แนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
สำนักงานสาธารณสุขจังหวัดชัยนาท และหน่วยงานในสังกัด

ตามประกาศมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานสาธารณสุขจังหวัดชัยนาท เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานสาธารณสุขจังหวัดชัยนาท เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย เพื่อให้สามารถป้องกันปัญหาหรือภัยคุกคามที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศซึ่งอาจก่อให้เกิดความเสียหายแก่หน่วยงาน จึงขอกำหนดแนวปฏิบัติ ดังนี้

ระดับผู้บริหาร

- ผู้บริหารระดับสูงของหน่วยงาน
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของหน่วยงาน (CIO)

๑.กำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

๒.วางแผน กำกับ ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๓.รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ระดับแอดมิน (Admin)

๑.สำรวจเว็บไซต์และระบบงานในความดูแลของหน่วยงาน และจัดทำทะเบียนชื่อเว็บไซต์และชื่อโดเมน และ IP Address เช่น ict-ops-moph.moph.go.th ๒๐๓.๑๕๗.XXXX

๒.ปิดเว็บไซต์และระบบงานที่ไม่ได้ใช้งาน รวมถึงเว็บไซต์และระบบงานที่พบความเสี่ยงทั้งหมดในทันที

๓.ดูแล Environments ทั้งหมดที่เกี่ยวข้อง ของเว็บไซต์ และอัปเดตให้ทันสมัย เช่น อัปเดตเวอร์ชัน และ Patch ของระบบปฏิบัติการและซอฟต์แวร์ให้เป็นปัจจุบัน

๔.ติดตั้งอุปกรณ์ป้องกันภัยคุกคามไซเบอร์ เช่น Firewall, Web Application Firewall และAntivirus เป็นต้น พร้อมตั้งค่าให้ถูกต้อง เหมาะสมกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

๕.เฝ้าระวังภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง โดยต้องจัดให้มีเจ้าหน้าที่ปฏิบัติงานเป็นประจำอย่างน้อย ๑ คน

๖.รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๗.ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจาก บุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๘.รับผิดชอบ...

๘.รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต

๙.ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๑๐.หากเกิดภัยคุกคามให้รีบประสานเป็นการด่วนตามช่องทางต่อไปนี้

๑.ระดับจังหวัด

โทรศัพท์ ๐๘ ๗๘๔๘ ๐๗๗๑, ๐๙ ๑๘๗๑ ๐๕๐๔, ๐ ๕๖๔๐ ๕๕๑๘ ต่อ ๒๑๖

อีเมล: chainatdatacenter@gmail.com

เว็บไซต์: www.cnto.moph.go.th/

Line Official: @๕๓๘efwiz

๒. ระดับกระทรวง Health CERT

โทรศัพท์ ๐๘ ๓๐๖๔ ๙๘๖๗, ๐ ๒๕๙๐ ๑๑๖๙, ๐ ๒๕๙๐ ๑๒๐๐

อีเมล: health-cirt@moph.go.th

Line Official: @health-cirt

เว็บไซต์แจ้งเหตุการณ์ไซเบอร์: https://health-cirt.moph.go.th

เว็บไซต์เผยแพร่ประชาสัมพันธ์ข้อมูลข่าวสารทางไซเบอร์: https://cyber.moph.go.th/

ระดับผู้ปฏิบัติงาน (USER)

๑.ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานสาธารณสุขจังหวัดชัยนาท

๒.ไม่นำอุปกรณ์อื่นใดเข้ามาติดตั้งใช้งานในสำนักงานก่อนได้รับอนุญาต

๓.ไม่ดัดแปลงแก้ไขอุปกรณ์เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง หรือระบบ Network ของสำนักงาน

๔.เมื่อพบเหตุผิดปกติของเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง หรือระบบ Network ให้แจ้งผู้ดูแลโดยทันที

๕.ไม่เปิดสื่อออนไลน์ที่ไม่รู้จักแหล่งที่มา ที่มีความเสี่ยงต่อภัยคุกคามทางไซเบอร์โดยเด็ดขาด

๖.ตรวจสอบข้อมูลที่ตนเองเผยแพร่ในสื่อออนไลน์ทั้งหมด หากเป็นข้อมูลส่วนบุคคลให้นำออกทั้งหมด

๗.ก่อนนำข้อมูลส่วนบุคคลขึ้นสู่สื่อออนไลน์จะต้องได้รับความเห็นชอบหรืออนุญาต (อย่างมีหลักฐาน) จากผู้บริหารสูงสุดของหน่วยงาน

๘.ข้อมูลที่นำเข้าสู่สื่อออนไลน์ต้องทำการเข้ารหัสเพื่อป้องกันผู้ไม่เกี่ยวข้องนำไปใช้