

# สำเนาฉบับ



คำสั่งโรงเรียนช่างฝีมือทหาร

(เฉพาะ)

ที่ ๑๔๖ /๖๒

เรื่อง นโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.ชท.สปท.

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของ รร.ชท.สปท. เป็นไปด้วยความเรียบร้อยมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสอดคล้องกับนโยบายของผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief information Officer : CIO) ของ รร.ชท.สปท. จึงให้ดำเนินการดังนี้

๑. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (internet) ผ่านระบบรักษาความปลอดภัย ของ รร.ชท.สปท. ที่จัดสรรไว้ให้เท่านั้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นมีเหตุผลความจำเป็น ต้องทำหนังสือแจ้งให้ทาง ผกม.บก.รร.ชท. ทราบเพื่อขออนุมัติจากผู้บังคับบัญชา จึงจะดำเนินการได้

๒. ผู้ใช้งานสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศ ตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเท่านั้น และเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของ รร.ชท.สปท. ต้องไม่ใช้ระบบอินเทอร์เน็ต ของ รร.ชท.สปท. เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมและกฎหมาย เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือ เว็บไซต์ที่เป็นภัยต่อสังคมละเมิดสิทธิผู้อื่น หรือข้อมูลที่สามารถสร้างความเสียหายให้กับหน่วยงาน

๓. ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข การตั้งค่าพารามิเตอร์ต่างๆ ของคอมพิวเตอร์ เช่น เลขที่อยู่เครื่องคอมพิวเตอร์ (IP Address) หรือปรับเปลี่ยนการตั้งค่าต่างๆ ของระบบคอมพิวเตอร์ รวมถึงห้ามนำอุปกรณ์อื่นใดมาติดตั้งเพิ่มเติมในระบบคอมพิวเตอร์ด้วยตนเอง

๔. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยมิได้รับอนุญาต

๕. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่าแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิตทอร์เรนต์ (Bit Torrent), อีมูล (Emule) เป็นต้น

๖. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของ รร.ชท.สปท. หากเกิดการสูญหาย นำไปใช้ในทางที่ผิด และเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายนั้น

๗. ผู้ดูแลระบบ หรือเจ้าหน้าที่ที่รับผิดชอบ สามารถประสานขอเข้าตรวจสอบระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ของหน่วยต่างๆ หากคาดว่าจะเกิดผลกระทบต่อระบบสารสนเทศ ของ รร.ชท.สปท. ได้ตลอดเวลา รวมทั้ง หากพบว่ามีกรณีฝ่าฝืนแนวปฏิบัติฯ ดังกล่าว ให้รายงานผู้บังคับบัญชาตามลำดับชั้นเพื่อพิจารณาลงโทษต่อไป

/ศ. ผู้บริหาร...

๘. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ รร.ชท.สปท. สามารถพิจารณากำหนด  
บทลงโทษหากพบผู้กระทำการฝ่าฝืนแนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.ชท.สปท. ได้  
ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป


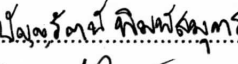
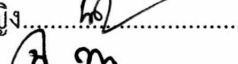
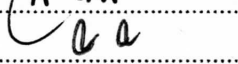
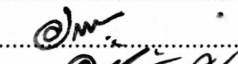

สั่ง ณ วันที่ ๒๕ กรกฎาคม พ.ศ.๒๕๖๒

พล.ต. 

(ภาณุพงศ์ สุวีณนุสส์)

ผบ.รร.ชท.สปท.

กองบัญชาการ

ร.ท.  รำง ๑๕ ก.ค.๖๒  
พ.อ.อ.  ๑๕ ก.ค.๖๒  
น.ต.หญิง  ร.น. ตรวจ ๑๕ ก.ค.๖๒  
พ.อ.  ตรวจ ๑๕ ก.ค.๖๒  
พ.อ.  ตรวจ ๑๖ ก.ค.๖๒  
พ.อ.  ตรวจ ๑๖ ก.ค.๖๒