ประกาศศูนย์คอมพิวเตอร์ โรงพยาบาลท่าวุ้ง
เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านการควบคุมการเข้าถึงระบบเครือข่าย

.....

เพื่อให้การดำเนินงานตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสาร สามารถดำเนินการได้อย่างมีประสิทธิภาพ ศูนย์คอมพิวเตอร์ โรงพยาบาลท่าวุ้ง จึงได้กำหนดแนวปฏิบัติการรักษา ความมั่นคงปลอดภัยด้านการควบคุมการเข้าถึงระบบเครือข่าย ดังนี้

๑. การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) กำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) ผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการทีได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) การใช้งานระบบสารสนเทศที่สำคัญ ไม่ว่าจะเป็นระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

(๔) การใช้งานระบบเครือข่ายไร้สายจะต้องมีการลงทะเบียนตาม ใช้งานชื่อผู้ใช้รหัสผ่านและสิทธ์ตามแนวปฏิบัติการเข้าถึงของผู้ใช้งาน

๒. การยืนยันตัวบุคคลสาหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) จะต้องมีขอปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

(๒) ต้องตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

(๓) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน อย่างน้อย ๑ วิธี

๓. มีบัญชีอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ที่ใช้งานและมีการยืนยันการเข้าถึงอุปกรณ์ดังกล่าว ดังนี้

(๑) การระบุอุปกรณ์และการจัดเก็บข้อมูล

๑) ใช้หมายเลข IP Address ในการระบุอุปกรณ์ โดยกำหนดเป็นช่วงของหมายเลข IP แยกตามประเภทของอุปกรณ์

๒) จัดเก็บข้อมูล อุปกรณ์บนเครือขายโดยระบุชนิดของอุปกรณ์การใช้งาน และเก็บบันทึกในรูปแบบสื่ออิเล็กทรอนิกส์

(๒) มีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ โดยการกำหนดให้กรอกชื่อผู้ใช้งานและรหัสผ่าน

๑) สิทธิการเข้าถึงอุปกรณ์บนอุปกรณ์เครือข่าย

๒) เมื่อกรอกชื่อผู้ใช้และรหัสผ่านที่ไม่ถูกต้องระบบจะไม่ยอมให้เข้าใช้งาน

(๓) ควบคุมการใช้งานอย่างเหมาะสม

(๔) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบแสะปรับแต่งระบบทั้งการเข้าถึง ทางกายภาพและทางเครือข่าย

(๑) การปรับเปลี่ยนหรือควบการเข้าถึงพอร์ตต้องการทำหนังสือขออนุญาตจากผู้บริหารจากระบบสารสนเทศเป็นลายลักษณ์อักษร

(๒) บันทึกและควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึง ทางกายภาพและการเข้าถึงทางเครือข่าย

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้ อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๕. การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอกและ มีการแบ่งแยกเครือข่ายตามแต่ละหน่วยงานและการใช้งาน (VLAN)

๖. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๗. การควบคุมการจัดเส้นทางบนเครือขาย (Network Routing Control) ต้องควบคุมการจัดเส้นทาง บนเครือขายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับ แนวปฏิบัติการควบคุมการเขาถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชือมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๘. การควบคุมการเข้าใช้งานระบบจากภายนอก

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของหน่วยงาน ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายขององค์กร ต้องควบคุมบุคคลที่จะเข้าสู่ระบบขององค์กรจากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ ระบบภายใน

(๓) วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการโรงพยาบาลท่าวุ้ง หรือบุคคลที่ได้รับมอบหมายจากโรงพยาบาลท่าวุ้ง และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของโรงพยาบาลและเข้าระบบและข้อมูลอย่างเคร่งครัด

(๔) การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

(๕) การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวให้ตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

จึงประกาศให้ทราบทั่วกัน

ประกาศ ณ วันที่ ๑๗ มกราคม พ.ศ.๒๕๖๕

(นายสันติ ลาภเบญจกุล)
ผู้อำนวยการโรงพยาบาลท่าวุ้ง