นโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลท่ากระดาน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มั่นความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาล ทีมนำระบบสารสนเทศ จึงได้กำหนดแนวทางในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยี โดยอ้างอิงจากแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วย ๘ หมวด ได้แก่

หมวด ๑ ว่าด้วยเรื่องการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

๑. ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลและรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้ามทำการเผยแพร่แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) ของตนเอง

๒. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๓. ผู้ใช้งานต้องตั้งรหัสของตนเป็นข้อมูลเฉพาะเพื่อให้เกิดความปลอดภัย

๔. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๖๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๕. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้งานระบบสารสนเทศของโรงพยาบาลท่ากระดาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านโดนล็อคก็ดี หรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

๕.๑ การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๕.๒ คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

๕.๓ การใช้งานระบบคอมพิวเตอร์โดยอุปกรณ์อื่นๆ ในเครือข่าย ได้แก่ แท็บเล็ต ไอแพ็ด และโทรศัพท์มือถือ เป็นต้น

๕.๔ เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานในภายหลังทุกครั้ง

๕.๕ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้อจอ (Screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที

หมวด ๒ ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

๑. ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ของโรงพยาบาลท่ากระดาน ถือเป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

๒. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๓. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครื่องแม่ข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

๔. ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มของผู้อื่นไม่ว่ากรณีใดๆ

๕. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์เกี่ยวกับการใช้งาน ก่อนได้รับอนุญาต

๖. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่โรงพยาบาลท่ากระดานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

๗. กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของโรงพยาบาลท่ากระดานตามที่ได้รับมอบหมาย

๘. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สินหากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

๙. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์หรือโน้ตบุ๊กไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

๑๐. ทรัพย์สินและระบบสารสนเทศต่างๆ ที่โรงพยาบาลท่ากระดานจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของโรงพยาบาลท่ากระดานเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่โรงพยาบาลไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อโรงพยาบาล

๑๑. ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๑๐ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวดที่ ๓ ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

๑. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลท่ากระดาน หรือเป็นข้อมูลของบุคลากรภายนอก

๒. ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของโรงพยาบาลท่ากระดานถือเป็นทรัพย์สินของโรงพยาบาลท่ากระดาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ ทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๓. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลท่ากระดานหรือข้อมูลของผู้รับบริการหากเกิดการสูญเสีย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๔. ผู้ใช้งานต้องป้องกัน ดูแลรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

๕. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลท่ากระดานจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่โรงพยาบาลท่ากระดานอาจแต่งตั้งให้มีผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด ๔ ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

๑. ผู้มีใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

๑.๑ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

๑.๒ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

๑.๓ พัฒนาโปรแกรมใดที่จะทำซ้ำโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๑.๔ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้งาน (License) ซอฟต์แวร์

๑.๕ นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพที่ไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงานของประเทศไทย กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๒. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit torrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง และเล่นเกมส์ เป็นต้น ระหว่างปฏิบัติงาน

๔. ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใด ของโรงพยาบาลท่ากระดานที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาลท่ากระดาน

๕. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลท่ากระดานเพื่อหาประโยชน์ทางการค้า

๖. ห้ามกระทำการใดๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของโรงพยาบาลท่ากระดานโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

๗. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของโรงพยาบาลท่ากระดานต้องหยุดชะงัก

๘. ห้ามใช้ระบบสารสนเทศของโรงพยาบาลท่ากระดานเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด ๕ ว่าด้วยการปฏิบัติตามกฎหมายข้อบังคับ (Law and Compliance)

บรรดากฎหมายใดๆ ที่ได้รับประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของโรงพยาบาลท่ากระดาน ถือว่าเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด ๖ ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

๑. โรงพยาบาลท่ากระดานได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟต์แวร์ที่โรงพยาบาลอนุญาตให้ใช้งานหรือที่โรงพยาบาลมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ ความจำเป็น และโรงพยาบาลท่ากระดานห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการ

ตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ โรงพยาบาลท่ากระดานถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๒. ซอฟต์แวร์ (Software) ที่โรงพยาบาลท่ากระดาน ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

หมวด ๗ ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

๑. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่โรงพยาบาลท่ากระดานได้ประกาศให้ใช้ หมั่นตรวจสอบและอัพเดตระบบปฏิบัติการ (Operating System) เช่น Windows หรือซอฟต์แวร์ที่ใช้ให้เป็นปัจจุบัน เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนาระบบป้องกันโดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

๒. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๓. ผู้ใช้งานต้องทำการรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๔. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา เมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบทราบ

๕. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์สู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบทราบ

๖. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งอื่นใดๆ ที่เป็นทรัพย์สินของโรงพยาบาลท่ากระดานหรือของอื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๗. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของโรงพยาบาลท่ากระดาน

หมวด ๘ ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

๑. ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy) ดังนี้

๑.๑ ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

๑.๒ ควรเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือน

๑.๓ ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email address) ของผู้อื่นเพื่ออ่านหรือรับ ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (Email) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (Email) ของตน

๑.๔ หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์ (Email) เสร็จสิ้น ควรลงบันทึกออก (Logout) ทุกครั้ง