คู่มือการกำกับดูแลและบริหารจัดการระบบสารสนเทศ
ตามเกณฑ์ GECC ข้อ 4.5
สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี
ประจำปีงบประมาณ พ.ศ. 2569

บทที่ 1 บทนำ

คู่มือนี้จัดทำขึ้นเพื่อกำหนดแนวทางการกำกับดูแลและบริหารจัดการระบบสารสนเทศของสถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ให้สอดคล้องตามเกณฑ์ GECC ข้อ 4.5 โดยเน้นการแต่งตั้งผู้ดูแลระบบ การติดตามดูแลระบบอย่างต่อเนื่อง และการกำหนดมาตรฐานระยะเวลาในการแก้ไขปัญหาอย่างชัดเจน

บทที่ 2 โครงสร้างการกำกับดูแลระบบ (IT Governance)

หน่วยงานได้แต่งตั้งเจ้าหน้าที่ผู้ดูแลระบบอย่างเป็นทางการ ทำหน้าที่ Monitoring
ตรวจสอบสถานะระบบอย่างสม่ำเสมอ
และประสานงานกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาฝีมือแรงงานเมื่อเกิดเหตุขัดข้อง เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่อง

บทที่ 3 การตอบสนองเหตุการณ์และ SLA

เมื่อเกิดเหตุการณ์ผิดปกติ
เจ้าหน้าที่ผู้ดูแลระบบจะดำเนินการตรวจสอบและประเมินความรุนแรงของปัญหา
พร้อมแจ้งส่วนกลางภายใน 30 นาที ตามมาตรฐาน SLA
และดำเนินการกู้คืนระบบให้สามารถกลับมาใช้งานได้ภายใน 48 ชั่วโมง
เพื่อลดผลกระทบต่อการให้บริการประชาชน

บทที่ 4 แผนบริหารความต่อเนื่องในภาวะวิกฤต (BCP)

หน่วยงานได้จัดทำแผนบริหารความต่อเนื่องในภาวะวิกฤต
และแผนรองรับภาวะฉุกเฉินด้านเทคโนโลยีสารสนเทศ เพื่อรองรับเหตุการณ์ที่อาจส่งผลกระทบต่อระบบ
โดยกำหนดแนวทางการสำรองข้อมูล การกู้คืนระบบ และโครงสร้างทีม BCP อย่างชัดเจน

บทที่ 5 สรุปผลการดำเนินงาน

การดำเนินงานของหน่วยงานแสดงให้เห็นถึงการกำกับดูแลระบบอย่างเป็นระบบ มี Monitoring
อย่างต่อเนื่อง กำหนด SLA แจ้งเหตุภายใน 30 นาที กู้คืนระบบภายใน 48 ชั่วโมง และมีแผน BCP
รองรับสถานการณ์วิกฤตอย่างครบถ้วน สอดคล้องตามเกณฑ์ GECC ปี 2569 ระดับ 2 คะแนนเต็ม

กรมพัฒนาฝีมือแรงงานได้มอบหมายเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทำหน้าที่เป็นผู้ดูแลระบบและติดตามดูแลระบบ (Monitoring) ของส่วนกลาง ที่มีหน้าที่ในการปฏิบัติตามแผนกำกับดูแลการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Governance) และความเสี่ยงด้านภัยคุกคามไซเบอร์ (Cyber Risk) และตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมพัฒนาฝีมือแรงงาน ประกอบกับแผนรองรับภาวะฉุกเฉินและภัยธรรมชาติ (IT Contingency Plan) โดยดำเนินการแก้ปัญหาเพื่อให้ระบบต่างๆ สามารถกลับมาใช้งานได้ตามปกติภายใน 48 ชั่วโมง และกำกับดูแลผู้ดูแลระบบของหน่วยงานในภูมิภาคเพื่อให้หน่วยงานที่ตั้งในภูมิภาคสามารถใช้งานระบบในการให้บริการได้อย่างต่อเนื่อง

สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ได้ดำเนินการมอบหมายเจ้าหน้าที่เป็นผู้ดูแลระบบและติดตามดูแลระบบ (Monitoring) เพื่อดำเนินการให้สอดคล้องกับแผนฯ ของส่วนกลาง โดยมีการแต่งตั้งเจ้าหน้าที่ จำนวน 2 คน เพื่อประสานงานกับส่วนกลางในการแก้ไขปัญหาอย่างเร่งด่วน และบริหารจัดการระบบการให้บริการต่าง ๆ ของหน่วยงานในเบื้องต้น เพื่อไม่ให้ระบบเกิดการบริการหยุดชะงัก ทั้งในส่วนสำหรับผู้รับบริการและเจ้าหน้าที่ ซึ่งเจ้าหน้าที่จะได้รับการอบรมหลักสูตรการใช้งานระบบสำหรับให้บริการประชาชนและปฏิบัติงานภายใน เป็นประจำทุกปี

1. หนังสือ/คำสั่ง มอบหมายหรือแต่งตั้งเจ้าหน้าที่เป็นผู้ดูแลระบบและติดตามดูแลระบบของหน่วยงาน

2. แผนกำกับดูแลการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Governance) และความเสี่ยงด้านภัยคุกคามไซเบอร์ (Cyber Risk)

2.1 แผน IT Governance & Cyber Risk สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ได้กำหนดแผนกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance) และการบริหารความเสี่ยงด้านภัยคุกคามไซเบอร์ (Cyber Risk) เพื่อใช้เป็นกรอบแนวทางในการควบคุม กำกับ และบริหารจัดการระบบสารสนเทศของหน่วยงานให้มีความมั่นคงปลอดภัย และสามารถรองรับการให้บริการประชาชนผ่านระบบอิเล็กทรอนิกส์ได้อย่างต่อเนื่อง โดยดำเนินการให้สอดคล้องกับนโยบายและแผนของกรมพัฒนาฝีมือแรงงาน

2.2 นโยบายความมั่นคงปลอดภัยสารสนเทศ หน่วยงานถือปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพัฒนาฝีมือแรงงาน โดยกำหนดมาตรการควบคุมการเข้าถึงข้อมูล การกำหนดสิทธิ์ผู้ใช้งาน การรักษาความลับของข้อมูลราชการ และการป้องกันการรั่วไหลของ

ข้อมูลส่วนบุคคล รวมทั้งสร้างความตระหนักรู้ให้แก่เจ้าหน้าที่เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินงานเป็นไปอย่างปลอดภัยและเป็นระบบ

2.3 แผนรองรับภาวะฉุกเฉิน (IT Contingency Plan) สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรีมีการดำเนินงานภายใต้แผนรองรับภาวะฉุกเฉินและภัยธรรมชาติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเตรียมความพร้อมรองรับกรณีระบบขัดข้องหรือเกิดเหตุการณ์ไม่คาดคิด เช่น ระบบล่ม ไฟฟ้าดับ หรือการโจมตีทางไซเบอร์ โดยกำหนดแนวทางการสำรองข้อมูล การกู้คืนระบบ และการประสานงานกับส่วนกลาง เพื่อให้ระบบสามารถกลับมาใช้งานได้ตามปกติในระยะเวลาที่กำหนด (เอกสารแนบ)

2.4 การติดตามดูแลระบบ (Monitoring & Coordination) หน่วยงานได้แต่งตั้งเจ้าหน้าที่ผู้ดูแลระบบสารสนเทศ ทำหน้าที่ติดตาม ตรวจสอบ และเฝ้าระวังการทำงานของระบบอย่างสม่ำเสมอ (Monitoring) เพื่อป้องกันมิให้ระบบการให้บริการเกิดการหยุดชะงัก ทั้งนี้ เมื่อพบปัญหา เจ้าหน้าที่จะดำเนินการแก้ไขเบื้องต้น และประสานงานกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของส่วนกลางทันที เพื่อให้สามารถแก้ไขปัญหาได้อย่างรวดเร็วและลดผลกระทบต่อผู้รับบริการ

2.5 การป้องกันภัยคุกคามไซเบอร์ (Cyber Threat Management) หน่วยงานมีมาตรการป้องกันภัยคุกคามไซเบอร์ เช่น การติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัส การอัปเดตระบบปฏิบัติการอย่างสม่ำเสมอ การควบคุมการเข้าถึงระบบ และการสร้างความรู้ความเข้าใจแก่บุคลากรเกี่ยวกับการป้องกันภัยคุกคามเช่น Malware และ Phishing ทั้งนี้ เพื่อป้องกันการโจมตีที่อาจส่งผลกระทบต่อข้อมูลและระบบสารสนเทศของหน่วยงาน

2.6 การสำรองข้อมูลและการตอบสนองเหตุการณ์ (Backup & Incident Response) สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ดำเนินการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ และจัดเตรียมแนวทางการตอบสนองเมื่อเกิดเหตุการณ์ผิดปกติ (Incident Response) เพื่อให้สามารถกู้คืนข้อมูลและระบบกลับมาใช้งานได้อย่างรวดเร็ว ทั้งนี้ การดำเนินงานดังกล่าวช่วยลดความเสียหายและสร้างความมั่นใจให้แก่ผู้รับบริการว่าหน่วยงานมีความพร้อมในการบริหารจัดการเหตุการณ์ฉุกเฉิน

3. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมพัฒนาฝีมือแรงงาน

สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ดำเนินงานภายใต้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพัฒนาฝีมือแรงงาน โดยมีวัตถุประสงค์เพื่อกำหนดแนวทางและมาตรการในการคุ้มครองข้อมูลสารสนเทศของทางราชการ ให้มีความถูกต้อง ครบถ้วน พร้อมใช้งาน และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ทั้งนี้ เพื่อให้การให้บริการประชาชนผ่านระบบสารสนเทศและระบบอิเล็กทรอนิกส์เป็นไปอย่างปลอดภัยและต่อเนื่อง (เอกสารแนบ)

แนวทางสำคัญของนโยบาย

3.1 การควบคุมการเข้าถึงข้อมูล (Access Control) กำหนดสิทธิ์การเข้าถึงข้อมูลตามระดับหน้าที่ความรับผิดชอบของเจ้าหน้าที่ และมีการกำหนดรหัสผ่านที่มีความปลอดภัย รวมถึงการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

3.2 การป้องกันภัยคุกคามไซเบอร์ (Cyber Security Protection) ติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัส (Antivirus) และระบบ Firewall อย่างสม่ำเสมอ พร้อมอัปเดตระบบปฏิบัติการและโปรแกรมต่าง ๆ เพื่อป้องกันมัลแวร์ การโจมตีทางไซเบอร์ และการรั่วไหลของข้อมูล

3.3 การสำรองและกู้คืนข้อมูล (Backup & Recovery) ดำเนินการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ และสามารถกู้คืนข้อมูลได้เมื่อเกิดเหตุการณ์ผิดปกติ เพื่อให้ระบบสามารถกลับมาใช้งานได้ตามปกติ

3.4 การสร้างความตระหนักรู้ (Awareness) ส่งเสริมให้เจ้าหน้าที่มีความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ เช่น การระวังการเปิดอีเมลหรือไฟล์แนบที่ไม่ปลอดภัย การป้องกันการหลอกลวงทางออนไลน์ (Phishing) และการรักษาความลับของข้อมูลราชการ

3.5 การติดตามและประเมินผล มีการติดตาม ตรวจสอบ และรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศต่อผู้บังคับบัญชา และประสานศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรมทันทีเมื่อพบเหตุผิดปกติ

4. แผนรองรับภาวะฉุกเฉินและภัยธรรมชาติ (IT Contingency Plan)

4.1 สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ได้จัดทำแผนรองรับภาวะฉุกเฉินและภัยธรรมชาติด้านเทคโนโลยีสารสนเทศ เพื่อเตรียมความพร้อมรองรับเหตุการณ์ที่อาจส่งผลกระทบต่อระบบสารสนเทศและการให้บริการประชาชน เช่น ระบบขัดข้อง ไฟฟ้าดับ อินเทอร์เน็ตล่ม ภัยธรรมชาติ หรือการโจมตีทางไซเบอร์ ทั้งนี้ เพื่อให้หน่วยงานสามารถดำเนินงานได้อย่างต่อเนื่อง ลดผลกระทบต่อผู้รับบริการ และรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศของทางราชการ

4.2 วัตถุประสงค์ แผนรองรับภาวะฉุกเฉินนี้มีวัตถุประสงค์เพื่อกำหนดแนวทางปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ ให้ระบบสามารถกลับมาใช้งานได้ตามปกติภายในระยะเวลาที่กำหนด ลดความเสียหายที่อาจเกิดขึ้นต่อข้อมูลและระบบงาน และสร้างความมั่นใจว่าการให้บริการประชาชนของหน่วยงานจะไม่เกิดการหยุดชะงัก

4.3 ขอบเขตและสถานการณ์ที่ครอบคลุม แผนครอบคลุมระบบสารสนเทศที่ใช้ในการให้บริการประชาชนและระบบงานภายในของหน่วยงาน โดยพิจารณาความเสี่ยงที่อาจเกิดขึ้นจากเหตุการณ์ต่าง ๆ เช่น ระบบล่ม อุปกรณ์เครือข่ายชำรุด ไฟฟ้าดับ ภัยธรรมชาติ และภัยคุกคามทางไซเบอร์ ซึ่งอาจส่งผลกระทบต่อการให้บริการและความปลอดภัยของข้อมูล

4.4 แนวทางการดำเนินการเมื่อเกิดเหตุฉุกเฉิน เมื่อเกิดเหตุการณ์ผิดปกติ เจ้าหน้าที่ผู้ดูแลระบบจะดำเนินการตรวจสอบและประเมินสถานการณ์เบื้องต้น จากนั้นดำเนินการแก้ไขปัญหาในระดับหน่วยงาน และประสานงานกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาฝีมือแรงงานโดยทันที เพื่อกู้คืน ระบบให้สามารถกลับมาใช้งานได้ตามปกติ ทั้งนี้ หน่วยงานมีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ และจัดเตรียมอุปกรณ์สำรองเพื่อรองรับการกู้คืนระบบในกรณีจำเป็น

4.5 การติดตามและทบทวนแผน หน่วยงานกำหนดให้มีการทบทวนแผนรองรับภาวะฉุกเฉินอย่างน้อยปีละหนึ่งครั้ง เพื่อให้แผนมีความทันสมัยและสอดคล้องกับสภาพแวดล้อมด้านเทคโนโลยีที่เปลี่ยนแปลงอยู่เสมอ พร้อมทั้งรายงานผลการดำเนินงานและเหตุการณ์ที่เกิดขึ้นต่อผู้บริหาร เพื่อปรับปรุงแนวทางการป้องกันและแก้ไขให้มีประสิทธิภาพยิ่งขึ้น (เอกสารแนบ)

กรมพัฒนาฝีมือแรงงานได้กำหนดมาตรฐานในการแก้ปัญหา โดยระบบอิเล็กทรอนิกส์ทั้งในส่วนผู้รับบริการ (e-Service) และในส่วนเจ้าหน้าที่ต้องกลับมาใช้งานตามปกติได้ภายใน 48 ชั่วโมง เพื่อให้เกิดการให้บริการและการบันทึกข้อมูลต่าง ๆ เป็นไปอย่างราบรื่น ต่อเนื่อง และลดผลกระทบต่อผู้ใช้งาน โดยหน่วยงานในฐานะผู้ให้บริการประชาชนในพื้นที่และเป็นผู้ใช้งานระบบโดยตรง จึงได้จัดทำแผนเพื่อรองรับให้สามารถให้บริการได้อย่างต่อเนื่องที่สอดคล้องกับแผนบริหารความต่อเนื่องในภาวะวิกฤต (BCP) ในด้านเทคโนโลยีของหน่วยงาน โดยกำหนดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญ การจัดเตรียมเครื่องคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ และมีการมอบหมายเจ้าหน้าที่ผู้ปฏิบัติงานพร้อมแนวทางในการให้บริการเมื่อเกิดปัญหาจากระบบ ทั้งนี้ ได้กำหนดให้ผู้ดูแลระบบของหน่วยงานจะต้องประสานไปยังส่วนกลางทันทีเมื่อพบปัญหา ภายใน 30 นาที ตามมาตรฐานระยะเวลาที่ส่วนกลางกำหนด

นอกจากนั้นระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณ อยู่ในสภาพพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ และนำอุปกรณ์สำรองข้อมูลที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยผู้ดูแลระบบดำเนินการกู้ระบบคืนกลับมาเพื่อให้สามารถกลับมาให้บริการตามปกติโดยเร็วภายใน 48 ชั่วโมง

1.แผนบริหารความต่อเนื่องในภาวะวิกฤต (BCP) ของหน่วยงาน

1.1 หลักการและเหตุผล สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ได้จัดทำแผนบริหารความต่อเนื่องในภาวะวิกฤต (Business Continuity Plan: BCP) เพื่อเตรียมความพร้อมในการรองรับเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ทั้งในด้านอาคารสถานที่ บุคลากร และโดยเฉพาะด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นระบบสนับสนุนหลักในการให้บริการประชาชน ทั้งนี้ เพื่อให้หน่วยงานสามารถดำเนินภารกิจได้อย่างต่อเนื่อง ลดความเสียหาย และรักษาความเชื่อมั่นของผู้รับบริการ

1.2 วัตถุประสงค์ แผนบริหารความต่อเนื่องในภาวะวิกฤตมีวัตถุประสงค์เพื่อกำหนดแนวทางและขั้นตอนในการรับมือกับสถานการณ์ฉุกเฉินหรือวิกฤตที่อาจทำให้การปฏิบัติงานหยุดชะงัก โดยเฉพาะระบบสารสนเทศและระบบอิเล็กทรอนิกส์ที่ใช้ในการให้บริการประชาชน เพื่อให้สามารถฟื้นฟูการดำเนินงานและกลับมาให้บริการได้ภายในระยะเวลาที่เหมาะสม

1.3 ขอบเขตการดำเนินงานด้านเทคโนโลยีสารสนเทศ แผนครอบคลุมระบบสารสนเทศที่ใช้ในการให้บริการประชาชนและระบบงานภายในของหน่วยงาน โดยกำหนดมาตรการรองรับกรณีระบบขัดข้อง ไฟฟ้าดับ อินเทอร์เน็ตล่ม การโจมตีทางไซเบอร์ หรือเหตุการณ์ภัยธรรมชาติที่อาจส่งผลกระทบต่อ

อุปกรณ์คอมพิวเตอร์และเครือข่าย ทั้งนี้ มีการสำรองข้อมูลสารสนเทศที่สำคัญ การจัดเตรียมอุปกรณ์สำรอง และการกำหนดผู้รับผิดชอบในการกู้คืนระบบอย่างชัดเจน

1.4 แนวทางการดำเนินการเมื่อเกิดภาวะวิกฤต เมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบหรือการให้บริการ หน่วยงานจะดำเนินการตามขั้นตอนที่กำหนดไว้ในแผน ได้แก่ การประเมินสถานการณ์ การแจ้งผู้บริหารและผู้เกี่ยวข้อง การดำเนินการแก้ไขเบื้องต้น และการประสานงานกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาฝีมือแรงงาน เพื่อให้สามารถกู้คืนระบบและกลับมาให้บริการได้อย่างรวดเร็ว ทั้งนี้ จะมีการบันทึกเหตุการณ์และสรุปผลเพื่อใช้ปรับปรุงแผนในอนาคต

1.5 ผลที่คาดว่าจะได้รับ การจัดทำแผนบริหารความต่อเนื่องในภาวะวิกฤตช่วยให้สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี สามารถดำเนินงานได้อย่างต่อเนื่องแม้เกิดเหตุการณ์ไม่คาดคิด ลดผลกระทบต่อการให้บริการประชาชน และสอดคล้องตามเกณฑ์การประเมิน GECC ปี 2569

(เอกสารแนบ)โครงสร้างทีมบริหารความต่อเนื่องในภาวะวิกฤต (BCP Team Structure)

2. Workflow ในการดำเนินการประสานงานกรณีที่เกิดปัญหาในระบบที่ส่วนกลางพัฒนา

สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ได้กำหนดแนวทางการดำเนินการประสานงานกรณีเกิดปัญหาในระบบที่ส่วนกลางพัฒนา โดยเมื่อเจ้าหน้าที่ผู้ดูแลระบบตรวจพบเหตุขัดข้อง จะดำเนินการตรวจสอบและประเมินความรุนแรงของปัญหา พร้อมบันทึกรายละเอียดและแจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาฝีมือแรงงานภายในระยะเวลาที่กำหนด เพื่อให้ส่วนกลางดำเนินการแก้ไขอย่างเร่งด่วน ทั้งนี้ หน่วยงานจะติดตามสถานะการแก้ไขอย่างใกล้ชิด และทดสอบระบบเมื่อแก้ไขแล้วเสร็จ เพื่อให้สามารถกลับมาให้บริการได้อย่างต่อเนื่อง ลดผลกระทบต่อผู้รับบริการ และสอดคล้องตามเกณฑ์ GECC ปี 2569 (เอกสารแนบ)

3. แผนรับมือภัยคุกคามทางไซเบอร์ของหน่วยงาน

3.1 หลักการและวัตถุประสงค์ สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ เพื่อกำหนดมาตรการป้องกัน ตรวจจับ และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เช่น การโจมตีด้วยมัลแวร์ การหลอกลวงทางอีเมล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการรั่วไหลของข้อมูล ทั้งนี้ เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลราชการ และให้การให้บริการประชาชนผ่านระบบอิเล็กทรอนิกส์เป็นไปอย่างต่อเนื่องตามมาตรฐานที่กำหนด (เอกสารแนบ)

3.2 การป้องกันและเฝ้าระวัง (Prevention & Monitoring) หน่วยงานดำเนินการติดตั้งและปรับปรุงระบบป้องกันไวรัส ระบบ Firewall และมาตรการควบคุมการเข้าถึงข้อมูลอย่างสม่ำเสมอ พร้อมกำหนดสิทธิ์การใช้งานตามระดับหน้าที่ของเจ้าหน้าที่ และติดตามสถานะระบบอย่างต่อเนื่อง เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งนี้ เจ้าหน้าที่ผู้ดูแลระบบมีหน้าที่เฝ้าระวังและรายงานเหตุผิดปกติทันทีเมื่อพบความเสี่ยง

3.3 ขั้นตอนการตอบสนองเหตุการณ์ (Incident Response Process) เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เจ้าหน้าที่ผู้ดูแลระบบจะดำเนินการตรวจสอบและยืนยันเหตุการณ์ พร้อมประเมินระดับความรุนแรงของปัญหา หากพบว่าเป็นเหตุการณ์ที่ส่งผลกระทบต่อระบบหลักหรือการให้บริการประชาชน จะต้องแจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาฝีมือแรงงานภายใน 30 นาที ตามมาตรฐาน SLA ที่กำหนด พร้อมรายงานรายละเอียดของเหตุการณ์เพื่อให้ส่วนกลางดำเนินการแก้ไขอย่างเร่งด่วน ในระหว่างนั้น หน่วยงานจะดำเนินการควบคุมสถานการณ์ในเบื้องต้น เช่น การแยกเครื่องที่ได้รับผลกระทบออกจากเครือข่าย การจำกัดสิทธิ์การเข้าถึง หรือการใช้ช่องทางบริการสำรอง เพื่อลดผลกระทบต่อผู้รับบริการ

3.4 การกู้คืนระบบและระยะเวลามาตรฐาน (Recovery & SLA Compliance) ภายหลังการแก้ไขจากส่วนกลางหรือการดำเนินการในระดับหน่วยงาน ระบบจะต้องสามารถกลับมาใช้งานได้ตามปกติภายใน 48 ชั่วโมง ตามมาตรฐานระยะเวลาที่กำหนด เพื่อให้การให้บริการประชาชนและการบันทึกข้อมูลเป็นไปอย่างต่อเนื่อง ทั้งนี้ เจ้าหน้าที่ผู้ดูแลระบบจะทดสอบการทำงานของระบบหลังการกู้คืน ตรวจสอบความสมบูรณ์ของข้อมูล และจัดทำรายงานสรุปเหตุการณ์ รวมถึงแนวทางป้องกันไม่ให้เกิดเหตุซ้ำในอนาคต

3.5 การปรับปรุงและพัฒนาอย่างต่อเนื่อง หลังเหตุการณ์สิ้นสุด หน่วยงานจะนำผลการวิเคราะห์เหตุการณ์มาทบทวนมาตรการควบคุมและแผนรับมือภัยคุกคามทางไซเบอร์ เพื่อปรับปรุงแนวทางปฏิบัติให้มีความรัดกุมยิ่งขึ้น พร้อมทั้งส่งเสริมการอบรมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศแก่เจ้าหน้าที่อย่างต่อเนื่อง เพื่อยกระดับมาตรฐานความปลอดภัยของหน่วยงานให้สอดคล้องตามเกณฑ์ GECC ปี 2569

สรุปการดำเนินงานตามข้อ 4.5

การกำกับดูแลและบริหารจัดการระบบสารสนเทศของหน่วยงาน สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ประจำปีงบประมาณ พ.ศ. 2569

สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ได้ดำเนินการแต่งตั้งเจ้าหน้าที่ผู้ดูแลระบบสารสนเทศและติดตามดูแลระบบ (Monitoring) อย่างเป็นทางการ เพื่อทำหน้าที่เฝ้าระวัง ตรวจสอบ และติดตามสถานะการทำงานของระบบอิเล็กทรอนิกส์ทั้งในส่วนที่ใช้ให้บริการประชาชนและระบบงานภายในอย่างต่อเนื่อง ทั้งนี้เพื่อป้องกันมิให้ระบบเกิดการหยุดชะงัก และสามารถตอบสนองต่อเหตุการณ์ผิดปกติได้อย่างทันท่วงที

เมื่อเกิดเหตุขัดข้องหรือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เจ้าหน้าที่ผู้ดูแลระบบจะดำเนินการตรวจสอบและประเมินความรุนแรงของปัญหา พร้อมแจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาฝีมือแรงงานภายใน 30 นาที ตามมาตรฐานข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ที่กำหนด เพื่อให้ส่วนกลางดำเนินการแก้ไขอย่างเร่งด่วน ทั้งนี้ หน่วยงานจะดำเนินการควบคุมสถานการณ์เบื้องต้นเพื่อลดผลกระทบต่อผู้รับบริการ พร้อมติดตามสถานะการแก้ไขอย่างใกล้ชิดจนกว่าระบบจะกลับมาใช้งานได้ตามปกติ

ภายหลังการแก้ไข ระบบจะต้องสามารถกู้คืนและกลับมาให้บริการได้ภายใน 48 ชั่วโมง ตามมาตรฐานระยะเวลาที่กำหนด โดยเจ้าหน้าที่ผู้ดูแลระบบจะดำเนินการทดสอบการใช้งาน ตรวจสอบความถูกต้องของข้อมูล และจัดทำรายงานสรุปเหตุการณ์ เพื่อใช้เป็นข้อมูลในการปรับปรุงมาตรการป้องกันในอนาคต

นอกจากนี้ หน่วยงานได้จัดทำแผนบริหารความต่อเนื่องในภาวะวิกฤต (Business Continuity Plan: BCP) และแผนรองรับภาวะฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อรองรับเหตุการณ์ที่อาจส่งผลกระทบต่อระบบ เช่น ภัยธรรมชาติ ระบบล่ม หรือการโจมตีทางไซเบอร์ โดยกำหนดแนวทางการสำรองข้อมูล การกู้คืนระบบ การจัดเตรียมอุปกรณ์สำรอง และการกำหนดผู้รับผิดชอบอย่างชัดเจน เพื่อให้การให้บริการประชาชนเป็นไปอย่างต่อเนื่อง

การดำเนินงานดังกล่าวแสดงให้เห็นถึงการบริหารจัดการระบบสารสนเทศของสถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี อย่างเป็นระบบ มีการกำหนด Monitoring อย่างต่อเนื่อง มีมาตรฐาน SLA ในการแจ้งเหตุภายใน 30 นาที มีการกำหนดระยะเวลากู้คืนระบบภายใน 48 ชั่วโมง และมีแผน BCP รองรับสถานการณ์วิกฤตอย่างครบถ้วน ซึ่งสอดคล้องตามเกณฑ์การประเมิน GECC ปี 2569

หมายเหตุ คู่มือการกำกับดูแลและบริหารจัดการระบบสารสนเทศตามเกณฑ์ GECC
สถาบันพัฒนาฝีมือแรงงาน 2 สุพรรณบุรี ประจำปีงบประมาณ พ.ศ. 2569