ภาคผนวก ข.
แผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ของสำนักงานกิจการยุติธรรม พ.ศ. ๒๕๖๕
(IT Contingency Plan)

แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม พ.ศ. ๒๕๖๕
(IT Contingency Plan)

---

๑. หลักการและเหตุผล

ปัจจุบันหน่วยงานราชการมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์การ การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์กรจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

สำนักงานกิจการยุติธรรม ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการแก่เจ้าหน้าที่ในการปฏิบัติงานให้ได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๒. วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม สามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติงาน ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของสำนักงานกิจการยุติธรรม

๓. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของสำนักงานกิจการยุติธรรมมีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์และตรวจสอบความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ของสำนักงานกิจการยุติธรรม พบความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบป้องกันการเข้าถึงข้อมูลล้มเหลว กระแสไฟฟ้าขัดข้อง ระบบคอมพิวเตอร์ถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ระบบจัดเก็บข้อมูลเสียหายเป็นต้น

๒. ความเสี่ยงด้านภัยต่างๆ ที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ ได้แก่ อุทกภัย วาตภัย ดินโคลนถล่ม/อาคารถล่ม แผ่นดินไหว การชุมนุมประท้วงหรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๓. ความเสี่ยงด้านบุคคลหรือผู้ปฏิบัติงาน รวมถึงการบริหารจัดการ เป็นความเสี่ยงที่อาจเกิดขึ้นจากการถูกโจรกรรมทรัพย์สินขององค์กร และความเสี่ยงจากการที่ผู้บริหารสำนักเทคโนโลยีสารสนเทศฯ หรือผู้ปฏิบัติงานรวมถึงผู้ดูแลระบบไม่สามารถปฏิบัติหน้าที่ได้ จนอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศ

ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม

๔. แผนรองรับความเสี่ยงและสถานการณ์ฉุกเฉิน

๔.๑ การป้องกันด้านเทคนิค

๔.๑.๑ ระบบป้องกันการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ล้มเหลว

<u>การป้องกัน/การแก้ไข</u>

(๑) เปิดให้ผู้ใช้สามารถเปลี่ยน Username และ Password ได้ในภายหลัง

(๒) กำหนดให้ใช้วัตถุอื่นเพื่อเข้าสู่ระบบ ได้แก่ บัตร ชิปการ์ด เป็นต้น

(๓) ใช้อุปกรณ์ที่ตรวจสอบลักษณะเฉพาะบุคคลเพื่ออนุญาตให้เข้าสู่ระบบหรือคอมพิวเตอร์

(๔) ใช้การกำหนดรหัสผ่านแบบ ๒ ชั้น ในการเข้าสู่ระบบ ได้แก่ เข้าสู่ระบบด้วยการพิสูจน์ตัวตนด้วย Username/Password และรหัสผ่านแบบครั้งเดียวจากเบอร์โทรศัพท์ที่ลงทะเบียนไว้

<u>หลักการปฏิบัติ</u>

(๑) หลีกเลี่ยงการใช้ข้อมูลส่วนตัว ข้อมูลที่ง่ายต่อการคาดเดาในการตั้งชื่อผู้ใช้งานและรหัสผ่าน

(๒) Update Patch เพื่ออุดช่องโหว่ของระบบอย่างสม่ำเสมอ

(๓) ติดตั้งโปรแกรมป้องกันไวรัส Trend Micro Office Scan และ Update อย่างสม่ำเสมอ

(๔) ล็อกหน้าจอทุกครั้งที่ไม่ใช้งาน และ Logout ระบบทุกครั้งเมื่อใช้งานเสร็จสิ้น

๔.๑.๒ ระบบการเชื่อมต่อเครือข่ายล้มเหลว

การแก้ไข/ป้องกัน

(๑) ติดตั้งไฟร์วอลล์ (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตหรือผู้ไม่ประสงค์ดีเข้าสู่ระบบสารสนเทศและเครือข่ายขององค์กรได้

(๒) ติดตั้งโปรแกรม Proxy Server เพื่อช่วยลดปริมาณข้อมูลที่เดินทางเข้า-ออกเครือข่ายทำให้เครือข่ายภายในองค์กรมีประสิทธิภาพมากขึ้น และกลั่นกรองข้อมูลเว็บไซต์ต่างๆ จากภายนอกให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร

(๓) มีระบบตรวจสอบปริมาณข้อมูลการใช้งานเครือข่ายอินเทอร์เน็ตขององค์กร

(๔) Update Patch เพื่ออุดช่องโหว่ของระบบและซอฟต์แวร์อย่างสม่ำเสมอ

(๕) ติดตั้งซอฟต์แวร์ติดตามการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย

หลักการปฏิบัติ

(๑) ผู้ดูแลระบบต้องเปิดใช้งานไฟร์วอลล์ (Firewall) และซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ตลอดเวลา

(๒) ผู้ดูแลระบบจะต้องกำหนดค่าของ Proxy Server เพื่อกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบเครือข่ายขององค์กร

(๓) ผู้ดูแลระบบจะต้องทำการตรวจสอบปริมาณข้อมูลบนระบบเครือข่ายขององค์กรอย่างสม่ำเสมอ

(๔) ผู้ดูแลระบบจะต้องติดตาม (Monitoring) และตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายให้สามารถใช้งานได้เป็นปกติ

(๕) ผู้ดูแลระบบจะต้องรีบรายงานให้ผู้อำนวยการศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติทราบ และประสานงานผู้ที่เกี่ยวข้องให้ดำเนินการแก้ไขโดยด่วนที่สุด ทั้งนี้ หากมีเหตุจำเป็นที่จะต้องใช้เวลาเพื่อแก้ไขนานเกิน ๑ วัน ให้ออกประกาศแจ้งผู้ใช้งานทราบ

๔.๑.๓ อุปกรณ์จัดเก็บข้อมูลเสียหาย

การแก้ไข/ป้องกัน

(๑) ติดตั้งระบบสำรองข้อมูลสำหรับเครื่องคอมพิวเตอร์แม่ข่าย

(๒) สำรองข้อมูลไว้ใน Hard drive

(๓) สำหรับข้อมูลที่สำคัญมาก สำรองข้อมูลโดยการพิมพ์ออกทางกระดาษเก็บไว้

(๔) ทดสอบความถูกต้องของระบบสำรองอยู่เสมอ

หลักการปฏิบัติ

(๑) กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย ให้ผู้ดูแลระบบตรวจสอบสาเหตุความเสียหายเบื้องต้น พร้อมรายงานให้ผู้อำนวยการศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติทราบ หากพบว่าแนวทางที่จะทำการกู้คืนข้อมูลในอุปกรณ์นั้นกลับมาได้ให้ดำเนินการโดยด่วน และหากไม่สามารถกู้คืนข้อมูลกลับมาได้ให้นำข้อมูลที่สำรองไว้มาใช้แทน

(๒) กรณีของผู้ใช้งาน เมื่อเกิดกรณีอุปกรณ์จัดเก็บข้อมูลเสียหายให้รายงานผู้บังคับบัญชาของตนทราบ จากนั้นให้แจ้งผู้ดูแลระบบหรือเจ้าหน้าที่ด้าน

สารสนเทศให้ตรวจสอบสาเหตุความเสียหาย หากสามรถกู้คืนข้อมูลกลับมาได้ให้ดำเนินการโดยด่วน หากไม่สามารถกู้คืนข้อมูลกลับมาได้ให้นำข้อมูลที่สำรองไว้มาใช้แทน

(๓) ให้ส่งอุปกรณ์จัดเก็บข้อมูลที่เสียหายดังกล่าวซ่อมตามระเบียบของทางราชการ

๔.๑.๔ กระแสไฟฟ้าดับ/ขัดข้อง

การแก้ไข/ป้องกัน

(๑) ติดตั้งระบบสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) เพื่อป้องกันการเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย

(๒) ติดตั้งระบบสำรองไฟฟ้าสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล (PC)

หลักการปฏิบัติ

(๑) เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดเวลาที่เปิดใช้ใช้งานเครื่องคอมพิวเตอร์ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

(๒) เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่และปิดอย่างปลอดภัย (Shut down) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในองค์กรด้วย

(๓) ผู้ดูแลระบบติดต่อการไฟฟ้าในพื้นที่เพื่อตรวจสอบปัญหาและติดตามการแก้ไข ทั้งนี้ เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติสามารถให้กำลังไฟฟ้าสำรองได้ในเวลา ๔๐ – ๖๐ นาที หากไฟฟ้าดับเป็นเวลา ๓๐ นาที ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและให้แจ้งผู้ใช้งานทราบ

๔.๒ การป้องกันภัยที่เกิดจากธรรมชาติ

๔.๒.๑ ไฟไหม้

การป้องกัน/แก้ไข

(๑) ติดตั้งระบบดับเพลิงอัตโนมัติ Pyrogen ในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย

(๒) ติดตั้งระบบแจ้งเตือนอัตโนมัติ (SMS Alarm) หากมีควันหรือเกิดไฟไหม้ในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย โดยระบบจะทำการแจ้งเตือนเป็นข้อความไปยังโทรศัพท์มือถือของผู้ดูแลระบบทันที

(๓) ติดตั้งถังก๊าซดับเพลิงในบริเวณพื้นที่ห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายและทั่วพื้นที่ใช้งานระบบสารสนเทศ

(๔) โทรศัพท์แจ้งฝ่ายดูแลอาคารทันทีที่หมายเลข ๐๘ ๑๘๕๙ ๓๕๐๐ หรือ ๐๘ ๑๗๕๕ ๗๔๒๒ และโทรศัพท์แจ้งสถานีดับเพลิงใกล้เคียงทันที หมายเลข ๐ ๒๕๒๑ ๐๓๙๗ หรือสายด่วนศูนย์ดับเพลิงกรุงเทพมหานคร หมายเลข ๑๙๙ เพื่อให้มาระงับเหตุ

(๕) กำหนดให้ผู้ดูแลระบบและเจ้าหน้าที่สารสนเทศเข้าร่วมอบรมวิธีการใช้งานเครื่องดับเพลิงและการระงับเหตุไฟไหม้ รวมถึงการหนีไฟ อย่างน้อยปีละ ๒ ครั้ง

(๖) ติดตั้งฉนวนกันความร้อนและฉนวนกันความชื้นภายในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย

(๗) มีเครื่องรักษาอุณหภูมิห้องปฏิบัติการเครื่องคอมพิวเตอร์ จำนวน ๒ เครื่อง และเปิดให้ทำงานตลอด ๒๔ ชั่วโมง

หลักการปฏิบัติ

(๑) ผู้ดูแลระบบหมั่นตรวจสอบระบบท่อน้ำเลี้ยงระบบรักษาอุณหภูมิ และระบบก๊าซ Pyrogen อยู่เสมอ

(๒) ผู้ดูแลระบบต้องตรวจสอบถังดับเพลิงที่ติดตั้งตามจุดต่างๆ ตามรอบระยะเวลาที่กำหนด

(๓) ในกรณีที่เกิดเหตุไฟไหม้ขณะปฏิบัติงาน แต่ไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบนำอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ประกอบด้วย ๑) เครื่องแม่ข่ายสำหรับจัดเก็บข้อมูล (Storage) Dell SC4020 ที่อยู่ใน Rack 1 โดยการถอดสายไฟที่ด้านหลังเครื่องและปลดล็อกชั้นวางจำนวน ๒ ตัว แล้วดึงออกมาทั้งเครื่อง จากนั้นรีบนำออกไปในพื้นที่ที่ปลอดภัยโดยเร็ว และ ๒) เครื่องแม่ข่ายสำหรับสำรองข้อมูล (Backup) Dell PowerEdge R520 ที่อยู่ใน Rack 1 โดยการถอดสายไฟที่ด้านหลังเครื่อง และดึงออกมาทั้งเครื่อง รีบนำออกไปในพื้นที่ที่ปลอดภัยโดยเร็ว

(๔) กรณีเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน หรือกรณีมาระงับเหตุไม่ทัน ปรากฏผลว่าอุปกรณ์ต่างๆ ชำรุดเสียหาย ให้รีบดำเนินการตรวจสอบ หากกู้คืนข้อมูลกลับมาได้ให้ดำเนินการโดยด่วน หรือส่งซ่อม แล้วแต่กรณี

๔.๒.๒ น้ำรั่วซึมในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย

การป้องกัน/แก้ไข

(๑) ห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงานกิจการยุติธรรม ได้มีการติดตั้งระบบอัตโนมัติตรวจจับการรั่วซึมของน้ำ

(๒) หากพบมีน้ำรั่วซึมในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย ระบบแจ้งเตือนอัตโนมัติ (SMS Alarm) จะทำการแจ้งเตือนเป็นข้อความไปยังโทรศัพท์มือถือของผู้ดูแลระบบทันที เพื่อให้ทราบและดำเนินการตรวจสอบ และหาสาเหตุที่เกิดปัญหา

หลักการปฏิบัติ

(๑) ผู้ดูแลระบบต้องตรวจสอบระบบท่อน้ำเลี้ยงระบบรักษาอุณหภูมิภายในห้องปฏิบัติการเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

(๒) ตรวจสอบและทดสอบระบบแจ้งเตือนอัตโนมัติ (SMS Alarm) อย่างน้อยปีละ ๒ ครั้ง

(๓) กรณีมีเหตุน้ำรั่วซึมซึ่งไม่สามารถควบคุมหรือแก้ไขได้ ให้ผู้ดูแลระบบโทรศัพท์แจ้งฝ่ายดูแลอาคารทันทีที่หมายเลขโทรศัพท์ ๐๘ ๑๘๕๙ ๓๕๐๐ และ ๐๘ ๑๗๕๕ ๗๔๒๒

(๔) หากพบว่ายังไม่สามารถแก้ไขปัญหาได้ ซึ่งอาจส่งผลกระทบกับอุปกรณ์สารสนเทศให้ผู้ดูแลระบบรายงานผู้อำนวยการศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติฯ ทราบ

(๕) ดำเนินการปิดระบบเทคโนโลยีสารสนเทศ และเคลื่อนย้ายอุปกรณ์สารสนเทศที่อาจจะเกิดความเสียหายออกนอกพื้นที่ และแจ้งให้ผู้ใช้งานทราบ

(๖) หากแก้ไขน้ำที่รั่วซึมเสร็จสิ้นแล้ว ให้เคลื่อนย้ายอุปกรณ์กลับเข้าที่เดิม และทำการเปิดระบบเทคโนโลยีสารสนเทศให้สามารถใช้งานได้ตามปกติ พร้อมกับแจ้งให้ผู้ใช้งานทราบ

๔.๒.๓ น้ำท่วม

<u>การป้องกัน/แก้ไข</u>

(๑) เมื่อเกิดภาวะเสี่ยงที่จะเกิดน้ำท่วมหรืออุทกภัยในท้องที่ตั้งสำนักเทคโนโลยีสารสนเทศ ให้ผู้ดูแลระบบประสานงานกับเจ้าหน้าที่ฝ่ายดูแลอาคารเพื่อประเมินและวางแผนรับมือกับสถานการณ์

(๒) ผู้ดูแลระบบต้องสำรองข้อมูลทั้งหมดเก็บไว้ในสื่อบันทึกข้อมูล พร้อมกับประสานงานกับฝ่ายดูแลอาคารไว้เป็นระยะๆ เพื่อทราบถึงเหตุการณ์ และประเมินว่าควรจะดำเนินการปิดระบบหรือไม่ แต่ต้องสำรองข้อมูลไว้ก่อนด้วย

(๓) ให้ผู้ดูแลระบบติดตามสถานการณ์น้ำท่วมในท้องที่ตั้งสำนักเทคโนโลยีสารสนเทศอย่างต่อเนื่อง และรายงานให้ผู้อำนวยการศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติ ทราบเป็นระยะๆ เพื่อประเมินสถานการณ์และพิจารณาสั่งการ

(๔) ผู้ดูแลระบบและเจ้าหน้าที่สารสนเทศ เคลื่อนย้ายสื่อบันทึกข้อมูล และอุปกรณ์ขึ้นไปบนชั้นสูงสุดของอาคาร และมีกุญแจล็อกแน่นหนา พร้อมทั้งประสานกับทางฝ่ายดูแลอาคารเพื่อปิดการจ่ายกระแสไฟฟ้า

(๕) เมื่อสถานการณ์เป็นปกติ ให้ตรวจสอบความเสียหายของอุปกรณ์ หากมีอุปกรณ์ชำรุดหรือเสียหายให้ทำการซ่อมแซมหรือเปลี่ยนใหม่โดยเร็ว และทำการติดตั้งระบบ/เปิดระบบเทคโนโลยีสารสนเทศฯ เพื่อให้บริการตามปกติ พร้อมทั้งแจ้งให้ผู้ใช้งานทราบ

<u>หลักการปฏิบัติ</u>

(๑) ผู้ดูแลระบบและเจ้าหน้าที่สารสนเทศ ร่วมกันประเมิน ติดตาม และแก้ไขปัญหาเมื่อเกิดภาวะเสี่ยงน้ำท่วมหรืออุทกภัย

(๒) จัดฝึกอบรมหรือเข้าร่วมการฝึกอบรมเกี่ยวกับแผนรับมือสถานการณ์น้ำท่วม

๔.๒.๔ แผ่นดินไหว

<u>หลักการปฏิบัติ/แก้ไข</u>

(๑) ให้ผู้ปฏิบัติงานทุกคนรีบออกภายนอกตัวอาคาร

(๒) ผู้ดูแลระบบนำข้อมูลสำรองที่สำรองเตรียมไว้ในสื่อไปด้วยหากสามารถทำได้

(๓) เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

๔.๒.๕ เกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง ได้แก่ การก่อการร้าย การชุมนุมประท้วง

หลักการปฏิบัติ/แก้ไข

(๑) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ให้ผู้ดูแลระบบ Remote Access เพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้อำนวยการสำนักเทคโนโลยีฯ ให้ทราบ

(๒) หลังเหตุการณ์ความไม่สงบผ่านไปแล้ว ให้ผู้ดูแลระบบเข้าตรวจสอบรายการสินทรัพย์ ความชำรุดเสียหาย ซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว โดยหากพบความชำรุดเสียหาย ให้ทำการแจ้งผู้อำนวยการสำนักเทคโนโลยีฯ เพื่อดำเนินการบำรุงรักษา ซ่อมแซม ให้ใช้งานได้ตามปกติ

๔.๓ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล และการบริหารจัดการ

๔.๓.๑ โจรกรรม

หลักการปฏิบัติ/แก้ไข

(๑) ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

(๒) สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

(๓) ผู้ดูแลระบบ รีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม เพื่อให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆ ได้โดยเร็ว

๔.๓.๒ ผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

หลักการปฏิบัติ/แก้ไข

(๑) แจ้งให้ผู้บังคับบัญชาทราบล่วงหน้า หรือหากไม่สามารถแจ้งล่วงหน้าได้ ให้ทำการติดต่อโดยเร็วที่สุด

(๒) ปฏิบัติตามคู่มือการดำเนินงานที่จัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

๔.๓.๓ ผู้อำนวยการสำนักเทคโนโลยีฯ ไม่สามารถมาปฏิบัติงานได้

หลักการปฏิบัติ/แก้ไข

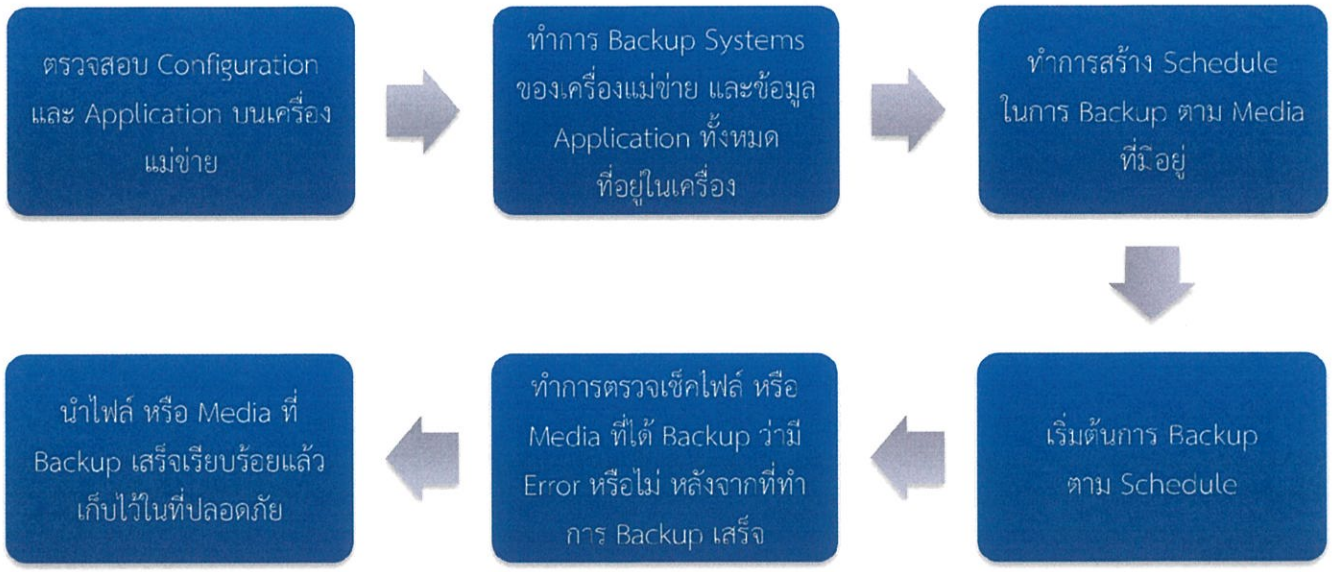
(๑) หากมีเหตุจำเป็นให้แจ้งหรือประสานงานกับผู้ที่ได้รับมอบอำนาจให้ดำเนินการแทน

(๒) หากไม่มีการมอบอำนาจให้ดำเนินการแทน ให้แจ้งหรือประสานงานกับผู้บังคับบัญชาตามลำดับ

๕. ขั้นตอนการปฏิบัติในการสำรองข้อมูล และการกู้คืนข้อมูลที่สำรองไว้

ผู้ดูแลระบบต้องทำการสำรองข้อมูลไว้ตามที่กำหนดในนโยบายและแนวปฏิบัติเพื่อใช้ในกรณีที่ข้อมูลเกิดการสูญหาย หรือระบบที่ใช้งานอยู่เกิดปัญหาขึ้น รวมถึงการกู้คืนข้อมูลที่ได้ทำการสำรองไว้ เพื่อให้ใช้งานข้อมูลได้ดังเดิม ซึ่งการสำรองข้อมูลของสำนักงานกิจการยุติธรรม แบ่งได้เป็น Physical Hardware Virtual Machine

๕.๑ สำรองข้อมูลสำหรับระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของระบบโครงสร้างพื้นฐาน ในกรณีที่เป็น Physical Hardware



๕.๒ สำรองข้อมูลสำหรับระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของระบบโครงสร้างพื้นฐาน ในกรณีที่เป็น Virtual Machine

๕.๓ สรุปตารางการสำรองข้อมูลระบบ (Backup System) ของสำนักงานกิจการยุติธรรม

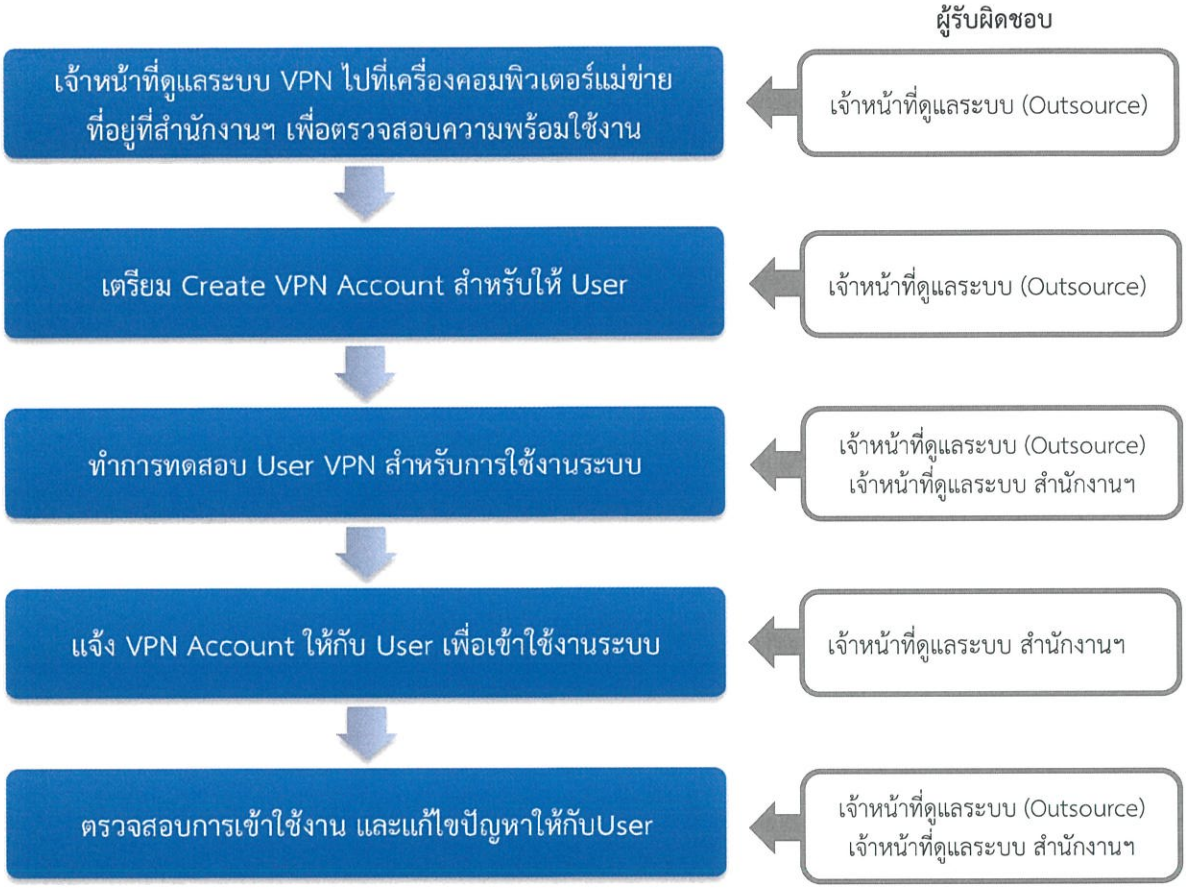
Job No.	Jobs Name	ระบบงาน	Server Name	Selection	Destination	Schedule	Schedule plan	Schedule time	No. of Recovery Point
๑	VMWare-Backup-vmtools	Network Management	OJA-AMP	VM (All Drive)	Disk	Incremental	Daily	11.30pm	๒๑
	(ฐานข้อมูล Data รวมของทุกระบบ)	Network Management	OJA-Clearpass	VM (All Drive)	Disk	Incremental	Weekly (sat)	11.30pm	๑๕
		Network Management	OMNM6	VM (All Drive)	Disk	Incremental	monthly (Day 3)	11.30pm	๑๕
		VM Managmenet	vcenter	VM (All Drive)	Disk				
		File Server	fileserver	VM (All Drive)	Disk				
		External Web Server	webfront1	VM (All Drive)	Disk				
		External Web Server	webfront2	VM (All Drive)	Disk				
		Print Server	printerserver	VM (All Drive)	Disk				
		DNS Server (External)	ext-dns-1	VM (All Drive)	Disk				
		DNS Server (External)	ext-dns-2	VM (All Drive)	Disk				
		Application Server	jrdapp	VM (All Drive)	Disk				
		Application Server	appserver	VM (All Drive)	Disk				
		Application Server	edocserver	VM (All Drive)	Disk				
		Application Server	esarabanserver	VM (All Drive)	Disk				
		Application Server	barcode-server	VM (All Drive)	Disk				
		Mail Server	lyncserver	VM (All Drive)	Disk				
		Antivirus Server	antivirus	VM (All Drive)	Disk				
		Application Server	dpisserver	VM (All Drive)	Disk				

Job No.	Jobs Name	ระบบงาน	Server Name	Selection	Destination	Schedule	Schedule plan	Schedule time	No. of Recovery Point
๒	VMWare-Backup-No-vmtools	Access Control	biostar (Access Control)	VM (All Drive)	Disk	Incremental	Daily	12.00am	๒๑
	(ระบบสแกนลายนิ้วมือ บันทึกเวลาเข้า-ออก)					Incremental	Weekly (sat)	12.15am	๑๕
๓	OJA-Main-Intranet-Windows- Agent-All	Domain Controller	pdcserver	Physical (All Drive)	Disk	Incremental	Daily	10.00pm	๒๑
	(Domain ของสำนักงานฯ)					Incremental	Weekly (sun)	10.00pm	๑๕
						Incremental	monthly (Day 2)	10.00pm	๑๕
๔	Exchange2010 (ระบบ E-mail สำนักงานฯ)	Mail Server	Exchange-1	VM (All Drive)	Disk	Incremental	Custom Daily snapshot (2Hr)	8.00am - 600pm Mon-Fri	๒๐๐
		Mail Server	Exchange-2	VM (All Drive)	Disk	Incremental	Daily	12.00am	๒๐
						Incremental	Weekly (fri)	11.00pm	๒๕
						Incremental	monthly (Day 1)	11.00pm	๒๐
๕	Sharepoint	Intranet Web Server	sharepoint-1	VM (All Drive)	Disk	Incremental	Daily	10.00pm	๒๐
	(ระบบอินทราเน็ต)	Intranet Web Server	sharepoint-2	VM (All Drive)	Disk	Incremental	Weekly (fri)	10.00pm	๒๕
						Incremental	monthly (Day 1)	10.00pm	๒๐
๖	SQL-Server	Database Server	SQL-Server-1	VM (All Drive)	Disk	Incremental	Daily	10.15pm	๒๐
	(ฐานข้อมูลของแต่ละระบบ)	Database Server	SQL-Server-2	VM (All Drive)	Disk	Incremental	Weekly (fri)	10.15pm	๒๕
						Incremental	monthly (Day 1)	10.15pm	๒๐

๖. ขั้นตอนการกู้คืนระบบ

๖.๑ กรณีที่เหตุการณ์ฉุกเฉินเป็นปกติแล้ว User สามารถกลับเข้ามาทำงานที่สำนักงาน และเจ้าหน้าที่ดูแลระบบสามารถเข้ามาดำเนินการที่ห้อง Server ได้

๖.๒ กรณีที่ไม่สามารถเข้ามาทำงานที่สำนักงานได้ แต่ระบบยังทำงานได้อยู่



๗. การกำหนดผู้รับผิดชอบ และช่องทางการติดต่อผู้ดูแลระบบเมื่อเกิดเหตุฉุกเฉิน

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม ประกอบด้วย

๗.๑ ด้านการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ ผู้ดูแลระบบและเจ้าหน้าที่สารสนเทศเมื่อเกิดสถานการณ์ฉุกเฉินข้างต้น ได้แก่

๗.๑.๑ นายชัยวัฒน์ ร่างเล็ก ผู้อำนวยการศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติ

ปฏิบัติหน้าที่ : ปฏิบัติงานในฐานะผู้อำนวยการศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติ ในการวางแผนบริหารจัดการ จัดระบบงาน อำนวยการ สั่งราชการ มอบหมาย กำกับ แนะนำ ตรวจสอบ ประเมินผลงาน ตัดสินใจ และแก้ปัญหางานในหน้าที่ รวมถึงด้านงานการพัฒนาระบบเทคโนโลยีระบบสารสนเทศและการสื่อสาร งานการวิเคราะห์ข้อมูล เพื่อให้การดำเนินงานของกลุ่มเทคโนโลยีสารสนเทศและการสื่อสารกระบวนการยุติธรรมมีประสิทธิภาพและสามารถบรรลุผลสำเร็จตามแผนยุทธศาสตร์ และภารกิจขององค์กร

ติดต่อ : โทรศัพท์ : ๐ ๒๑๔๑ ๓๖๖๖
โทรศัพท์มือถือ : ๐๙ ๒๕๑๕ ๙๑๕๕
โทรสาร : ๐ ๒๑๔๓ ๘๓๓๔
E-Mail : r_chaiwat@oja.go.th

๗.๒ ด้านการสำรวจตรวจสอบรายการทรัพย์สิน และตรวจสอบการดำเนินงานของดูแลระบบเจ้าหน้าที่ด้านสารสารสนเทศ และ Outsource ของสำนักงานกิจการยุติธรรม ได้แก่

๗.๒.๑ นางสาทิมา ทองศรีจันทร์ นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

ปฏิบัติหน้าที่ : หัวหน้ากลุ่มเทคโนโลยีสารสนเทศและการสื่อสารกระบวนการยุติธรรม หัวหน้าผู้ดูแลระบบ บริหารจัดการ กำกับดูแลการปฏิบัติงานของผู้ดูแลระบบ เจ้าหน้าที่สารสนเทศ และ Outsource รวมถึงคอยให้ข้อเสนอแนะ คำปรึกษา และตัดสินใจในการแก้ปัญหาให้แก่ผู้ดูแลระบบและเจ้าหน้าที่สารสนเทศ ตลอดจนกำกับการปฏิบัติงานให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ติดต่อ : โทรศัพท์ : ๐ ๒๑๔๑ ๓๗๒๒
โทรศัพท์มือถือ : ๐๘ ๑๘๓๒ ๙๑๙๐
โทรสาร : ๐ ๒๑๔๓ ๘๓๕๔
E-Mail : t_satima@oja.go.th

๗.๓ ด้านการปฏิบัติงาน การดูแลระบบ ดูแลห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายและประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๗.๓.๑ นางสาวน้ำทิพย์ ฉิมสุด นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ปฏิบัติหน้าที่ : ผู้ดูแลระบบ ปฏิบัติหน้าที่ในฐานะผู้ดูแลระบบสารสนเทศขององค์กร สนับสนุนการปฏิบัติงานของหัวหน้าผู้ดูแลระบบให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ กำกับดูแลการสำรองข้อมูล ดำเนินการตามแผนเตรียมความพร้อมฉุกเฉิน ระบบการตรวจจับการบุกรุก การเข้าถึงข้อมูลสารสนเทศและคอมพิวเตอร์แม่ข่าย รวมถึงกำหนดให้มีการให้ความรู้ความเข้าใจและการจัดการฝึกอบรมด้านสารสนเทศให้กับเจ้าหน้าที่สารสนเทศและผู้ใช้งาน ตลอดจนการรายงานสถานการณ์ต่างๆ

ให้ผู้อำนวยการศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติ และหัวหน้ากลุ่มเทคโนโลยีสารสนเทศและการสื่อสารกระบวนการยุติธรรม หัวหน้าผู้ดูแลระบบทราบ

ติดต่อ : โทรศัพท์ : ๐ ๒๑๔๑ ๓๗๓๔
โทรศัพท์มือถือ : ๐๙ ๕๕๘๔ ๒๙๙๒
โทรสาร : ๐ ๒๑๔๓ ๘๓๕๔
E-Mail : c_namthip@oja.go.th

๗.๓.๒ นายคทาวุธ อินทรทัต นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ปฏิบัติหน้าที่ : ผู้ดูแลระบบ ปฏิบัติหน้าที่ในฐานะผู้ดูแลระบบสารสนเทศขององค์กรอีกคนหนึ่ง ซึ่งสามารถปฏิบัติงานทดแทน เมื่อผู้ดูแลระบบคนที่หนึ่งไม่อยู่ หรือช่วยกันปฏิบัติงานดูแลระบบ รวมถึงกำกับ ติดตาม ประเมินความเสี่ยงด้านสารสนเทศ การจัดการด้านความปลอดภัยสารสนเทศ การทบทวนนโยบายและสารสนเทศให้เป็นปัจจุบัน ทันสมัยอยู่เสมอ กำกับดูแลการสำรองข้อมูลและการกู้คืนข้อมูลสารสนเทศ การจัดซื้อและส่งซ่อมอุปกรณ์ การจัดการเว็บไซต์ และระบบสารสนเทศภายใน การจัดการทางด้านกายภาพ รับเรื่องร้องเรียนและแก้ไขปัญหาการร้องเรียน ดูแลฐานข้อมูลและข้อมูลขององค์กร รวมถึงฐานข้อมูลที่องค์กรให้บริการ ควบคุมการเข้าออกของบุคคลภายนอก การให้ความรู้แก่ผู้ใช้งานในลักษณะเกร็ดความรู้ด้านเทคโนโลยีสารสนเทศ กำกับดูแล Outsource ในการพัฒนาระบบ และสนับสนุนการปฏิบัติงานของผู้ดูแลระบบและรายงานให้ผู้ดูแลระบบทราบ

ติดต่อ : โทรศัพท์ : ๐ ๒๑๔๑ ๓๖๙๐
โทรศัพท์มือถือ : ๐๘ ๑๙๖๒ ๙๒๑๐
โทรสาร : ๐ ๒๑๔๓ ๘๓๕๔
E-Mail : i_khathawut@oja.go.th

๗.๔ ด้านการปฏิบัติงานในฐานะผู้รับจ้างบำรุงรักษาระบบเทคโนโลยีสารสนเทศจากภายนอก (Outsource) ซึ่งมาปฏิบัติงานประจำที่สำนักงานกิจการยุติธรรม

๗.๔.๑ นายบุญคริษฐ์ ทรัพย์ประดิษฐ์ เจ้าหน้าที่ Outsource

ปฏิบัติหน้าที่ : ปฏิบัติงานในฐานะเจ้าหน้าที่สารสนเทศ ในการติดตั้ง ปรับปรุง อัพเดท และดูแลการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายของผู้ใช้งาน รับเรื่องร้องเรียนและปัญหาการใช้งานระบบและรายงานผู้ดูแลระบบทราบ

ติดต่อ : โทรศัพท์ : ๐ ๒๑๔๑ ๓๗๕๙
โทรศัพท์มือถือ : ๐๘ ๗๓๒๗ ๓๓๓๓
โทรสาร : ๐ ๒๑๔๓ ๘๓๕๔
E-Mail : s_boonkarit@oja.go.th

๗.๔.๒ นายศุภณัฐ สงวนสัตย์ เจ้าหน้าที่ Outsource

ปฏิบัติหน้าที่ : ปฏิบัติงานในฐานะผู้รับจ้างพัฒนาระบบจากภายนอก (Outsource) ในการบำรุงรักษาอุปกรณ์ด้านสารสนเทศ การสำรองข้อมูลและกู้คืนข้อมูล การดูและระบบสนับสนุนการทำงานของสารสนเทศ รวมถึงการแก้ไขปัญหาด้านสารสนเทศขององค์กร ภายใต้การกำกับดูแลของผู้ดูแลระบบและหัวหน้าผู้ดูแลระบบ

ติดต่อ : โทรศัพท์ : ๐ ๒๙๓๐ ๒๓๙๙
โทรศัพท์มือถือ : ๐๘ ๙๕๑๘ ๑๗๑๗
โทรสาร : ๐ ๒๖๒๗ ๑๒๖๖
E-Mail : suppanut@pragma.co.th

แผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency plan) ของสำนักงานกิจการยุติธรรมฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการที่กำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานกิจการยุติธรรม เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

พันตำรวจโท
(พงษ์ธร ธัญญสิริ)
ผู้อำนวยการสำนักงานกิจการยุติธรรม