
 โรงพยาบาลค่ายพิชัยดาบหัก	ระเบียบปฏิบัติ (Work Procedure)	วันที่มีผลบังคับใช้ 3/2/63
	เรื่อง นโยบายและระเบียบปฏิบัติ ด้านความมั่นคงปลอดภัยในระบบ IT	เอกสารประจำหน่วย รพ.ค่ายพิชัยดาบหัก จำนวน 1/5 หน้า
ผู้เสนอ พ.ต.หญิงดวงมณี มูลเกษ ผู้เกี่ยวข้อง เจ้าหน้าที่สารสนเทศ ผู้จัดทำ น.ส.ภัทราพร ควรคิด		ทบทวนครั้งที่ 1 ผู้อนุมัติ พ.อ.  (สมัย ขำพันธ์) ผอ.รพ.ค่ายพิชัยดาบหัก

นโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT

โรงพยาบาล ได้จัดให้มีอุปกรณ์คอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ขึ้น เพื่อความสะดวกแก่เจ้าหน้าที่ในการปฏิบัติงานให้แก่องค์กร ดังนั้น เพื่อให้การใช้คอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดจากการใช้งานทางเทคโนโลยีสารสนเทศโรงพยาบาล เห็นสมควรวางระเบียบต่อไปนี้

บทที่ 1 นิยาม

“องค์กร” หมายถึง ชื่อ โรงพยาบาล

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างขององค์กร


“เจ้าหน้าที่” หมายถึง เจ้าหน้าที่และลูกจ้างขององค์กร รวมถึงบุคคลอื่นที่องค์กรมอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

“เครือข่ายคอมพิวเตอร์” หมายถึง เครือข่ายคอมพิวเตอร์ขององค์กร

“ข้อมูล” หมายถึง ข้อมูลสำคัญของโรงพยาบาล ข้อมูลผู้ป่วย และสิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้น จะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด และไม่ว่าได้จัดทำไว้ในรูปแบบเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง ภาพวาดภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียงการบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“ระดับของข้อมูล” มี 4 ระดับ ดังนี้


 โรงพยาบาลค่ายพิชัยดาบหัก	ระเบียบปฏิบัติ (Work Procedure)	วันที่มีผลบังคับใช้ 3/2/63
	เรื่อง นโยบายและระเบียบปฏิบัติ ด้านความมั่นคงปลอดภัยในระบบ IT	เอกสารประจำหน่วย รพ.ค่ายพิชัยดาบหัก จำนวน 2/5 หน้า

1. ข้อมูลทั่วไป หมายถึง ข้อมูลทั่วไปของโรงพยาบาล ได้แก่ ประเภทการบริการ เวลาทำการ รายชื่อแพทย์แผนกที่ออกตรวจ ตารางออกตรวจ บริการห้องพักรักษาตัว ค่ารักษาพยาบาล เป็นต้น
2. ข้อมูลส่วนบุคคลของผู้ป่วย หมายถึง ข้อมูลส่วนตัวของผู้ป่วยที่ไม่เกี่ยวข้องกับการรักษาพยาบาล ได้แก่ ชื่อ - สกุลผู้ป่วย อายุ ที่อยู่ หมายเลขห้องพักรักษาตัว เป็นต้น
3. ข้อมูลความลับ หมายถึง ข้อมูลที่เกี่ยวข้องกับการรักษาพยาบาลของผู้ป่วย ทั้งที่อยู่ในเวชระเบียนและในระบบอิเล็กทรอนิกส์ ได้แก่ ผลการรักษาที่ผู้ป่วยได้รับ การวินิจฉัยโรค ผลการตรวจทางห้องปฏิบัติการผลเอกซเรย์ และผลการตรวจพิเศษต่างๆที่ผู้ป่วยได้รับ เป็นต้น
4. ข้อมูลสำคัญของโรงพยาบาล หมายถึง ข้อมูลที่โรงพยาบาลใช้ในการวางแผนงาน การกำหนดกลยุทธ์ การประเมินผลการดำเนินงาน และผลประกอบการได้แก่ นโยบาย แผนกลยุทธ์ ผลประกอบการ ตัวชี้วัดระดับโรงพยาบาล และเอกสารในระบบคุณภาพ เป็นต้น

บทที่ 2 กำหนดอำนาจหน้าที่ของคณะกรรมการหรือผู้ดูแลความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ให้มี “ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์” ที่ผู้บังคับบัญชาแต่งตั้งจากเจ้าหน้าที่ขององค์กร โดยมีอำนาจหน้าที่ดังต่อไปนี้

- ให้คำปรึกษาแก่ผู้ใช้ทราบเกี่ยวกับการปฏิบัติตามระเบียบนี้
- กำกับดูแลให้คำแนะนำเกี่ยวกับการปฏิบัติงานของผู้ดูแลเครือข่ายคอมพิวเตอร์ในการปฏิบัติตามระเบียบนี้
- ให้คำแนะนำและคำเสนอแนะต่อผู้บังคับบัญชาในการกำหนดนโยบายและมาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูล
- จัดทำรายงานเกี่ยวกับการปฏิบัติตามระเบียบนี้เสนอผู้บังคับบัญชาเป็นครั้งคราวตามความเหมาะสม
- ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในระเบียบนี้
- ดำเนินการเรื่องอื่นตามที่ผู้บังคับบัญชามอบหมาย

 โรงพยาบาลค่ายพิชัยดาบหัก	ระเบียบปฏิบัติ (Work Procedure)	วันที่มีผลบังคับใช้ 3/2/63
	เรื่อง นโยบายและระเบียบปฏิบัติ ด้านความมั่นคงปลอดภัยในระบบ IT	เอกสารประจำหน่วย รพ.ค่ายพิชัยดาบหัก จำนวน 3/5 หน้า

บทที่ 3 ข้อปฏิบัติของเจ้าหน้าที่ในการใช้คอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์

1. เจ้าหน้าที่ที่มีสิทธิใช้ระบบเครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้ การฝ่าฝืนข้อกำหนดดังกล่าวในวรรคหนึ่งและก่อให้เกิดความเสียหายแก่องค์กรหรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่เจ้าหน้าที่ที่ฝ่าฝืนตามความเหมาะสมต่อไป

2. เจ้าหน้าที่ที่พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ Download ไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น

3. เจ้าหน้าที่ที่พึงใช้ข้อมูลสุขภาพ และถูกต้องตามธรรมเนียม ปฏิบัติในการใช้เครือข่ายคอมพิวเตอร์ อาทิ เช่น ไม่ส่ง E-Mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น หรือ การใช้ข้อความไม่เหมาะสมที่สุภาพชนทั่วไปพึงใช้ โดยข้อความที่ส่งไปถึงบุคคลอื่น เป็นต้น

4. เจ้าหน้าที่มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

5. เพื่อประโยชน์ในการใช้รหัสผ่านส่วนบุคคลเจ้าหน้าที่จะต้อง

- ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่เจ้าหน้าที่ครอบครองใช้งานอยู่ ทั้งในระดับระบบปฏิบัติการ (Operating System) โดยรหัสผ่านส่วนบุคคลดังกล่าวต้องมีความยาวไม่น้อยกว่า 6 ตัวอักษร ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวที่มีความสัมพันธ์ใกล้ชิดกับตนหรือจากคำศัพท์ที่ใช้ในพจนานุกรม

- ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์


- ไม่ใช่โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสส่วนบุคคลอัตโนมัติ (Remember my password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่เจ้าหน้าที่ครอบครองอยู่

- ไม่จดหรือบันทึกรหัสผ่านบุคคลไว้บนสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

- รหัสผ่านส่วนบุคคล (User Account) ที่องค์กรให้กับเจ้าหน้าที่นั้น เจ้าหน้าที่จะต้องเป็นผู้รับผิดชอบผลอันอาจเกิดขึ้นรวมถึงผลเสียหายต่างๆ ที่เกิดจากรหัสผ่านส่วนบุคคล (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของบุคคลอื่น

6. เพื่อความปลอดภัยในการใช้คอมพิวเตอร์เครือข่ายคอมพิวเตอร์โดยส่วนรวมเจ้าหน้าที่จะต้อง

- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

 วิทยาลัยราชภัฏจันทบุรี	ระเบียบปฏิบัติ (Work Procedure)	วันที่มีผลบังคับใช้ 3/2/63
	เรื่อง นโยบายและระเบียบปฏิบัติ ด้านความมั่นคงปลอดภัยในระบบ IT	เอกสารประจำหน่วย รพ.ค่ายพิชัยดาบหัก จำนวน 4/5 หน้า

- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาก่อน

- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้นหรือเครือข่ายคอมพิวเตอร์ขององค์กรได้

7. เจ้าหน้าที่จะต้องไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ดังต่อไปนี้


- เพื่อการกระทำทางผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- เพื่อการพาณิชย์
- เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติให้แก่องค์กร ไม่ว่าจะ เป็นข้อมูลขององค์กร หรือบุคคลภายนอกก็ตาม

- เพื่อการกระทำอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือบุคคลอื่น
- เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้มีสิทธิในข้อมูลดังกล่าว

- เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรือ อาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กร

- เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กร ไปยังที่ อยู่เว็บ (Web site) ใดๆ ในลักษณะที่จะก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

- เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น ไปยังเจ้าหน้าที่หรือบุคคลอื่น เป็นต้น

 โรงพยาบาลค่ายพิชัยดาบหัก	ระเบียบปฏิบัติ (Work Procedure)	วันที่มีผลบังคับใช้ 3/2/63
	เรื่อง นโยบายและระเบียบปฏิบัติ ด้านความมั่นคงปลอดภัยในระบบ IT	เอกสารประจำหน่วย รพ.ค่ายพิชัยดาบหัก จำนวน 5/5 หน้า

บทที่ 4 ข้อปฏิบัติของผู้ดูแลเครือข่ายคอมพิวเตอร์

1. ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องดูแลรักษาปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดียิ่งขึ้น รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ของเจ้าหน้าที่เพื่อให้เป็นไปตามระเบียบ หากผู้ดูแลเครือข่ายคอมพิวเตอร์พบว่าเจ้าหน้าที่ผู้ใดพฤติกรรมส่อไปในทางที่จะละเมิดข้อกำหนดการใช้เครือข่ายคอมพิวเตอร์แห่งระเบียบนี้ ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องรายงานให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปทราบโดยเร็วที่สุดในกรณีที่เป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับองค์กร ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจในการระงับใช้งานเครือข่ายคอมพิวเตอร์ของเจ้าหน้าที่ดังกล่าวได้ทันที
2. ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่ได้รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิ์ในการเข้าถึงข้อมูลนั้น และจะต้องไม่เปิดเผยข้อมูลที่ได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ
3. ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการเสนอความเห็นข้อสังเกตต่อคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปเพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารเครือข่ายคอมพิวเตอร์ หรือปฏิบัติหน้าที่อื่นเกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ตามที่ผู้บังคับบัญชามอบหมาย
4. ผู้ดูแลเครือข่ายคอมพิวเตอร์ มีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัส ข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่างๆ ดังกล่าวให้ใช้งานได้ดียิ่งขึ้น
5. เมื่อผู้ดูแลเครือข่ายคอมพิวเตอร์พ้นจากหน้าที่แล้วจะต้องคืนทรัพย์สินอันเกี่ยวกับการปฏิบัติหน้าที่ของตนเป็นองค์กร เช่น ข้อมูลและสำเนาข้อมูล กุญแจ บัตรประจำตัว ฯลฯ ให้แก่องค์กรทันทีที่พ้นจากหน้าที่และให้คณะกรรมการระบบสารสนเทศดำเนินการตรวจสอบการคืนทรัพย์สินของผู้ดูแลเครือข่ายคอมพิวเตอร์ที่ได้พ้นจากหน้าที่โดยละเอียดเพื่อความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ขององค์กร
6. ผู้ดูแลเครือข่ายคอมพิวเตอร์ที่ฝ่าฝืนข้อกำหนดในระเบียบนี้ และก่อให้เกิดความเสียหายแก่องค์กรหรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์นั้นตามความเหมาะสมต่อไป