แบบฟอร์มที่ 2

แผนความพร้อมใช้งานระบบสารสนเทศในภาวะฉุกเฉินระดับหน่วยงาน

ชื่อหน่วยงาน สำนักงานป้องกันควบคุมโรคที่ 9 จังหวัดนครราชสีมา กรมควบคุมโรค

ชื่อแผน แผนความพร้อมใช้งานระบบสารสนเทศในภาวะฉุกเฉิน กรณีพบไวรัสคอมพิวเตอร์

ความสำคัญ/วัตถุประสงค์ของการจัดทำแผนนี้

ระบบเครือข่ายคอมพิวเตอร์ รวมถึงระบบข้อมูลสารสนเทศ ถือเป็นทรัพยากรที่มีความสำคัญต่อองค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย และมั่นใจได้ว่าระบบเครือข่ายคอมพิวเตอร์ และระบบข้อมูลสารสนเทศสามารถใช้ได้งานได้ตามปกติ ส่งเสริมสนับสนุนการปฏิบัติตามภารกิจของกรมควบคุมโรคได้

สำนักงานป้องกันควบคุมโรคที่ 9 จังหวัดนครราชสีมา ได้ตระหนักถึงภัยคุกคามระบบสารสนเทศ ทั้งในรูปแบบไวรัสคอมพิวเตอร์ การโจมตีระบบจากผู้ไม่ประสงค์ดี จึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยคุกคามระบบสารสนเทศ ของสำนักฯ (IT Contingency Plan) เพื่อเป็นกรอบ แนวทางในการแก้ไขปัญหาให้ระบบสารสนเทศกลับคืนสู่ความเป็นปกติ ตลอดจนการดูแลรักษาระบบสารสนเทศให้มีเสถียรภาพ พร้อมใช้งานได้อย่างมีประสิทธิภาพต่อไป

วัตถุประสงค์

1. เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากภัยคุกคามระบบสารสนเทศ
2. เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้การปฏิบัติราชการ ดำเนินไปได้อย่างมีเสถียรภาพ
4. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยด้านเทคโนโลยีสารสนเทศ

การวิเคราะห์ภัยคุกคามและผลกระทบต่อหน่วยงาน

เนื่องจากภารกิจสำนักงานป้องกันควบคุมโรคที่ 9 มีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศ มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงได้วิเคราะห์และตรวจสอบความเสี่ยงต่างด้านสารสนเทศ สำนักงานป้องกันควบคุมโรคที่ 9 พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศดังนี้

1. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง ส่วนใหญ่เกิดจากการถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

2. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของกรมเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

3. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

4. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสำนักงานป้องกันควบคุมโรคที่ 9 ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ คือ ความเสี่ยงด้านเทคนิคที่เกิด**จากการ**ถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานป้องกันควบคุมโรคที่ 9 มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของสำนักงานป้องกันควบคุมโรคที่ 9

การจัดทำแผนบริหารความต่อเนื่อง (BCP – Business Continuity Plan) สำหรับกลุ่มกิจกรรมที่ได้รับผลกระทบจากการหยุดชะงักของระบบสารสนเทศ

แบบฟอร์ม BCP 1 ทำความเข้าใจในภารกิจขององค์กร (ตามภารกิจในกลุ่ม/ศูนย์/งาน) “กลุ่มพัฒนาองค์กร”
วัตถุประสงค์ : เพื่อวิเคราะห์กิจกรรม/บริการที่เป็นภารกิจที่สำคัญขององค์กร (ตามภารกิจในกลุ่ม/ศูนย์/งาน)

กิจกรรม/บริการที่สำคัญของกลุ่ม/ศูนย์/งาน	ความจำเป็นของกิจกรรม/บริการในภาวะการณ์เกิดการระบาดของโรค/ สาธารณภัย		สามารถดำเนินกิจกรรมภายนอกองค์กรได้หรือไม่	สิ่งที่ต้องการสนับสนุนในกิจกรรม/บริการที่จำเป็น
	จำเป็น	ไม่จำเป็น		
กลุ่มพัฒนาองค์กร สำนักงานป้องกันควบคุมโรคที่ 9 นครราชสีมา 1. พัฒนาคุณภาพระบบบริหารจัดการองค์กรตามมาตรฐานสากล โปร่งใส ตรวจสอบได้		√	ได้	- บุคลากรที่มีทักษะด้านการบริหารจัดการองค์กร
2. วางแผนและพัฒนาบุคลากรให้มีศักยภาพและสมรรถนะการดำเนินงานตามภารกิจของหน่วยงานอย่างมีประสิทธิภาพ คุณภาพและประสิทธิผล	√		ได้	- บุคลากรที่มีสมรรถนะด้านการป้องกันควบคุมโรค กฎหมาย พรบ. เมื่อเกิดการระบาดของโรค/ สาธารณภัย
3. พัฒนาระบบการจัดทำ กำกับ ติดตาม ปรับปรุงให้ผลการปฏิบัติงานบรรลุผลตามเป้าหมายคำรับรองการปฏิบัติราชการของบุคลากร/ กลุ่มงาน/ หน่วยงาน	√		ได้	- การรายงานข้อมูลตัวชี้วัดคำรับรองฯ ในระบบ EstimatesSM ที่สามารถใช้งานได้อย่างต่อเนื่อง
4. พัฒนาระบบบริหารผลการปฏิบัติงาน (PMS) ของบุคลากร/ หน่วยงาน ในส่วนการประเมินสมรรถนะและแผนพัฒนารายบุคคล (IDP)		√	ได้	- ระบบสารสนเทศทรัพยากรบุคคล DPIS ที่สามารถรายงานผลการปฏิบัติงาน (PMS online) ได้ตามระยะเวลาที่กำหนด
5. จัดทำระบบฐานข้อมูล ปรับปรุงระบบและการสืบค้นข้อมูลที่สำคัญด้านบริหารและวิชาการ รวมทั้งให้คำปรึกษาและให้การสนับสนุนงานด้านเทคโนโลยีสารสารสนเทศ	√		ได้	- ระบบฐานข้อมูล และเทคโนโลยีสารสนเทศที่สามารถใช้งานได้อย่างต่อเนื่อง ตลอดเวลา - อุปกรณ์การสื่อสาร

แบบฟอร์ม BCP 2 รายชื่อบุคลากรหลัก และบุคลากรสำรองกลุ่ม/ศูนย์/งานสำนักงานป้องกันควบคุมโรคที่ 9 นครราชสีมา

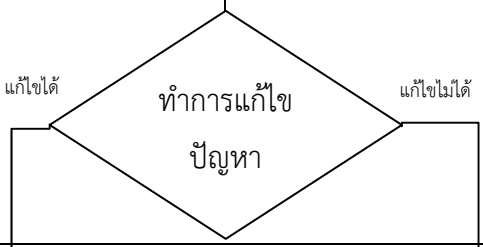
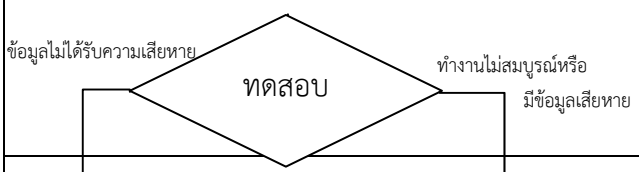
บุคลากรหลัก		บทบาท/งาน	บุคลากรสำรอง	
ชื่อ – สกุล/ตำแหน่ง	**โทรศัพท์มือถือ**		**ชื่อ – สกุล/ตำแหน่ง**	**โทรศัพท์มือถือ**
นายประวิทย์ ลายจันทึก	081-9978123	จัดทำระบบฐานข้อมูล ปรับปรุงระบบและการสืบค้นข้อมูลที่สำคัญด้านบริหารและวิชาการ รวมทั้งให้คำปรึกษาและสนับสนุนงานด้านเทคโนโลยีสารสารสนเทศ	นายจิระเดช พลสวัสดิ์	090-9536223

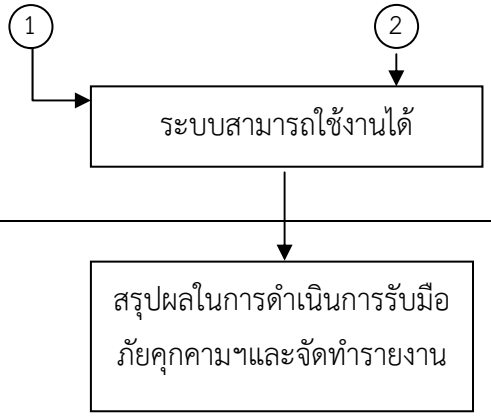
ขั้นตอนการปฏิบัติการ และกลยุทธ์การกู้คืนกิจกรรมที่สำคัญ

กลยุทธ์การป้องกันไวรัสคอมพิวเตอร์

1. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ
2. Backup ข้อมูลที่สำคัญไว้อย่างสม่ำเสมอ
3. ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ
    - 3.1 สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
    - 3.2 ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย
    - 3.3 ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา
4. ใช้ความระมัดระวังในการเปิด E-mail
    - 4.1 ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
    - 4.2 ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา
5. ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต
    - 5.1 ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ
    - 5.2 ไม่ดาวน์โหลดไฟล์จาก website ที่ไม่น่าเชื่อถือ
    - 5.3 ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ
    - 5.4 หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น
6. ปิดการใช้งานฟังก์ชัน Autoplay เพื่อป้องกันไม่ให้ไวรัสที่แพร่ระบาดผ่านทางสื่อเก็บข้อมูลแบบพกพาใช้เป็นช่องทางในการรันไฟล์ไวรัสโดยอัตโนมัติ

ขั้นตอนการปฏิบัติการ

เหตุการณ์	รายละเอียด
	จากการเฝ้าระวังตรวจสอบ Log จะช่วยให้ตรวจพบภัยคุกคามก่อนที่จะสร้างเสียหายในวงกว้าง
	ตรวจสอบถึงชนิดประเภท ความรุนแรงและกระทบที่คาดว่าจะเกิดกับระบบ
	ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือ ขยายวงไปยังจุด อื่นๆ เช่น ปิดระบบ, ตัดการเชื่อมต่อ เป็นต้น
	แก้ไขหรือสามารถกำจัดภัยคุกคามได้ในเบื้องต้นให้ทำการแก้ไขในทันที
	หากไม่สามารถแก้ไขได้ให้ติดต่องานสารสนเทศและงานพัสดุ เพื่อทำการแก้ไข หรือส่งร้านซ่อม และเบิกเครื่องคอมพิวเตอร์สำรองไปใช้งาน
	เมื่อแก้ไขภัยคุกคามได้สำเร็จให้ตรวจหาช่องโหว่และทำการป้องกันเพื่อไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำ
	ตรวจสอบการใช้งานระบบว่าทำงานได้ปกติหรือมีข้อมูลสูญหายหรือไม่
	หากพบว่ามีความเสียหายให้กู้คืนข้อมูลหรือระบบตามที่มีการ Backup ไว้

	ระบบอยู่ในสภาพการให้บริการตามปกติ สรุปผลในการดำเนินการรับมือภัยคุกคามฯ รวมทั้งแจ้งผลการดำเนินการให้ผู้ที่เกี่ยวข้องรับทราบ และบันทึกรายงานการดำเนินงาน เพื่อให้บุคคลที่เกี่ยวข้องได้ทราบ และใช้เป็นกรณีศึกษาในภายหลัง

กำหนดทรัพยากรและบุคลากรสำคัญหรือจำเป็นต่อการบริหารความต่อเนื่อง

1. การจัดเตรียมอุปกรณ์ที่จำเป็น
    1.1 แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
    1.2 สื่อบันทึกข้อมูลสำรอง เช่น Hard disk external, Flash Drive, DVD RW
    1.3 ข้อมูลและระบบงานที่สำคัญ
    1.4 แผ่นโปรแกรม antivirus/spyware
    1.5 แผ่น driver อุปกรณ์ต่างๆ
    1.6 ระบบสำรองไฟฉุกเฉิน
    1.7 อุปกรณ์สำรองต่างๆ เช่นเครื่องคอมพิวเตอร์, Hard disk
2. การจัดเตรียมบุคลากร

ทีมบริหารความต่อเนื่อง ชื่อ-สกุล กลุ่มงาน/ตำแหน่งงาน	โทรศัพท์ ที่ทำงาน	โทรศัพท์ ที่บ้าน	โทรศัพท์ มือถือ	E-mail
นายประวิทย์ ลายจันทึก นักวิชาการคอมพิวเตอร์	044-212900 ต่อ 128	-	081-9978123	velkyrie@hotmail.com
นายจิระเดช พลสวัสดิ์ เจ้าพนักงานคอมพิวเตอร์	044-212900 ต่อ 128	-	090-9536223	jira2524@hotmail.com
นางสาวนันท์นภัส สุขใจ	044-212900 ต่อ 128	-	087-2491252	fonitdpc5@yahoo.com

วัน-เดือน-ปี และสถานที่ ที่จัดการซ้อมแผน

วันที่ซ้อมแผน 6 มิถุนายน 2560 ณ ห้องประชุมราชพฤกษ์ ชั้น3 สำนักงานป้องกันควบคุมโรคที่ 9 นครราชสีมา

วิธีการซ้อมแผนกรณีพบไวรัสคอมพิวเตอร์

วิธีการกำจัด Virus

1. เมื่อตรวจสอบจาก Log พบว่ามี ไวรัส หรือมีผู้ใช้งานแจ้งเหตุ
2. ให้ผู้ใช้งานตรวจสอบ antivirus และ Update Antivirus ที่มีอยู่ในเครื่องที่ติด Virus โดยการคลิกขวา Icon Antivirus ที่ Taskbar (มุมด้านล่างขวา) เลือก Update
3. ตัดการเชื่อมต่อเครือข่าย Network (ดึงสาย LAN ออก, ปิดระบบ WiFi)
4. Backup ข้อมูลที่สำคัญไว้ในสื่อบันทึกข้อมูลอื่น เช่น Flash drive, External Hard disk, สื่อบันทึกข้อมูลอื่นๆ
5. ปิดระบบ System Restore โดย
    1. คลิ้กขวาที่ไอคอน My Computer บน Desktop และ เลือก Properties
    2. เลือกแถบ System Restore
    3. คลิก เลือก Turn off System Restore on all drives
    4. กด Ok
6. ยกเลิก ไฟล์ที่ซ่อนไว้ (ทำใน Folder option --> View) โดย
    1. ดับเบิ้ลคลิก My Computer
    2. เลือก Tool เลือก Folder Option
    3. เลือก View ที่ Hidden file and folders เลือก Show hidden files and folders
    4. ให้เอาเครื่องหมายถูกออก ที่ Hide extensions for know file types และ Hide protected operation system file (Recommended)
7. ลบ Temp file , File Temporary Internet ทั้งหมด โดย การทำ Disk Cleanup
8. Scan virus แบบ Full
9. สังเกตจาก Status ของ Antivirus ชนิดนั้นๆ ว่ากำจัดไวรัสได้หรือไม่
10. Restart เครื่อง

หมายเหตุ : หากทำตามขั้นตอนดังกล่าวแล้ว ไม่สามารถกำจัด Virus ได้ให้เขียนใบแจ้งซ่อม และส่งเครื่องคอมพิวเตอร์มาซ่อมที่พัสดุ และเบิกเครื่องสำรองไปใช้งานในระหว่างที่ส่งซ้อม

.....