แผนการบริหารความพร้อมกรณีเกิดภัยคุกคามทางไซเบอร์ ระบบเทคโนโลยีสารสนเทศ

ศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี

แผนการบริหารความพร้อม (Business Continuity Planning)
กรณีเกิดภัยคุกคามทางไซเบอร์ระบบเทคโนโลยีสารสนเทศ
เรือนจำจังหวัดสุพรรณบุรี

ชื่อเหตุการณ์ :	เหตุการณ์หมายเลขที่ :	วัน เวลา ที่เริ่มเกิดเหตุ :
แผนรองรับฉุกเฉินกรณีเหตุคุกคามทางไซเบอร์ ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)		วันที่ :

สรุปสถานการณ์

ศูนย์บริการประชาชนเรือนจำจังหวัดสุพรรณบุรี ได้นำระบบเทคโนโลยีสารสนเทศมาใช้ในการให้บริการและการปฏิบัติงานของเจ้าหน้าที่ เช่น การให้บริการเยี่ยมญาติผ่านระบบออนไลน์ การจำหน่ายสินค้าร้านสงเคราะห์ การรับฝากเงิน การเยี่ยมญาติ การลงทะเบียนข้อมูลการเยี่ยมญาติ การจัดทำสื่อประชาสัมพันธ์ผ่านทาง facebook และกลุ่มไลน์ การจำหน่ายสินค้าผ่านไลน์ การนำเทคโนโลยีสารสนเทศมาใช้ในการบริการต่างๆ ดังกล่าว เน้นการเพิ่มประสิทธิภาพการให้บริการ และเพิ่มการอำนวยความสะดวกแก่ผู้รับบริการ สามารถให้บริการได้โดยไม่ต้องเสียเวลาและค่าใช้จ่ายในการเดินทางมารับบริการที่เรือนจำจังหวัดสุพรรณบุรี

ทั้งนี้ การนำเทคโนโลยีสารสนเทศมาใช้ในงานบริการดังกล่าว มีความเสี่ยงสูงที่จะถูกภัยคุกคามทางไซเบอร์ระบบเทคโนโลยีสารสนเทศ เช่น ภัยประเภทมิจฉาชีพบนโซเชียลมีเดีย ภัยประเภท Email หลอกลวง Phishing และภัยประเภทการขโมยข้อมูลส่วนบุคคล (Data Theft) เป็นต้น ซึ่งหากภัยคุกคามทางไซเบอร์ระบบเทคโนโลยีสารสนเทศดังกล่าวเกิดขึ้นกับระบบการใช้บริการของศูนย์บริการประชาชน จะส่งผลให้การให้บริการต้องหยุดชะงักลง ไม่สามารถให้บริการแก่ประชาชนได้ทำความต้องการของประชาชน

ดังนั้น ศูนย์บริการประชาชนเรือนจำจังหวัดสุพรรณบุรี จึงจัดทำแผนการบริหารความพร้อม (Business Continuity Planning) กรณีเกิดภัยคุกคามทางไซเบอร์ระบบเทคโนโลยีสารสนเทศ เรือนจำจังหวัดสุพรรณบุรี ขึ้น โดยมีสรุปสถานการณ์ ดังนี้

วันพุธที่ ๑ กุมภาพันธ์ ๒๕๖๖ ศูนย์บริการประชาชนได้เปิดให้บริการประชาชนตามปกติโดยมีผู้มารับบริการเป็นจำนวนมาก จากนั้นเวลา ๑๐.๐๐ น. ในระหว่างที่มีการให้บริการประชาชนอยู่นั้น ปรากฏว่าระบบการลงทะเบียนจองเยี่ยมผู้ต้องขังออนไลน์ ไม่สามารถให้บริการได้ เจ้าหน้าที่งานการลงทะเบียนจองเยี่ยมระบบออนไลน์ จึงรายงานให้หัวหน้าฝ่ายสวัสดิการผู้ต้องขังทราบ เพื่อดำเนินการตามแผนการบริหารความพร้อม (Business Continuity Planning) ตามขอบเขตการดำเนินงานที่กำหนดไว้ ดังนี้

๑. ขั้นตอนและแนวทางการป้องกันเบื้องต้น
๒. การเตรียมความพร้อม
๓. รายงานการแก้ไขปัญหา/แผนผังกระบวนการแก้ไขปัญหา
๔. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์คุกคามทางไซเบอร์
๕. การติดตามผลและรายงานผล

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมรับมือสถานการณ์คุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี

๒. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี

๓. เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๔. เพื่อให้ศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี สามารถให้บริการประชาชนได้อย่างต่อเนื่องในสถานการณ์เกิดภัยคุมคามทางไซเบอร์

ขอบเขตการดำเนินงาน

แผนการบริหารความพร้อม (Business Continuity Planning) กรณีเกิดภัยคุกคามทางไซเบอร์ระบบเทคโนโลยีสารสนเทศ ที่ศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรีจัดทำขึ้นสำหรับเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของเรือนจำจังหวัดสุพรรณบุรี ประกอบด้วย

๑. ขั้นตอนและแนวทางการป้องกันเบื้องต้น

๒. การเตรียมความพร้อม

๓. กระบวนการแก้ไขปัญหา / แผนผังกระบวนการแก้ไขปัญหา

๔. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์คุกคามทางไซเบอร์

๕. การติดตามและรายงานผล

๑.ขั้นตอนและแนวทางการป้องกันเบื้องต้น

๑.๑ กำหนดขั้นตอนการดำเนินงาน

ศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี จัดเตรียมขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์คุกคามทางไซเบอร์ หรือผิดปกติในเรือนจำฯ โดยกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่างๆที่เกิดขึ้น รวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุก เพื่อให้สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนระบบ

๑.๒ การติดต่อประสานงาน

มีการจัดทำข้อมูลรายชื่อหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัย กรณีที่มีความจำเป็นฉุกเฉิน เช่น บริษัททริปเปิลที บรอดแบนด์ จำกัด (มหาชน) 3BB , บริษัททีโอที จำกัด (มหาชน) TOT , การไฟฟ้า , สถานีดับเพลิง , สถานีตำรวจ , ผู้ดูแลระบบส่วนกลางกรมราชทัณฑ์ , ผู้ดูแลระบบของเอกชนที่เป็นเครือข่ายร่วมกัน เป็นต้น

๑.๓ การจัดเตรียมอุปกรณ์

ศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี ซึ่งเป็นหน่วยงานที่ดูแลระบบเทคโนโลยีสารสนเทศระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ ดังนี้

- เครื่องคอมพิวเตอร์PC/เครื่องคอมพิวเตอร์ Notebook
- แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการของเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
- อุปกรณ์สำรองข้อมูลและระบบงานที่สำคัญ

- โปรแกรมantivirus
- Driverอุปกรณ์ต่างๆ
- ระบบสำรองไฟฟ้าอัตโนมัติ
- อุปกรณ์สำรองต่างๆของเครื่องคอมพิวเตอร์

๑.๔ การสำรองข้อมูล

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเกิดความเสียหาย ถูกทำลายจากไวรัสหรือผู้บุกรุกแทรกแซงเปลี่ยนแปลงข้อมูล และสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยเรือนจำฯ มีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์ และแผนการสำรองข้อมูล ดังนี้

- การสำรองข้อมูลเว็บไซต์ และระบบงานต่าง ๆ
- การสำรองข้อมูลเครือข่าย (Configuration)

๑.๕ การป้องกันและกำจัดไวรัส

มีการติดตั้งซอฟต์แวร์ป้องกันและกำจัดไวรัส สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อในระบบเครือข่าย โดยผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่ออินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้บุกรุกสามารถเข้ามาทำลายระบบได้

๑.๖ การป้องกันการบุกรุกและภัยคุกคามทางไซเบอร์

เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย มีแนวทาง ดังนี้

- กำหนดมาตรการควบคุมการเข้า – ออก ห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหายโดยห้องควบคุมจะมีกุญแจ และ keycard ส่วนกลางเพียง ๑ ชุดเท่านั้น กรณีที่ผู้เกี่ยวข้องต้องการเข้าไปในห้องควบคุมต้องลงชื่อเบิกกุญแจ และ keycard ในสมุดควบคุมการเข้า – ออก ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็น ให้เจ้าหน้าที่ของศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี เป็นผู้รับผิดชอบพาเข้าไป ภายในห้องควบคุมที่มีการติดตั้งกล้องโทรทัศน์วงจรปิด
- มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้ โดยกำหนดให้ Firewall ควบคุมการเข้า-ออก หรือการควบคุมการรับ-ส่งข้อมูล ในระบบเครือข่าย และเปิดใช้งานตลอดเวลา
- มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเตอร์เน็ตของศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี เพื่อตรวจสอบการใช้งานบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและหาวิธีการป้องกันต่อไป
- การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยได้จัดหาระบบบริหารจัดเก็บข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้าระวังในเครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายของศูนย์บริการประชาชน เรือนจำจังหวัดสุพรรณบุรี ให้ดียิ่งขึ้น

๒. การเตรียมความพร้อม

๒.๑ การเตรียมความพร้อมกรณีเกิดการคุกคามทางไซเบอร์

เมื่อเกิดเหตุโจมตี บุกรุก ผ่านทางเว็บไซต์ให้ดำเนินการ ดังนี้

๑) สกัดกั้นการเข้าถึงเครื่องให้บริการ เพื่อไม่ให้เกิดการเปลี่ยนแปลงของข้อมูล ด้วยการถอดสาย Network ออกจากเครื่อง

๒) ตรวจสอบความเปลี่ยนแปลงของข้อมูลในระบบ

๓) ตรวจสอบ Log File หรือ แฟ้มกิจกรรมของระบบ เพื่อดูพฤติกรรมที่น่าสงสัย

๔) ดำเนินการปิดช่องโหว่บนหน้าเว็บไซต์ โดยให้คำนึงถึงสิ่งต่างๆ ดังนี้

- การตรวจสอบการป้อนข้อมูล
- SQL Injection
- XSS (Cross Site Scripting)

๕) หากไม่สามารถดำเนินการแก้ไขได้โดยเร็ว ให้ทำการปิดการใช้งานในส่วนที่เกิดปัญหาก่อน ปรับปรุงซอฟต์แวร์ที่เกี่ยวข้องให้เป็นรุ่นล่าสุดที่มีความมั่นคงปลอดภัยสูง

๒.๒ แผนปฏิบัติกรณีเกิดการแทรกแซงเว็บไซต์

๑) เจ้าหน้าที่ได้รับแจ้งทางอีเมล์หรือโทรศัพท์ว่า เว็บไซต์ www.suphanburiprison.com ถูกแทรกแซงเปลี่ยนหน้าเว็บไซต์

๒) ทดลองเข้าเว็บไซต์ www.suphanburiprison.com เพื่อตรวจสอบหน้าเว็บไซต์อีกครั้ง

๓) หลังจากตรวจสอบเป็นที่แน่ชัดว่าหน้าเว็บไซต์ถูกเปลี่ยนแปลง ให้รีบเก็บหลักฐานโดยการ copy หน้าเว็บไซต์ไว้

๔) ตรวจสอบหาร่องรอยการเข้าโจมตี ตรวจสอบ log เพื่อหา IP ที่เข้าเปลี่ยนหน้าเว็บไซต์

๕) แก้ไขข้อบกพร่อง ช่องโหว่ทางเครือข่าย ที่เป็นสาเหตุให้ถูกโจมตี เปลี่ยน Password การเข้าใช้เครื่องแม่ข่ายหากจำเป็น

๖) เปลี่ยนหน้าเว็บไซต์กลับเป็นแบบเดิมพร้อมเชื่อมต่อเครือข่ายอินเตอร์เน็ต เข้ากับเครื่องให้บริการเว็บไซต์ เปิดการเชื่อมต่อให้สามารถใช้งานเครื่องแม่ข่ายได้ตามปกติ

๗) กรณีเกิดความเสียหายร้ายแรง ให้นำหลักฐานที่ได้ทั้งหมดเข้าแจ้งความกับตำรวจ

๒.๓ เตรียมความพร้อมในการเสริมสร้างความมั่งคงปลอดภัยให้กับระบบระบบเครือข่าย

ติดตั้งโปรแกรมสำหรับติดตามการทำงานของระบบคอมพิวเตอร์ และบริหารจัดการอุปกรณ์เครือข่าย (Solar Winds Network Monitoring) โดยอาศัยโปรโตคอล SNMP เพื่อตรวจสอบสถานะของอุปกรณ์เครือข่ายในระบบ ซึ่งจะช่วยให้ผู้ดูแลระบบนั้นสามารถที่จะพบปัญหาหรือตรวจสอบปัญหาได้อย่างรวดเร็ว

๒.๔ การเตรียมความพร้อมในการดำเนินการเกี่ยวกับโปรแกรมป้องกันและกำจัดไวรัส

๑) ดำเนินการติดตั้งโปรแกรมป้องกันและกำจัดไวรัส โดยติดตั้งโปรแกรมป้องกันและกำจัดไวรัสให้กับเครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่องอย่างเพียงพอ และได้ต่ออายุลิขสิทธิ์ของโปรแกรมทุกปี

๒) ดำเนินการปรับปรุงรุ่นของโปรแกรมให้เป็นปัจจุบันอยู่เสมอ

๓) ดำเนินการปรับปรุงฐานข้อมูลของไวรัสอย่างสม่ำเสมอ

๔) โปรแกรมป้องกันและกำจัดไวรัสที่ใช้งานอยู่ต้องมีการตรวจสอบแบบทันทีทันใด

๕) โปรแกรมป้องกันและกำจัดไวรัสที่ใช้งานอยู่ มีความสามารถในการตรวจสอบ การโจมตีจากไวรัสในรูปแบบต่างๆ ได้แก่ ตรวจสอบเมื่อเข้าใช้งานแฟ้มข้อมูล, ตรวจสอบเมื่อเข้าใช้งานโปรแกรมดูเว็บไซต์ และตรวจสอบเมื่อมีการใช้งาน E-mail

๓. กระบวนการแก้ไขปัญหา/แผนผังกระบวนการแก้ไขปัญหา

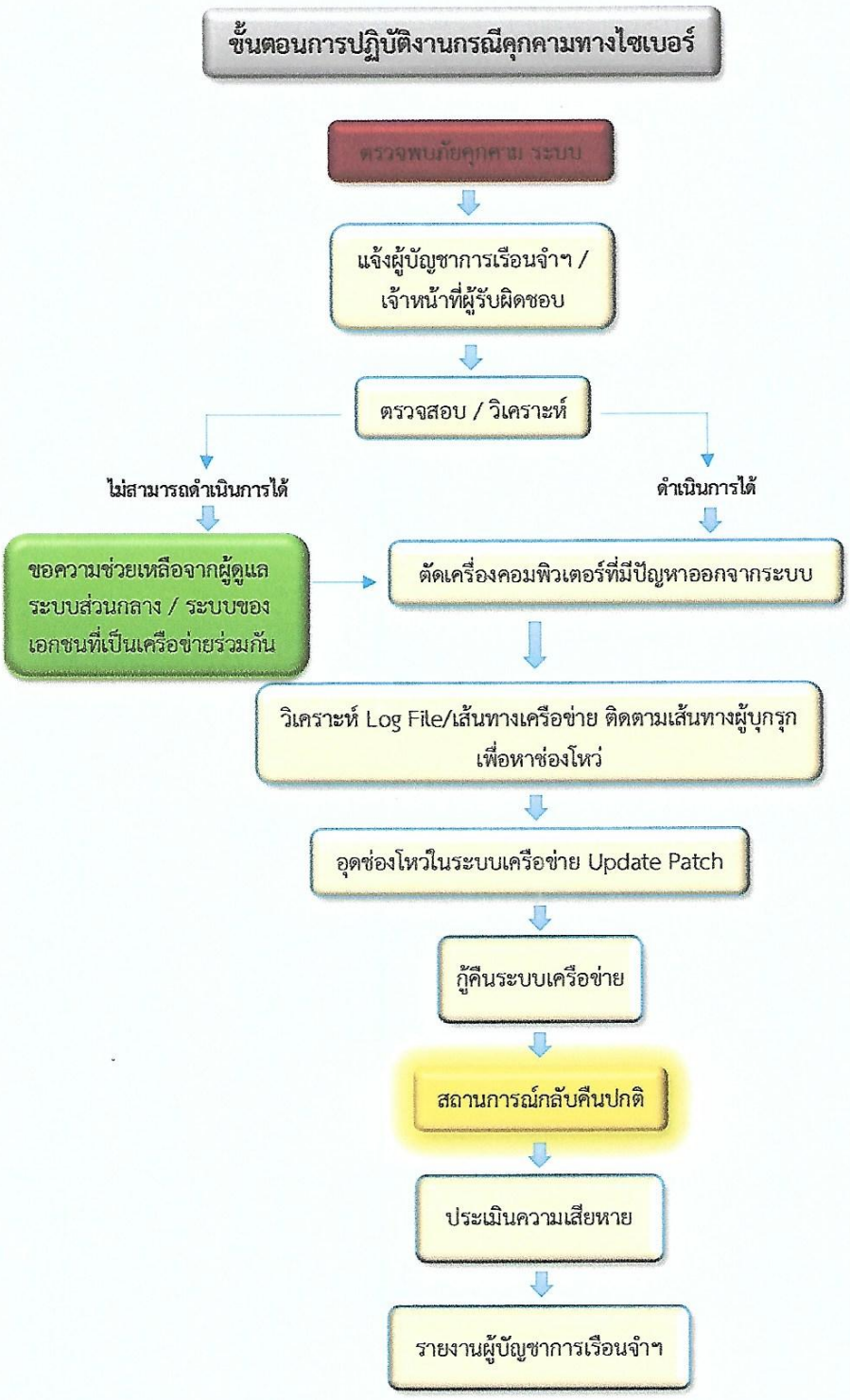
๓.๑ กรณีเกิดเหตุให้เจ้าหน้าที่แจ้งหัวหน้าฝ่ายสวัสดิการฯ ทราบ

๓.๒ หัวหน้าฝ่ายสวัสดิการฯ มอบหมายให้ นายชัยทัศน์ฯ ตรวจสอบสถานการณ์กรณีตรวจสอบแล้วไม่สามารถแก้ไขปัญหาได้ให้แจ้งผู้ดูแลระบบของเอกชนที่เป็นผู้สร้างระบบ

๓.๓ ในช่วงระยะเวลาการตรวจสอบและแก้ไขระบบสารสนเทศ ให้เจ้าหน้าที่งานเยี่ยมญาติ ให้บริการญาติโดยใช้ระบบ manual บันทึกข้อมูลการจองเยี่ยมผู้ต้องขังออนไลน์ กำหนดรอบเข้าเยี่ยม จดชื่อ-นามสกุล เบอร์โทรศัพท์ญาติ ชื่อ-นามสกุล ผู้ต้องขังที่เยี่ยม จำนวนญาติที่มาเยี่ยม ไว้ประกอบการตรวจสอบข้อมูล และจัดทำบัญชีการจองเยี่ยมผู้ต้องขังออนไลน์ ส่งให้ส่วนควบคุมผู้ต้องขังทราบ

๓.๔ ให้หัวหน้าฝ่ายสวัสดิการฯ และเจ้าหน้าที่ประชาสัมพันธ์ ปัญหาความขัดข้องให้ญาติทราบเป็นระยะๆ

ผังกระบวนการแก้ไขปัญหา



๔. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์คุกคามทางไซเบอร์

๔.๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้คำเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม วางแผน ตรวจสอบ ผู้รับผิดชอบ ได้แก่

๑.ผู้บัญชาการเรือนจำจังหวัดสุพรรณบุรี

๒.ผู้อำนวยการส่วนสวัสดิการและสงเคราะห์ผู้ต้องขัง

๓.ผู้อำนวยการส่วนควบคุมผู้ต้องขัง

๔.ผู้อำนวยการส่วนทัณฑปฏิบัติ

๔.๒ ระดับปฏิบัติ เทคโนโลยีสารสนเทศและเครือข่าย

เจ้าหน้าที่ผู้ดูแลระบบของหน่วยงาน รับผิดชอบการปฏิบัติงาน การบริหารจัดการศึกษา ทบทวน ติดตาม และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยแบ่งทีมงาน ดังนี้

ทีมกู้คืนระบบปฏิบัติการ ทำหน้าที่บริหารจัดการดำเนินการแก้ไขปัญหาเบื้องต้น กู้คืนระบบงาน ฐานข้อมูลต่างๆ และทำหน้าที่ติดตั้ง ค้นหาสาเหตุและวิธีการอุดช่องโหว่ในระบบ ให้สามารถกลับมาใช้งานได้ตามปกติ

๑.นางสริตา ศิลาโรจน์ ตำแหน่ง นักทัณฑวิทยาชำนาญการ

๒.นางหัทยา ขาวบริสุทธิ์ ตำแหน่ง นักทัณฑวิทยาชำนาญการ

๓.นายชัยทัศน์ ภูพวงจันทร์ ตำแหน่ง ผู้ช่วยพนักงานราชทัณฑ์

๔.นายสันทัศ ชาวกำแพง ตำแหน่ง ผู้ช่วยพนักงานราชทัณฑ์

๕.นายพงศ์พิสิฐ นิธิเสรีธำรง ตำแหน่ง ผู้ช่วยพนักงานราชทัณฑ์

ทีมกู้คืนเครือข่าย ทำหน้าที่บริหารจัดการดำเนินการจัดหาระบบป้องกันไม่ให้เกิดความเสียหายต่อระบบ และอุปกรณ์เครือข่าย ประสานงานการกู้คืนให้เครือข่ายกลับมาใช้งานได้ตามปกติ

๑.นางสริตา ศิลาโรจน์ ตำแหน่ง นักทัณฑวิทยาชำนาญการ

๒.นางหัทยา ขาวบริสุทธิ์ ตำแหน่ง นักทัณฑวิทยาชำนาญการ

๓.นายชัยทัศน์ ภูพวงจันทร์ ตำแหน่ง ผู้ช่วยพนักงานราชทัณฑ์

๔.นายสันทัศ ชาวกำแพง ตำแหน่ง ผู้ช่วยพนักงานราชทัณฑ์

๕.นายพงศ์พิสิฐ นิธิเสรีธำรง ตำแหน่ง ผู้ช่วยพนักงานราชทัณฑ์

ทีมประเมินความเสียหาย ทำหน้าที่ประเมินความเสียหายและให้ข้อมูลความเสียหายทั้งด้าน Hardware ละ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน ประสานงานตามคำสั่งการ ตรวจสอบ รายงานผลต่อผู้บัญชาการเรือนจำจังหวัดสุพรรณบุรีทราบ

๑.นางสริตา ศิลาโรจน์ ตำแหน่ง นักทัณฑวิทยาชำนาญการ

๒.นางหัทยา ขาวบริสุทธิ์ ตำแหน่ง นักทัณฑวิทยาชำนาญการ

๓.นายชัยทัศน์ ภูพวงจันทร์ ตำแหน่ง ผู้ช่วยพนักงานราชทัณฑ์

๕. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์คุกคามทางไซเบอร์ให้ผู้บัญชาการเรือนจำจังหวัดสุพรรณบุรีทราบ เพื่อนำเสนอรายงานสรุปให้ผู้บริหารระดับสูงของกรมราชทัณฑ์ เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันที ในกรณีที่เกิดเหตุคุกคามทางไซเบอร์ ต่อไป

จัดทำโดย ชื่อ : พ.ต.ท.ชินโชติ พุฒิวรรธธาดา โทรศัพท์ : ๐๘๐-๐๗๑-๔๑๓๕ ตำแหน่ง : ผู้บัญชาการเรือนจำจังหวัดสุพรรณบุรี	พันตำรวจโท (ชินโชติ พุฒิวรรธธาดา) ผู้บัญชาการเรือนจำจังหวัดสุพรรณบุรี