การบุกรุกระบบ (Intrusion), โปรแกรมไม่พึงประสงค์ (Malware/Ransomware), การโจรกรรมข้อมูล (Data Breach) และข้อมูลรั่วไหลสู่เว็บมืด (Dark Web)
- ภัยพิบัติธรรมชาติและอุบัติเหตุ: อุทกภัย, อัคคีภัย, แผ่นดินไหว และระบบไฟฟ้าขัดข้องเป็นระยะเวลานาน
- ภัยจากการกระทำของมนุษย์: การชุมนุมประท้วง, การจลาจล และความผิดพลาดจากการปฏิบัติงานของเจ้าหน้าที่ (Human Error)
- ภัยจากโรคระบาด: การแพร่ระบาดของโรคติดเชื้อไวรัสที่ส่งผลต่อการมาปฏิบัติงานของบุคลากรหลัก

๓. การระบุจุดอ่อนหรือช่องโหว่ (Vulnerability Identification) ตรวจสอบและบันทึกจุดอ่อนที่มีอยู่ในสินทรัพย์หรือมาตรการควบคุมปัจจุบัน ดังนี้

- ช่องโหว่ทางเทคนิค: ระบบที่ยังไม่ได้ลงโปรแกรมแก้ไข (Unpatched), การตั้งค่ารหัสผ่านที่เดาสุ่มได้ง่าย หรือพอร์ตบริการที่เปิดทิ้งไว้โดยไม่จำเป็น,

- ช่องโหว่ด้านกระบวนการ: การขาดแนวทางปฏิบัติที่ชัดเจน หรือการไม่ซักซ้อมแผนกู้คืนระบบ (DRP) ตามรอบระยะเวลา,
- ช่องโหว่ด้านบุคลากร: การขาดความตระหนักรู้ด้านความปลอดภัยไซเบอร์ (Security Awareness),

๔. การระบุผู้เป็นเจ้าของความเสี่ยง (Risk Owner Identification) ทุกความเสี่ยงที่ระบุได้ ต้องมีการกำหนดบุคคลหรือหน่วยงานที่มีอำนาจหน้าที่และ ความรับผิดชอบในการบริหารจัดการความเสี่ยง นั้น ๆ ให้ชัดเจน เพื่อให้สามารถสั่งการแก้ไขได้อย่างทันท่วงทีตามมาตรฐาน ISO ๒๗๐๐๑

๕. การบันทึกผลการระบุความเสี่ยง ผลลัพธ์ที่ได้จากการระบุความเสี่ยงทั้งหมด จะถูกรวบรวมไว้ใน ทะเบียนความเสี่ยง (Risk Register) ซึ่งต้องระบุถึงผลกระทบและโอกาสที่จะเกิดภัยคุกคามเหล่านั้น เพื่อนำไปใช้ในขั้นตอน การวิเคราะห์ความเสี่ยง (Risk Analysis) ต่อไป

- การวิเคราะห์ความเสี่ยง (Risk Analysis) ภายหลังจากเสร็จสิ้นขั้นตอนการระบุความเสี่ยง กรมการจัดหางานกำหนดให้มีการวิเคราะห์ความเสี่ยงอย่างเป็นระบบเพื่อประเมินระดับความรุนแรงของความเสี่ยงแต่ละรายการ โดยมีรายละเอียดการดำเนินงานดังนี้

๑. การประเมินโอกาสที่จะเกิดเหตุการณ์ (Likelihood Assessment) ให้ประเมินโอกาสที่ภัยคุกคามจะใช้ประโยชน์จากจุดอ่อนหรือช่องโหว่ของสินทรัพย์สารสนเทศจนเกิดเหตุการณ์จริง โดยพิจารณาจากปัจจัยดังต่อไปนี้:

- สถิติในอดีต: ความถี่ที่เคยถูกโจมตีหรือเกิดเหตุการณ์ในลักษณะเดียวกัน
- แรงจูงใจและขีดความสามารถของผู้โจมตี: เช่น กลุ่ม Hacker หรือผู้ไม่ประสงค์ดี
- ความยากง่ายในการใช้ช่องโหว่: เช่น ระบบที่ยังไม่ได้ลง Patch หรือมีการตั้งค่ารหัสผ่านที่เดาสุ่มง่าย

๒. การประเมินผลกระทบ (Impact Assessment) กรมฯ กำหนดเกณฑ์การพิจารณาผลกระทบโดยอ้างอิงจากแผน BCP ซึ่งแบ่งออกเป็น ๕ ระดับ ตามความเสียหายที่มีต่อภารกิจหลักและความเชื่อมั่นของประชาชน

- ระดับสูงมาก (Very High): ส่งผลให้ขีดความสามารถในการให้บริการประชาชน (เช่น ระบบไทยมีงานทำ) ลดลงมากกว่าร้อยละ ๕๐ หรือมีการสูญเสียชีวิตและทรัพย์สิน
- ระดับสูง (High): ขีดความสามารถลดลงร้อยละ ๒๕-๕๐ มีผลกระทบรุนแรงต่อบริการหลายส่วน และต้องการการบริหารจัดการอย่างเร่งด่วน
- ระดับปานกลาง (Medium): ขีดความสามารถลดลงร้อยละ ๑๐-๒๕ ต้องปรับแผนและทรัพยากรบางส่วน
- ระดับต่ำ (Low): มีผลเล็กน้อยต่อการให้บริการ กระทบขีดความสามารถร้อยละ ๕-๑๐

- ระดับต่ำมาก (Very Low): กระทบน้อยกว่าร้อยละ ๕ ไม่ส่งผลเสียต่อการให้บริการประชาชนอย่างมีนัยสำคัญ

๓. การวิเคราะห์ตามสถานการณ์สมมติ (Scenario-based Analysis) กรมฯ กำหนดให้มีการวิเคราะห์ความเสี่ยงเชิงลึกผ่านการจำลองเหตุการณ์ที่อาจเกิดขึ้นจริงกับระบบสำคัญ ดังนี้

- กรณีถูกโจมตีด้วย Ransomware: วิเคราะห์ผลกระทบหากฐานข้อมูลใน ระบบ DOE e-License ถูกเข้ารหัสจนไม่สามารถออกใบอนุญาตได้ และความพร้อมของข้อมูลสำรองบน GDCC
- กรณีข้อมูลรั่วไหล (Data Breach): วิเคราะห์ความเสียหายต่อชื่อเสียงและบทลงโทษตาม PDPA หากข้อมูลส่วนบุคคลของแรงงานไทยที่ไปทำงานต่างประเทศถูกโจรกรรม
- กรณีการบุกรุกระบบ (Intrusion): วิเคราะห์ช่องทางการเข้าถึงที่ผิดปกติและการทำงานของระบบ SOC ในการตรวจจับพฤติกรรมที่น่าสงสัย

๔. การกำหนดระดับของความเสี่ยง (Risk Level Determination) กรมฯ ใช้ตาราง Risk Matrix (โอกาส x ผลกระทบ) เพื่อคำนวณและระบุระดับของความเสี่ยงที่วิเคราะห์ได้ เพื่อนำไปเปรียบเทียบกับเกณฑ์การยอมรับความเสี่ยง (Risk Appetite) ในขั้นตอนการประเมินผล (Risk Evaluation) ต่อไป

ตารางที่ ๑: เกณฑ์การพิจารณาระดับของผลกระทบ (Impact Assessment Criteria)

อ้างอิงตามเกณฑ์ในแผน BCP ปี ๒๕๖๙ ของกรมการจัดหางาน

ระดับผลกระทบ	คำอธิบายระดับความเสียหาย
๕ : สูงมาก	มีการสูญเสียชีวิต, ขีดความสามารถในการให้บริการ (เช่น ระบบไทยมีงานทำ) ลดลงมากกว่า ๕๐%, เสียหายต่อชื่อเสียงอย่างรุนแรง
๔ : สูง	บาดเจ็บรุนแรง, ขีดความสามารถในการให้บริการลดลง ๒๕ – ๕๐%, ต้องการการบริหารจัดการอย่างเร่งด่วน
๓ : ปานกลาง	บาดเจ็บไม่รุนแรงแต่ต้องรักษาพยาบาล, ขีดความสามารถลดลง ๑๐ – ๒๕%, ต้องปรับแผนและทรัพยากรบางส่วน
๒ : ต่ำ	บาดเจ็บเล็กน้อย, ขีดความสามารถลดลง ๕ – ๑๐%, มีผลเล็กน้อยต่อบางหน่วยงานหรือการให้บริการ
๑ : ต่ำมาก	ส่งผลให้ขีดความสามารถลดลงน้อยกว่า ๕%, ไม่กระทบต่อการดำเนินงานหรือบริการประชาชนอย่างมีนัยสำคัญ

ตารางที่ ๒: เกณฑ์การพิจารณาโอกาสที่จะเกิดเหตุการณ์ (Likelihood Assessment Criteria)

กำหนดขึ้นตามมาตรฐานการบริหารความเสี่ยงระดับสากลเพื่อให้สัมพันธ์กับระดับผลกระทบ

ระดับโอกาส	คำอธิบายความถี่ของเหตุการณ์
๕ : สูงมาก	เกิดขึ้นประจำ (เช่น ทุกเดือน) หรือคาดว่าจะเกิดขึ้นแน่นอนในอนาคตอันใกล้
๔ : สูง	เกิดขึ้นบ่อย (เช่น ปีละหลายครั้ง) หรือมีสถิติการถูกโจมตี/ขัดข้องสูง
๓ : ปานกลาง	อาจจะเกิดขึ้นได้ (เช่น ปีละ ๑ ครั้ง) หรือระบบมีช่องโหว่ที่ผู้โจมตีเข้าถึงได้ไม่ยาก
๒ : ต่ำ	นาน ๆ เกิดครั้ง (เช่น ๒ - ๕ ปีต่อครั้ง) หรือระบบมีมาตรการป้องกันที่ค่อนข้างดี
๑ : ต่ำมาก	แทบจะไม่เคยเกิดขึ้นเลย (> ๕ ปีต่อครั้ง) หรือมีมาตรการควบคุมที่เข้มงวดมาก

ตารางที่ ๓: ตาราง Risk Matrix (โอกาส x ผลกระทบ)

ใช้สำหรับคำนวณระดับความเสี่ยงเพื่อกำหนดความเร่งด่วนในการจัดการ

โอกาส / ผลกระทบ	๑ (ต่ำมาก)	๒ (ต่ำ)	๓ (ปานกลาง)	๔ (สูง)	๕ (สูงมาก)
๕ (สูงมาก)	๕	๑๐	๑๕	๒๐	๒๕
๔ (สูง)	๔	๘	๑๒	๑๖	๒๐
๓ (ปานกลาง)	๓	๖	๙	๑๒	๑๕
๒ (ต่ำ)	๒	๔	๖	๘	๑๐
๑ (ต่ำมาก)	๑	๒	๓	๔	๕

ตารางที่ ๔: เกณฑ์ระดับความเสี่ยงและการจัดการ (Risk Level & Action)

เปรียบเทียบผลลัพธ์จาก Matrix กับเกณฑ์การยอมรับความเสี่ยง (Risk Appetite):

คะแนน (คะแนนรวม)	ระดับความเสี่ยง	แนวทางปฏิบัติ/การจัดการความเสี่ยง (Risk Treatment)
๑๖ - ๒๕	สูงมาก (Very High)	**ยอมรับไม่ได้:** ต้องกำหนดมาตรการควบคุมทันทีและมีแผนจัดการความเสี่ยงเร่งด่วน
๑๐ - ๑๕	สูง (High)	**ยอมรับไม่ได้:** ต้องกำหนดมาตรการลดความเสี่ยง (Mitigation) และรายงานผู้บริหาร
๕ - ๙	ปานกลาง (Medium)	**เฝ้าระวัง:** พิจารณาเพิ่มมาตรการควบคุมตามความเหมาะสม และติดตามผลสม่ำเสมอ
๑ - ๔	ต่ำ (Low)	**ยอมรับความเสี่ยง:** ยอมรับความเสี่ยงได้ภายใต้มาตรการปัจจุบัน แต่ต้องมีการทบทวนรายปี

- การประเมินผลความเสี่ยง (Risk Evaluation)กรมการจัดหางานกำหนดให้มีการประเมินผลความเสี่ยงเพื่อตัดสินใจว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้ และความเสี่ยงใดจำเป็นต้องได้รับการจัดการอย่างเร่งด่วน โดยมีขั้นตอนการดำเนินงานดังนี้

๑. การเปรียบเทียบผลการวิเคราะห์กับเกณฑ์ที่กำหนด (Comparison against Risk Criteria) ให้นำค่าระดับความเสี่ยง (Risk Level) ที่ได้จากขั้นตอนการวิเคราะห์ (โอกาส x ผลกระทบ) มาเปรียบเทียบกับ เกณฑ์การยอมรับความเสี่ยง (Risk Appetite) ที่กรมฯ กำหนดไว้

- ความเสี่ยงระดับต่ำ (Low): เป็นความเสี่ยงที่อยู่ในเกณฑ์ยอมรับได้ กรมฯ อาจพิจารณาเพียงการเฝ้าระวังและติดตามผล (Monitor) ตามรอบปกติ
- ความเสี่ยงระดับปานกลาง ถึง สูงมาก (Medium - Very High): เป็นความเสี่ยงที่เกินกว่าเกณฑ์การยอมรับ (Risk Tolerance) จำเป็นต้องกำหนดมาตรการจัดการความเสี่ยง (Risk Treatment) เพื่อลดระดับความเสี่ยงให้อยู่ในเกณฑ์ที่เหมาะสม

๒. การจัดลำดับความสำคัญของความเสี่ยง (Risk Prioritization) กรมฯ จะดำเนินการจัดลำดับความสำคัญของความเสี่ยงทั้งหมดที่ระบุได้ เพื่อจัดสรรทรัพยากรและงบประมาณในการป้องกันอย่างมีประสิทธิภาพ

- ลำดับที่ ๑: ความเสี่ยงที่มีผลกระทบต่อชีวิต ทรัพย์สิน หรือระบบให้บริการประชาชนหลัก (CII) เช่น ระบบไทยมีงานทำ หรือ ระบบ DOE e-License
- ลำดับที่ ๒: ความเสี่ยงที่มีผลต่อการเสียชื่อเสียงของหน่วยงานหรือบทลงโทษทางกฎหมาย (PDPA)
- ลำดับที่ ๓: ความเสี่ยงที่มีผลต่อประสิทธิภาพการทำงานภายใน

๓. การตัดสินใจในการจัดการความเสี่ยง (Risk Treatment Decision) สำหรับความเสี่ยงที่ยอมรับไม่ได้ คณะบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team) จะพิจารณาเลือกแนวทางจัดการตามความเหมาะสม

- การลดความเสี่ยง (Mitigation): นำมาตรการควบคุมจาก Annex A ของ ISO ๒๗๐๐๑ มาใช้งาน เช่น การติดตั้งระบบ SOC/EDR หรือการสำรองข้อมูลบน GDCC
- การโอนความเสี่ยง (Transfer): เช่น การทำประกันภัยไซเบอร์ หรือการจ้างผู้เชี่ยวชาญภายนอก (Outsource) ดูแลระบบ.
- การหลีกเลี่ยงความเสี่ยง (Avoidance): การยุติกิจกรรมหรือกระบวนการที่มีความเสี่ยงสูงเกินไป.
- การยอมรับความเสี่ยง (Acceptance): กรณีที่ต้นทุนในการจัดการสูงกว่าผลกระทบและผู้บริหารระดับสูงเซ็นรับรองอย่างเป็นลายลักษณ์อักษร.

๔. การจัดทำรายงานผลการประเมินความเสี่ยง (Reporting) สรุปผลการดำเนินการทั้งหมดจัดทำเป็น รายงานผลการประเมินความเสี่ยง (Risk Assessment Report) เพื่อเสนอต่ออธิบดีในฐานะผู้บริหารระดับสูงสุดเพื่อพิจารณาอนุมัติแผนจัดการความเสี่ยง

๔.๕.๕ การรายงานและการปรับปรุง

- การสรุปผล: จัดทำ รายงานผลการประเมินความเสี่ยง (Risk Assessment Report) และขอรับรองผลจากผู้บริหารระดับสูง (อธิบดี) ในฐานะเจ้าของความเสี่ยง
- การส่งรายงาน: จัดส่งสรุปผลการประเมินต่อ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน ๓๐ วันหลังจากดำเนินการเสร็จสิ้น
- การพัฒนาต่อเนื่อง: นำผลลัพธ์ที่ได้ไปปรับปรุงแผนบริหารความพร้อมต่อสภาวะวิกฤต (BCP) และแผนกู้คืนระบบ (DRP) ให้มีความพร้อมรับมือกับภัยคุกคามรูปแบบใหม่เสมอ

ภาคผนวก ก

รายชื่อบุคลากรและช่องทางติดต่อสื่อสาร (BCP Team)

เพื่อให้การบริหารความต่อเนื่องและการสื่อสารในสภาวะวิกฤตเป็นไปอย่างมีประสิทธิภาพ กรมการจัดหางานได้กำหนดรายชื่อคณะบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team) และช่องทางติดต่อสื่อสารไว้ดังนี้

ก.๑ รายชื่อคณะบริหารความพร้อมต่อสภาวะวิกฤต (BCP Team)

(ข้อมูล ณ มกราคม ๒๕๖๙)

บทบาทในทีม BCP	รายชื่อบุคลากรหลัก	เบอร์โทรศัพท์ที่ทำงาน	เบอร์โทรศัพท์มือถือ	บุคลากรสำรอง
หัวหน้าคณะบริหารความพร้อมฯ	นายสมชาย มรกต ศรีวรรณ (อธิบดี)	๐๒ ๒๔๘ ๖๘๖๖	๐๘๙ ๘๑๑ ๐๙๒๕	-
รองหัวหน้าคณะบริหารความพร้อมฯ	นายมงคล สงคราม (รองอธิบดี)	๐๒ ๒๔๘ ๖๘๖๙	๐๙๓ ๗๘๗ ๘๘๙๙	นายขัตติยะ แพนเดช
รองหัวหน้าคณะบริหารความพร้อมฯ	นายวิชิต อินทรเจริญ (รองอธิบดี)	๐๒ ๒๔๘ ๖๘๓๒	๐๘๐ ๐๔๓ ๙๕๒๘	-
ผู้ประสานงานคณะบริหารความพร้อมฯ	นางสาวศิริวรรณ ศุภมิตร	๐๒ ๒๔๕ ๖๘๒๙	๐๘๐ ๐๔๓ ๙๘๒๗	-
หัวหน้าทีมฯ (ICT)	นางจิณณาพัต ปาจรีย์อนันต์	๐๒ ๓๕๔ ๐๐๙๙	๐๙๙ ๐๕๑ ๔๑๔๗	นายสุรเจตน์ บัวชุม
หัวหน้าทีมฯ (แรงงานต่างด้าว)	นายสมมาตร อนันต์ธราทรัพย์	๐๒ ๓๕๔ ๐๐๘๒	๐๖๔ ๓๕๙ ๙๖๖๓	นางสาวอารีวรรณ โพธิ์นิ่มแดง
หัวหน้าทีมฯ (สจก. ๑ - ๑๐)	ผู้อำนวยการ สจก. พื้นที่ ๑ – ๑๐	(ตามพื้นที่)	(ตามพื้นที่)	ผู้ช่วยผู้อำนวยการ สจก.

[อ้างอิงรายชื่อและเบอร์โทรศัพท์ทั้งหมดจากตารางที่ ๑ ในแผน BCP หน้า ๔ - ๘]

ก.๒ ขั้นตอนการแจ้งเหตุฉุกเฉิน (Call Tree Protocol)

กรมฯ ใช้ระบบการสื่อสารแบบสายสัมพันธ์ (Call Tree) เพื่อกระจายข้อมูลในภาวะวิกฤต ดังนี้

จุดเริ่มต้น: หัวหน้าคณะบริหารความพร้อมฯ (อธิบดี) แจ้งเหตุไปยังผู้ประสานงาน (เลขานุการกรม)

การกระจายข้อมูลระดับบริหาร: ผู้ประสานงานแจ้งไปยังหัวหน้าทีมบริหารความพร้อมฯ ของแต่ละสำนัก/กอง/ศูนย์

การแจ้งระดับปฏิบัติการ: หัวหน้าทีมแต่ละหน่วยงานแจ้งต่อไปยังบุคลากรภายใต้บังคับบัญชาตามลำดับ

ช่องทางการติดต่อ:

ในเวลาทำการ: ใช้โทรศัพท์หน่วยงานเป็นอันดับแรก

นอกเวลาทำการ: หรือหากสถานที่หลักได้รับผลกระทบ ให้ใช้โทรศัพท์มือถือเป็นอันดับแรก

การรายงานผล: หัวหน้าหน่วยงานต้องโทรกลับมารายงานความพร้อมและความปลอดภัยของเจ้าหน้าที่ต่อผู้ประสานงานฯ เพื่อสรุปรายงานต่ออธิบดี

ก.๓ ช่องทางสื่อสารสำรอง (Back-up Channels)

ในกรณีที่ระบบโทรศัพท์หลักขัดข้อง ให้ใช้ช่องทางดังต่อไปนี้ในการประสานงาน:

แอปพลิเคชันออนไลน์: Line, Facebook, Zoom

อินเทอร์เน็ตฉุกเฉิน: Pocket Wi-Fi หรือการแชร์ Hotspot จากโทรศัพท์ Smartphone ของเจ้าหน้าที่

อีเมลกลาง: saraban@doe.go.th

ก.๔ การปรับปรุงข้อมูล

ทีมบริหารความพร้อมต่อสภาวะวิกฤตมีหน้าที่ต้องทบทวนและปรับปรุงรายชื่อบุคลากรและเบอร์โทรศัพท์ติดต่อให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงบุคลากรในตำแหน่งสำคัญ

ภาคผนวก ข

บัญชีระบบสารสนเทศและระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (RTO)

กรมการจัดหางานกำหนดลำดับความสำคัญของระบบสารสนเทศและฐานข้อมูลตามระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO) เพื่อให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) สามารถบริหารจัดการการกู้คืนระบบจาก ระบบคลาวด์กลางภาครัฐ (GDCC) ได้อย่างมีประสิทธิภาพ ดังนี้

ข.๑ ระบบให้บริการประชาชนและภาคธุรกิจ (Public Service Systems)

เป็นกลุ่มระบบที่มีความสำคัญสูงสุดต่อภารกิจหลัก หากหยุดชะงักจะส่งผลกระทบรุนแรงต่อประชาชนและความเชื่อมั่นขององค์กร

ชื่อระบบสารสนเทศ / ฐานข้อมูล	วัตถุประสงค์หลัก	ระยะเวลากู้คืน (RTO)
ระบบไทยมีงานทำ	บริการจับคู่งานและแจ้งตำแหน่งงานว่าง	ภายใน ๑ วัน
แพลตฟอร์มคนทำงาน (Khon Tham Ngan)	ระบบบริหารจัดการข้อมูลคนทำงาน	ภายใน ๑ วัน
ระบบส่งเสริมการมีงานทำ (Employmentguide)	ข้อมูลแนวอาชีพและส่งเสริมการมีงานทำ	ภายใน ๑ วัน
ระบบอิเล็กทรอนิกส์การบริหารแรงงานไทยไปต่างประเทศ	จัดการฐานข้อมูลและอนุญาตไปทำงานต่างประเทศ	ภายใน ๑ วัน
ระบบอนุญาตทำงานคนต่างด้าว ๔ สัญชาติ (e-WorkPermit)	การขอรับใบอนุญาตทำงานผ่านระบบออนไลน์	ภายใน ๑ วัน
ระบบแจ้งการทำงานของคนต่างด้าว	การแจ้งเข้า-ออกจากงานของแรงงานต่างด้าว	ภายใน ๑ วัน
ระบบ Single Window For Visa and Work Permit	เชื่อมโยงข้อมูลวีซ่าและใบอนุญาตทำงาน	ภายใน ๑ วัน
ระบบการให้สิทธิและขอรับสิทธิผู้พิการ (ม.๓๕)	บริการสิทธิประโยชน์สำหรับผู้พิการ	ภายใน ๑ วัน
เว็บไซต์กรมการจัดหางาน (DOE Website)	ช่องทางการสื่อสารข้อมูลข่าวสารหลักแก่ประชาชน	ภายใน ๑ วัน

ข.๒ ระบบโครงสร้างพื้นฐานและงานสนับสนุนภายใน (Infrastructure & Internal Support)

เป็นระบบที่จำเป็นสำหรับการสื่อสารและการบริหารงานภายในราชการ

ชื่อระบบสารสนเทศ / ฐานข้อมูล	วัตถุประสงค์หลัก	ระยะเวลากู้คืน (RTO)
ระบบอินเทอร์เน็ต (Main Internet)	การเชื่อมต่อโครงข่ายหลักของกรมฯ	ภายใน ๑ วัน
ระบบเชื่อมต่อฉุกเฉิน (Air card / Pocket Wi-Fi)	ช่องทางสำรองกรณีเครือข่ายหลักเสียหาย	ภายใน ๑ วัน
ระบบสารบรรณอิเล็กทรอนิกส์ (e-Saraban)	การรับ-ส่ง และบริหารจัดการหนังสือราชการ	ภายใน ๓ วัน
ระบบ Smart Office	การบริหารจัดการสำนักงานอัตโนมัติ	ภายใน ๓ วัน
ระบบประชุมทางไกล (VDO Conference)	การประสานงานและประชุมในภาวะวิกฤต	ภายใน ๓ วัน
ระบบ Call Center (๑๕๐๖ กด ๒)	ช่องทางตอบข้อซักถามและรับเรื่องร้องทุกข์	ภายใน ๓ วัน
ฐานข้อมูลงานการเงินและบัญชี	การเบิกจ่ายงบประมาณและนำส่งเงิน	ภายใน ๓ วัน
ระบบบริหารทรัพยากรบุคคล (HR System)	การบริหารข้อมูลบุคลากรและสิทธิสวัสดิการ	ภายใน ๗ วัน
ระบบ DOE e-License	การออกใบอนุญาตจัดหางานและงานทะเบียน	ภายใน ๑๕ วัน

ข.๓ ลำดับความสำคัญเชิงโครงสร้าง (Critical IT Assets)

การจัดลำดับการกู้คืนตามผลกระทบต่ออาคารและเทคโนโลยีสารสนเทศ

๑. ลำดับที่ ๑: ระบบสารสนเทศสำหรับให้บริการประชาชนทั้งหมด (RTO ๑ วัน)

๒. ลำดับที่ ๒: ระบบเครือข่ายสื่อสารข้อมูลที่เชื่อมโยงหน่วยงานภายในและภายนอก (RTO ๓ วัน)

๓. ลำดับที่ ๓: ระบบอัตโนมัติของห้อง Data Center เพื่อรักษาความพร้อมใช้ของฐานข้อมูลกลาง (RTO ๓ วัน)

ข้อมูล RTO นี้ใช้เป็นเกณฑ์ในการประกาศใช้แผนกู้คืนระบบ (DRP) และการทดสอบกู้คืนข้อมูลสำรองจาก GDCC อย่างน้อยปีละ ๑ ครั้ง ตามมาตรา ๕๖ แห่ง พรบ. ไซเบอร์ฯ และมาตรฐาน ISO ๒๗๐๐๑

ภาคผนวก ค

แบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามไซเบอร์

(Cyber Incident Reporting Form)

คำชี้แจง: ให้บุคลากรที่พบเหตุการณ์ผิดปกติ หรือเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ใช้แบบฟอร์มนี้ในการบันทึกและรายงานเหตุการณ์ภัยคุกคามไซเบอร์ต่อผู้บังคับบัญชา และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ตามความเหมาะสม

ส่วนที่ ๑: ข้อมูลผู้รายงานเหตุการณ์

- ชื่อ-นามสกุล: .....
- หน่วยงาน/กอง: .....
- เบอร์โทรศัพท์ติดต่อ: .....
- อีเมล: .....
- วันที่และเวลาที่พบเหตุการณ์: วันที่ ..... เดือน ..... พ.ศ. ..... เวลา ..... น.

ส่วนที่ ๒: รายละเอียดเหตุการณ์ (Incident Details)

- ประเภทของภัยคุกคาม (ระบุ):
    - [ ] การบุกรุกระบบ (Intrusion / Unauthorized Access)
    - [ ] โปรแกรมไม่พึงประสงค์ (Malware / Ransomware)
    - [ ] การปฏิเสธการให้บริการ (DoS/DDoS)
    - [ ] ข้อมูลรั่วไหล (Data Leak / Credentials Leak)
    - [ ] อื่นๆ (ระบุ) .....
- ระบบสารสนเทศหรือสินทรัพย์ที่ได้รับผลกระทบ:
    - [ ] ระบบไทยมีงานทำ / แพลตฟอร์มคนทำงาน
    - [ ] ระบบ DOE e-License / e-WorkPermit

- [ ] เว็บไซต์กรมการจัดหางาน (DOE Website)
- [ ] ระบบเครือข่ายภายใน / ห้อง Data Center
- [ ] อื่นๆ (ระบุ) .....

- คำอธิบายลักษณะเหตุการณ์เบื้องต้น:

.....

.....

ส่วนที่ ๓: การประเมินระดับความรุนแรง (Severity Level)

- [ ] ระดับไม่ร้ายแรง: ระบบด้อยประสิทธิภาพลง แต่ยังให้บริการได้
- [ ] ระดับร้ายแรง: ระบบสำคัญเสียหายจนให้บริการประชาชนไม่ได้ (เช่น ระบบไทยมีงานทำ ล่ม)
- [ ] ระดับวิกฤต: กระทบวงกว้างในระดับประเทศ หรือมีความเสี่ยงต่อชีวิตและทรัพย์สินประชาชน

ส่วนที่ ๔: การดำเนินการเบื้องต้น (Initial Response)

- การระงับเหตุที่ดำเนินการไปแล้ว: (เช่น ตัดการเชื่อมต่อเครือข่าย, ปิดเครื่องที่ติดเชื้อ)

.....

- สถานะปัจจุบันของเหตุการณ์:
  - [ ] อยู่ระหว่างการควบคุมสถานะ (Contained)
  - [ ] อยู่ระหว่างการกู้คืนระบบ (Recovery)
  - [ ] ดำเนินการเสร็จสิ้นแล้ว (Resolved)

ส่วนที่ ๕: การลงนามและการรายงาน

- ลงชื่อผู้รายงาน: ..... วันที่ .....
- ความเห็นของหัวหน้าทีมบริหารความพร้อมฯ (ผอ.กอง/สำนัก): .....
- คำสั่งการของหัวหน้าคณะบริหารความพร้อมฯ (อธิบดี): .....

หมายเหตุ:ให้จัดเก็บแบบฟอร์มนี้ไว้ใน สมุดบันทึกกิจกรรม (Log Book) เพื่อใช้ในการถอดบทเรียน (Lesson Learned) และสรุปรายงานประจำเดือนตามโครงการ SOC