META CORPORATION		
ชื่อเอกสาร : แผนรองรับสถานการณ์ฉุกเฉิน	วันที่ : 20 มิถุนายน 2561	หมายเลขเอกสาร :
หน่วยงาน : เทคโนโลยีสารสนเทศ	แก้ไขครั้งที่ :	หน้าที่ : 1
จัดทำโดย : นายคุณากร เนียมน้อย	ทบทวนโดย : นายคุณากร เนียมน้อย	อนุมัติโดย :

แผนรองรับสถานการณ์ฉุกเฉิน

1.กรณีการป้องกันไวรัสล้มเหลว

-กรณีถูกไวรัส เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบ เครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

-วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

-ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

-ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ หรือมีเหตุอันทำให้ไม่สามารถใช้งานระบบเครือข่ายได้ จะต้องประกาศให้ทุกฝ่ายทราบ

2.กรณีการป้องกันผู้บุกรุกล้มเหลว

-กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall

-ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

3.กรณีการเชื่อมโยงเครือข่ายล้มเหลว

-รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

-หากสายสัญญาณมีการชำรุดขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลระบบเครือข่าย เพื่อดำเนินการซ่อมแซมให้เสร็จเรียบร้อยโดยเร็ว

หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางส่วน ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยัง Access Point และ Core Switch ที่ติดตั้งอยู่ ณ ส่วนๆนั้น

4.กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

-รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

5.กรณีไฟฟ้าขัดข้อง

-อุปกรณ์และระบบมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ 1 ชั่วโมง

-หากไฟฟ้าขัดข้องใกล้ครบ 1 ชั่วโมง ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย

-หากเครื่องสำรองไฟฟ้ามีปัญหา ดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน