ต้นฉบับ

ฉบับสมบูรณ์
(ตามมติ ครั้งที่ 3 /2565 เมื่อวันที่ 28 เมษายน 2565
ลงชื่อประธาน/กรรมการฯ
(นางสาวดวงพร โต๊ะนาค)

คู่มือการปฏิบัติงาน

เรื่อง การจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่น ในกลุ่มโรคลำไส้ใหญ่และทวารหนัก

โดยวิธีปกติ

ของ

นางสาวธมลวรรณ ยอดกลกิจ
ตำแหน่งพยาบาลวิชาชีพ ระดับชำนาญการ
(ตำแหน่งเลขที่ พวช. 11401)
ฝ่ายการพยาบาล โรงพยาบาลวชิรพยาบาล
คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช

ขอประเมินเพื่อแต่งตั้งให้ดำรงตำแหน่ง

พยาบาลวิชาชีพ ระดับชำนาญการพิเศษ
(ตำแหน่งเลขที่ พวช. 11401)
ฝ่ายการพยาบาล โรงพยาบาลวชิรพยาบาล
คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช

คำนำ

ปัจจุบันเทคโนโลยีและสารสนเทศมีการพัฒนาอย่างรวดเร็วต่อเนื่อง รวมถึงผู้บริหารคณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช ได้กำหนดนโยบายการนำเทคโนโลยีมาใช้ให้เกิดประโยชน์สูงสุด มุ่งเน้นการลดขั้นตอนในการปฏิบัติงาน เปลี่ยนการจัดเก็บข้อมูลจากกระดาษสู่ไฟล์อิเลกทรอนิกส์ โดยเฉพาะในประเด็นการรวบรวมข้อมูลที่มาจากหลากหลายหน่วยงานเพื่อนำมาวิเคราะห์ภาพรวมการดูแลคนไข้กลุ่มต่าง ๆ ทำให้สามารถเชื่อมโยง ส่งต่อวิเคราะห์ผลลัพธ์ได้อย่างรวดเร็ว และสามารถนำข้อมูลมาวางแผนพัฒนาการดูแลผู้ป่วยกลุ่มโรคอย่างตรงประเด็น

โรคลำไส้ใหญ่และทวารหนักปัจจุบันมีแนวโน้มเพิ่มมากขึ้นจากพฤติกรรมของประชาชนในสังคมเปลี่ยนแปลงไป และการก้าวเข้าสู่สังคมผู้สูงอายุการรักษาที่สำคัญประการหนึ่ง คือ การผ่าตัดซึ่งต้องเข้ารับการรักษาในโรงพยาบาลกลุ่มโรคลำไส้ใหญ่และทวารหนักที่พบบ่อยที่สุดคือโรคมะเร็งลำไส้ใหญ่และทวารหนักซึ่งเป็นโรคที่จัดในกลุ่มซับซ้อนผู้ปฏิบัติการพยาบาลขั้นสูงมีบทบาทหน้าที่ในการดูแลผู้ป่วยกลุ่มโรคสำคัญที่มีความซับซ้อนรวบรวมข้อมูล และตัวชี้วัดด้านผลลัพธ์เพื่อนำมาวิเคราะห์ปรับปรุงพัฒนาระบบงานอย่างต่อเนื่องโดยหวังผลให้เกิดผลลัพธ์การรักษาพยาบาลดีที่สุด สามารถลดค่าใช้จ่าย และเพิ่มคุณภาพชีวิตของผู้ป่วยและครอบครัวเป็นสำคัญ ดังนั้นผู้จัดทำจึงเล็งเห็นถึงประโยชน์จากการใช้เทคโนโลยีด้านแอพลิเคชั่นมาช่วยในการจัดการข้อมูล เพื่อเป็นการพัฒนาระบบงานให้มีประสิทธิภาพและเป็นประโยชน์สูงสุด

ธมลวรรณ ยอดกลกิจ

ตุลาคม 2561

สารบัญ

สารบัญ(ต่อ)

สารบัญภาพ

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญ

พยาบาลเป็นบุคลากรที่มีความสำคัญต่อทีมสุขภาพ เนื่องจากเป็นผู้ให้บริการที่ใกล้ชิดผู้ป่วยมากที่สุด ทำให้สามารถค้นพบปัญหาและความต้องการของผู้ป่วยได้ทันท่วงที การตอบสนองความต้องการของผู้ป่วยที่ตรงประเด็นและยั่งยืน คือการใช้ข้อมูลที่มีอยู่มาตัดสินใจในการปฏิบัติการพยาบาล ซึ่งพยาบาลเป็นผู้ที่มีข้อมูลอยู่เป็นจำนวนมาก รวมทั้งส่วนใหญ่เป็นผู้ทำหน้าที่เก็บรวบรวมข้อมูลพื้นฐานของการให้บริการทางสุขภาพ แต่ยังไม่สามารถใช้ประโยชน์จากข้อมูลเหล่านั้นได้อย่างเต็มที่ รวมถึงข้อมูลที่เกิดขึ้นใหม่ทุกวัน การสื่อสารข้อมูลให้เชื่อมโยงมักเกิดความซ้ำซ้อน ล่าช้า สูญหาย ประกอบกับการสื่อสารข้อมูลด้วยกระดาษมีขั้นตอนที่ซับซ้อนและทรัพยากรที่ต้องใช้ในการสื่อสารกับทีมการดูแลรักษามีจำนวนมาก และมักตรวจจับความคลาดเคลื่อนของข้อมูลได้เมื่อมีการรวบรวมข้อมูลภาพรวมระดับองค์กรมักพบว่าตัวเลขผลลัพธ์เรื่องเดียวกัน แต่หลายหน่วยงานเก็บรวบรวมได้ไม่เท่ากัน เมื่อวิเคราะห์ปัญหาจะพบว่าความผิดพลาดอยู่ที่ขั้นตอนการส่งต่อข้อมูลระหว่างหน่วยงาน และความสามารถในการรวบรวมวิเคราะห์ข้อมูลของบุคคลากรปัจจุบันความก้าวหน้าด้านเทคโนโลยีคอมพิวเตอร์ในการรวบรวมและการวิเคราะห์ข้อมูลมีการพัฒนามาก โดยเฉพาะการนำสื่ออิเล็กทรอนิกส์มาใช้เพื่อให้พยาบาลสื่อสารกันได้อย่างมีประสิทธิภาพ เช่น การติดต่อผ่านระบบ cloud การใช้โปรแกรมคอมพิวเตอร์สำเร็จรูป และการใช้สื่อออนไลน์ เป็นต้น ส่งผลให้องค์กรต่าง ๆ เล็งเห็นถึงความจำเป็นของการใช้เทคโนโลยีมาประยุกต์กับการจัดเก็บข้อมูล

การจัดการข้อมูล หมายถึง การจัดเก็บข้อมูล การเรียกใช้ข้อมูล รวมถึงการวิเคราะห์ข้อมูลเพื่อการใช้งานที่รวดเร็ว จึงมักถูกจัดเก็บในรูปแบบของฐานข้อมูล ซึ่งมีข้อมูล (data) เป็นองค์ประกอบที่สำคัญ การจัดการข้อมูล (data management) เป็นกลยุทธ์หนึ่งในการบริหารองค์กรให้มีประสิทธิภาพ โดยเฉพาะอย่างยิ่งในยุคของเทคโนโลยี คอมพิวเตอร์ที่เจริญพัฒนาก้าวหน้าอย่างรวดเร็ว การจัดการข้อมูลที่มากมายต้องรวดเร็ว ถูกต้อง และทันต่อเหตุการณ์เพื่อนำไปสู่การตัดสินใจให้ถูกต้อง (วรกาล ไชยศล, 2561) ฐานข้อมูลเป็นการจัดเก็บข้อมูลอย่างเป็นระบบ ทำให้ผู้ใช้ข้อมูลที่เกี่ยวข้องในระบบงานต่าง ๆ สามารถใช้ร่วมกันได้โดยไม่เกิดความซ้ำซ้อนของข้อมูล เชื่อถือได้ และเป็นมาตรฐานเดียวกัน (Zhu et.al., 2019) ในระบบของฐานข้อมูลหรือการจัดการข้อมูลต่าง ๆ ต้องมีบุคคลที่มีหน้าที่ควบคุมดูแลฐานข้อมูล หรือผู้บริหารฐานข้อมูล (database manager)

ซึ่งมีหน้าที่กำหนดโครงสร้างหรือรูปแบบฐานข้อมูล อุปกรณ์เก็บข้อมูล วิธีการเข้าถึงข้อมูล โดยการวิเคราะห์การตัดสินใจ การเข้าถึง การจัดเก็บข้อมูล เทคนิคการจัดการข้อมูล และต้องมีแผนการสร้างข้อมูลสำรองไว้ทุกระยะ เพื่อสามารถเรียกข้อมูลกลับมาใช้ได้ในกรณีที่เกิดความผิดพลาดขึ้น ซึ่งการเข้าถึงข้อมูลต้องมีการประสานงานระหว่างผู้ให้คำปรึกษาและผู้ใช้ เพื่อให้ความช่วยเหลือหรือตรวจสอบความถูกต้อง

การดูแลรักษาผู้ป่วยในโรงพยาบาลวชิรพยาบาล มีทั้งผู้ป่วยนอกแบบฉุกเฉินไม่ฉุกเฉินและแบบผู้ป่วยใน ครอบคลุมงานบริการด้านการส่งเสริมสุขภาพ การป้องกันโรคการรักษาพยาบาล การฟื้นฟูสภาพ และการดูแลต่อเนื่องแบบสหสาขา รวมทั้งให้บริการในระดับตติยภูมิโดยรับผู้ป่วยส่งต่อจากศูนย์บริการสาธารณสุข โรงพยาบาลในเครือของกรุงเทพมหานคร และโรงพยาบาลอื่นๆ โดยเฉพาะอย่างยิ่งผู้ป่วยศัลยกรรมที่มีความซับซ้อน จากสถิติพบว่าโรคที่พบมาก 5 อันดับแรก ได้แก่ โรคมะเร็งเต้านม โรคมะเร็งลำไส้ใหญ่ โรคหลอดเลือดหัวใจตีบตันโรคเส้นเลือดในสมองโป่งพอง และโรคนิ่วในถุงน้ำดี ล้วนแต่เป็นโรคที่องค์กรมีความพร้อมในการรักษาพยาบาล มีบุคลากรที่มีความเชี่ยวชาญ มีความชำนาญ และยังผ่านการประเมินคุณภาพรายโรค (Disease Specific Certification: DSC) จากสถาบันรับรองคุณภาพสถานพยาบาล จำนวน 3 ใน 5 โรคที่กล่าวมานี้

ซึ่งการดูแลผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก จัดอยู่ในกลุ่มที่มีความซับซ้อนการรักษาผู้ป่วยที่ได้รับการผ่าตัดให้มีประสิทธิภาพและประสิทธิผล จึงเป็นบทบาทของทีมสหสาขาวิชาชีพร่วมกันในการพัฒนาการดูแลอย่างต่อเนื่องโดยมีการวิเคราะห์ข้อมูลผลลัพธ์การดูแล การจัดการความรู้ เพื่อให้ได้ผลลัพธ์การดูแลที่มีประสิทธิผล เช่น ภาวะแทรกซ้อน ค่าใช้จ่าย เป็นต้น ปัจจุบันการบันทึกข้อมูลเป็นลักษณะของเอกสารประเภทกระดาษโดยมีคณะกรรมการ QIT เป็นผู้รับผิดชอบรวบรวมข้อมูลแต่ข้อมูลหลายส่วนจำเป็นต้องนับจำนวนด้วยมือ และจัดส่งโดยมายังผู้มีหน้าที่รับผิดชอบในการรวบรวมและวิเคราะห์การวิเคราะห์ข้อมูลนั้นต้องมีขั้นตอนของการลงข้อมูลในคอมพิวเตอร์เพื่อประมวลผล และส่วนหนึ่งใช้เครื่องคิดเลขซึ่งมีขั้นตอนที่ล่าช้า ดังนั้นการใช้เทคโนโลยีสารสนเทศในยุคใหม่แอพลิเคชั่น เป็นหนทางหนึ่งของการพัฒนาระบบการจัดเก็บและรวบรวมข้อมูลได้รวดเร็วและปลอดภัยกว่าการใช้ระบบเอกสารมีความสามารถในการวิเคราะห์และเชื่อมโยงกับฐานข้อมูลต่าง ๆ ได้กว้างขวางทั่วโลก เพราะอยู่บนเครือข่ายที่มีบราวเซอร์ที่ทำหน้าที่ดึงข้อมูลมาแสดงอัตโนมัติ (รสสุคนธ์ วาริทสกุล, 2560)

จากปัญหาและความสำคัญดังกล่าว ผู้จัดทำในบทบาทผู้ปฏิบัติการพยาบาลขั้นสูง ซึ่งมีหน้าที่หนึ่งในการเป็นผู้นำการเปลี่ยนแปลงและพัฒนาระบบการดูแลผู้ป่วยประเมินผลกระบวนการและผลลัพธ์ของการดูแลกลุ่มผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก กำหนดตัวชี้วัด

และผลลัพธ์ รวบรวมสถิติข้อมูลผลลัพธ์ทางการพยาบาลและผลการดำเนินงานนำมาวิเคราะห์วางแผนปรับปรุงระบบการบริการโดยประเมินประสิทธิภาพประสิทธิผล ความคุ้มค่าคุ้มทุนเพื่อไปวางแผน ปรับปรุงพัฒนาระบบรวมทั้งคิดค้นนวัตกรรมที่จะทำให้เกิดผลสำเร็จของการดูแลผู้ป่วยจึงสนใจจะพัฒนาระบบการจัดจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนักโดยบุคลากรทางการพยาบาล เพื่อความรวดเร็ว ถูกต้องทันสมัยและประหยัดทรัพยากรจากการลดขั้นตอนการปฏิบัติงาน ทั้งยังสนองนโยบายระดับองค์กรในประเด็นการลดการใช้ทรัพยากรและตอบสนองนโยบายระดับประเทศในประเด็นการใช้เทคโนโลยีเพื่อพัฒนางานด้านการสาธารณสุข (Paul, 1998) จึงจัดทำคู่มือการจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนักและนำไปใช้ให้เกิดประโยชน์สูงสุด

วัตถุประสงค์

1. เพื่อใช้เป็นแนวทางสำหรับพยาบาลวิชาชีพในการจัดเก็บและวิเคราะห์ข้อมูลของผู้ป่วยโรคลำไส้ใหญ่และทวารหนักโดยใช้เว็บแอพลิเคชั่น
2. เพื่อลดระยะเวลาในการส่งต่อข้อมูล และการใช้ทรัพยากร

ประโยชน์ที่คาดว่าจะได้รับ

1. พยาบาลสามารถปฏิบัติการลงข้อมูลและจัดส่งได้สะดวก รวดเร็ว และมีประสิทธิภาพ
2. พยาบาลในหน่วยสามารถเข้าถึงข้อมูลได้อย่างมีประสิทธิภาพ
3. ใช้ประกอบการนิเทศพยาบาลวิชาชีพในการบันทึกข้อมูลได้ถูกต้อง ครบถ้วน

ขอบเขตของคู่มือปฏิบัติงาน

คู่มือการปฏิบัติงานฉบับนี้ใช้สำหรับพยาบาลที่รับผิดชอบดูแลผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก โดยมีเนื้อหาเกี่ยวกับแนวทางการปฏิบัติงาน อธิบายถึงขั้นตอน และรูปแบบในการลงข้อมูลตัวชี้วัด ซึ่งเป็นกระบวนการให้บุคลากรมีส่วนร่วมกันการพัฒนาระบบงาน เพื่อให้รวดเร็ว เท่าเทียม ลดระยะเวลา ทรัพยากร และสอดคล้องกับความต้องการของหน่วยงาน

คำจำกัดความเบื้องต้น

พยาบาลวิชาชีพ หมายถึง พยาบาลวิชาชีพที่ปฏิบัติงานในคณะกรรมการพัฒนาคุณภาพศัลยกรรมลำไส้ใหญ่และทวารหนัก (Quality Improvement Team : QIT)

กลุ่มโรคลำไส้ใหญ่และทวารหนัก หมายถึง ผู้ป่วยที่ได้รับการวินิจฉัยจากทีมแพทย์ว่าเป็นโรคเกี่ยวกับลำไส้ใหญ่และทวารหนัก และได้รับการรักษาด้วยการผ่าตัดในโรงพยาบาลวชิรพยาบาล

แอพลิเคชั่น หมายถึง โปรแกรม google form ซึ่งเป็นระบบปฏิบัติการที่คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช ได้จัดบริการแก่บุคลากรในสังกัด สำหรับใช้และเข้าถึงบริการของเว็บแอพลิเคชั่นนี้ฟรี สามารถส่งข้อมูลอย่างปลอดภัยเชื่อถือได้ และได้รับการสร้างแฟ้มสำหรับเก็บข้อมูลที่ต้องการ การจำกัดสิทธิ์เข้าถึง และกำหนดความปลอดภัยของข้อมูลต่าง ๆ ภายในแฟ้มบันทึกข้อมูลโดยคณะกรรมการพัฒนาคุณภาพศัลยกรรมลำไส้ใหญ่และทวารหนัก

ตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาล หมายถึง ข้อมูลที่บอกถึงความสำเร็จของกระบวนการดำเนินงานดูแลรักษาผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก และเป็นข้อมูลที่เกิดขึ้นกับผู้ป่วยที่มารับบริการหลังจากได้รับบริการพยาบาลโดยตรง ได้แก่ 1) อัตราผู้ป่วยที่ได้รับการผ่าตัด colorectal แบบ elective case ที่มีแผลติดเชื้อ 2) อัตราผู้ป่วย colorectal disease ที่ได้รับการผ่าตัดซ้ำในการ admission เดียวกัน 3) อัตราผู้ป่วยที่รอการผ่าตัดภายหลังได้รับการยืนยันผลชิ้นเนื้อเกิน 30 วัน โดยที่ไม่มีข้อห้ามในการผ่าตัดและไม่ต้องได้รับการฉายแสงก่อนผ่าตัด 4) อัตราผู้ป่วยที่ได้รับการพักฟื้นในโรงพยาบาลหลังผ่าตัดลำไส้แบบส่องกล้องเกิน 10 วัน 5) อัตราการแก้ไข colostomy ใน admission ครั้งเดียวกัน 6) อัตราแผลผ่าตัดติดเชื้อ 7) อัตราติดเชื้อระบบทางเดินปัสสาวะ 8) อัตราเกิดภาวะเส้นเลือดดำอุดตัน DVT 9) อัตราเกิดภาวะลำไส้รั่ว 10) ภาวะทุพโภชนาการของผู้ป่วยระดับรุนแรงระดับ 3 และระดับ 4 11) คุณภาพชีวิตของผู้ป่วยมะเร็งลำไส้ใหญ่ 1 ปี หลังได้รับการรักษาโดยการผ่าตัด 12) อัตราการเกิดภาวะ colostomy retraction 13) อัตราการเกิดภาวะ colostomy bleeding ที่จำเป็นต้องผ่าตัด 14) อัตราการเกิดภาวะ colostomy necrosis 15) อัตราการเกิดภาวะ colostomy infection 16) อัตราการเกิดภาวะ colostomy mucocutaneous fistular

บทที่ 2
โครงสร้างและหน้าที่ความรับผิดชอบ

บทบาทหน้าที่ความรับผิดชอบของตำแหน่ง

การปฏิบัติการพยาบาลขั้นสูง หมายถึง การกระทำการพยาบาลโดยตรงแก่ผู้ใช้บริการกลุ่มเป้าหมาย หรือกลุ่มโรคที่มีปัญหาซับซ้อน ซึ่งต้องอาศัยความชำนาญและทักษะการพยาบาลผู้ปฏิบัติการพยาบาลขั้นสูง ในการจัดการรายกรณีหรือใช้วิธีการอื่น ๆ จัดระบบการดูแลผู้ป่วยเฉพาะกลุ่ม หรือเฉพาะโรคที่มีประสิทธิภาพ ให้เหตุผลและตัดสินใจเชิงจริยธรรม โดยบูรณาการหลักฐานเชิงประจักษ์ ผลการวิจัย ความรู้ทฤษฎีการพยาบาลและทฤษฎีอื่น ๆ ที่เป็นปัจจุบัน มุ่งเน้นผลลัพธ์ทั้งระยะสั้นและระยะยาว พัฒนานวัตกรรมและกระบวนการการดูแลในกลุ่มผู้ใช้บริการกลุ่มเป้าหมาย หรือกลุ่มเฉพาะโรคอย่างต่อเนื่อง และเป็นที่ปรึกษาให้กับผู้ร่วมงานในการพัฒนาความรู้และทักษะงานเชิงวิชาชีพตลอดจนติดตามประเมินคุณภาพการจัดการผลลัพธ์โดยใช้กระบวนการวิจัยเชิงประเมินผลในการดูแลใช้บริการกลุ่มเป้าหมาย ซึ่งเป็นกลุ่มผู้ป่วยเฉพาะโรคที่มีปัญหาซับซ้อน

หน้าที่ความรับผิดชอบหลักของตำแหน่งผู้ปฏิบัติการพยาบาลขั้นสูง กลุ่มโรคลำไส้ใหญ่และทวารหนัก

1. พัฒนา จัดการ และกำกับระบบการดูแลผู้ป่วยกลุ่มโรคลำไส้ใหญ่และทวารหนักเพื่อการรักษาพยาบาลให้มีประสิทธิภาพตามมาตรฐานต่อเนื่องยั่งยืน

2. ปฏิบัติการพยาบาลแก่ผู้ป่วยในกลุ่มโรคลำไส้ใหญ่และทวารหนักที่มีปัญหาและความต้องการการดูแลที่ซับซ้อน โดยประเมินปัญหาและความต้องการของผู้ป่วยโรคลำไส้ใหญ่และทวารหนักอย่างครบถ้วนตามมาตรฐานการดูแล เพื่อนำไปสู่การวางแผนการพยาบาล ให้การวินิจฉัยทางการพยาบาล และให้การพยาบาลแบบองค์รวม สามารถประเมินคาดการณ์วิเคราะห์ ป้องกันและจัดการภาวะแทรกซ้อน รวมทั้งประเมินผลการพยาบาล ซึ่งการปฏิบัติการพยาบาลนี้ต้องดำเนินการอย่างถูกต้องตามหลักวิชาการและใช้หลักฐานเชิงประจักษ์เพื่อให้เกิดการดูแลผู้ป่วยที่มีประสิทธิภาพสูงสุดอย่างต่อเนื่อง

3. ประสานงานร่วมมือระหว่างสหสาขาวิชาชีพเพื่อตอบสนองความต้องการด้านสุขภาพของผู้ป่วยโรคลำไส้ใหญ่และทวารหนักได้อย่างครอบคลุม โดยใช้ข้อมูลที่เป็นผลจากการดูแลผู้ป่วยมาประกอบการตัดสินใจแก้ปัญหาร่วมกับทีมการพยาบาลและทีมสุขภาพอื่น ๆ เพื่อหาทางเลือกที่ปฏิบัติได้ดีที่สุด โดยอาศัยความรู้ทักษะ ประสบการณ์ทางด้านการพยาบาลเพื่อให้การบริการมีประสิทธิภาพ

4. เป็นพี่เลี้ยง สอน ฝึกทักษะในการปรับเปลี่ยนวิถีชีวิตของผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก เพื่อให้เกิดการปรับเปลี่ยนวิถีชีวิตที่มีภาวะสุขภาพดีขึ้น รวมถึงเป็นพี่เลี้ยง สอน และฝึกทักษะด้านการดูแลผู้ป่วยโรคลำไส้ใหญ่และทวารหนักให้แก่พยาบาลวิชาชีพ และสหสาขาวิชาชีพ

5. เป็นที่ปรึกษาให้แก่บุคลากรในทีมสุขภาพ กรณีผู้ป่วยโรคลำไส้ใหญ่และทวารหนักมีปัญหาซับซ้อนที่ต้องการความชำนาญหรือความสามารถพิเศษในการตัดสินใจ และเป็นที่ปรึกษาด้านวิชาการพยาบาลเกี่ยวกับการดูแลแผลและออสโตมีแก่พยาบาลวิชาชีพที่เข้ามาฝึกงานในหน่วยต่าง ๆ ของโรงพยาบาล และเป็นผู้ให้คำปรึกษาผู้ป่วยโรคลำไส้ใหญ่และทวารหนักเมื่อกลับไปอยู่บ้าน อาการ/อาการแสดง ที่ต้องรีบมาโรงพยาบาลรวมถึงการแก้ไขปัญหาเฉพาะหน้าเมื่อมีภาวะแทรกซ้อนเกิดขึ้น

6. เป็นผู้นำการเปลี่ยนแปลง สนับสนุนและประยุกต์วิธีการปฏิบัติการพยาบาลให้มีประสิทธิภาพ เหมาะสม ทันสมัยต่อความก้าวหน้าทางการแพทย์ และการพยาบาลสมัยใหม่

7. ปฏิบัติการพยาบาลที่ต้องตัดสินใจหรือแก้ปัญหาที่ยากตามมาตรฐานวิชาชีพ โดยใช้เหตุผลทางจริยธรรม เพื่อให้ผู้ป่วยได้รับการดูแลที่ถูกต้อง เหมาะสม และปลอดภัยพร้อมประเมินผลปฏิบัติการพยาบาล

8. วิเคราะห์ สังเคราะห์งานวิจัย และนำผลการศึกษามาใช้ในการพัฒนาการปฏิบัติการพยาบาลผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก และสร้างความรู้จากการปฏิบัติการพยาบาล การวิจัยเกี่ยวกับการพยาบาลผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก โดยมีการออกแบบการวิจัยที่น่าเชื่อถือ ผลการวิจัยสามารถนำไปปรับปรุงระบบงาน และเผยแพร่แก่หน่วยงานภายในและภายนอกองค์กร

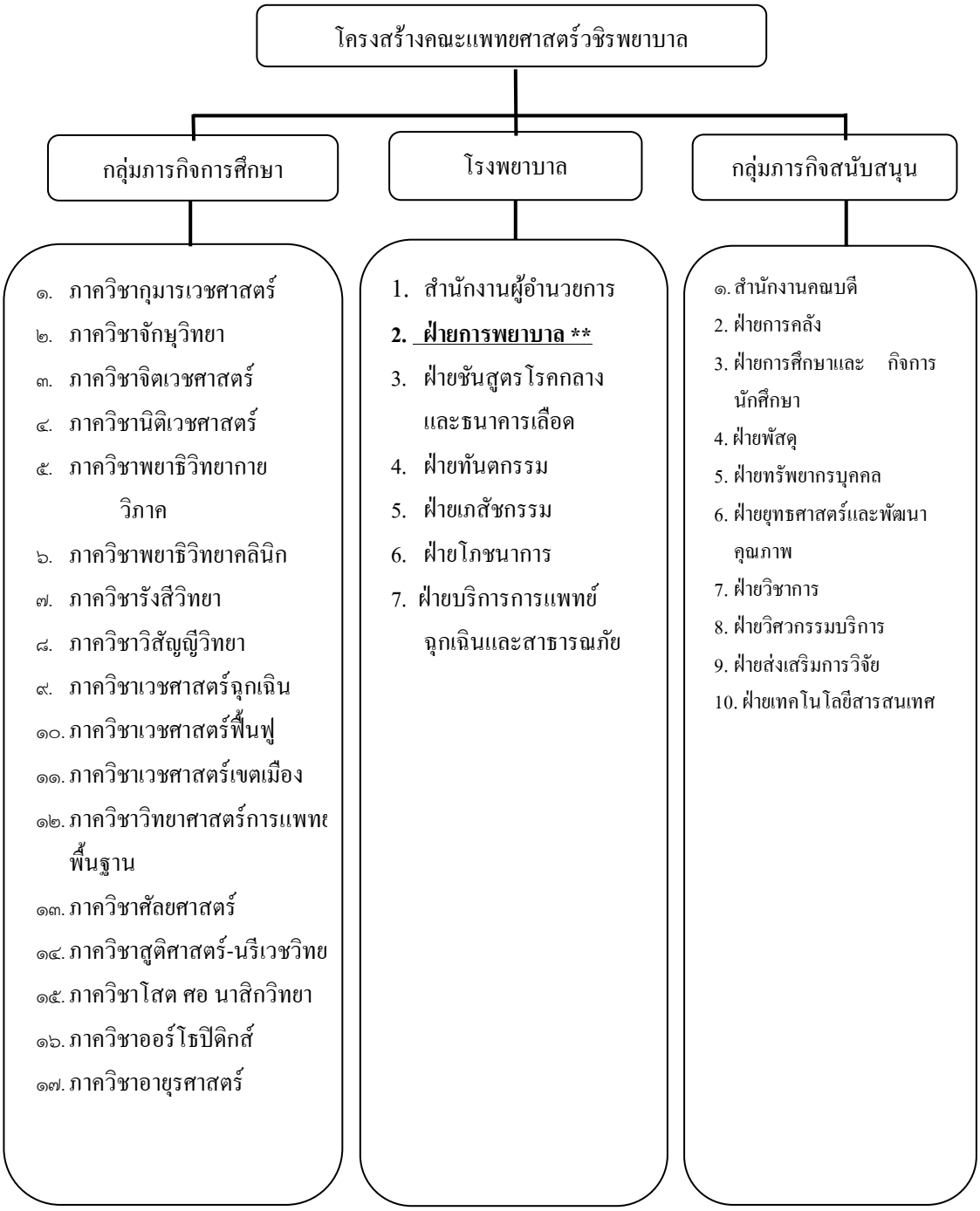
9. ประเมินผลกระบวนการและผลลัพธ์ของการดูแลกลุ่มผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก กำหนดตัวชี้วัดและผลลัพธ์ รวบรวมสถิติข้อมูลผลลัพธ์ทางการพยาบาลและผลการดำเนินงาน นำมาวิเคราะห์วางแผนปรับปรุงระบบการบริการโดยประเมินประสิทธิภาพประสิทธิผลความคุ้มค่าคุ้มทุนเพื่อไปวางแผน ปรับปรุงพัฒนาระบบ รวมทั้งคิดค้นนวัตกรรมที่จะทำให้เกิดผลสำเร็จของการดูแลผู้ป่วย

ลักษณะงานที่ปฏิบัติ

โรงพยาบาลวชิรพยาบาลมีบริบทด้านการรักษาพยาบาลผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก ผู้ป่วยส่วนใหญ่จะเข้าพักรักษาในทุกหอผู้ป่วยทางด้านศัลยกรรม จากสถิติสูงสุด 5 ลำดับ ได้แก่ หอผู้ป่วยเพชรรัตน์ 9B หอผู้ป่วยเพชรรัตน์ 10B หอผู้ป่วยเพชรรัตน์ 11B หอผู้ป่วยเพชรรัตน์ 9A และหอผู้ป่วยเพชรรัตน์ 10A จากสถิติผู้ป่วยที่เข้ารับการรักษากลุ่มโรคที่สำคัญคือโรคมะเร็งลำไส้ใหญ่

โรคมะเร็งลำไส้ตรง โรคลำไส้อุดตัน และโรคเยื่อบุผนังลำไส้โป่งพอง การผ่าตัดสูงสุด 3 ลำดับ ได้แก่การผ่าตัดลำไส้แบบเปิดช่องท้อง(explore lap) การผ่าตัดลำไส้แบบส่องกล้อง (laparoscopic colectomy) และการผ่าตัดทวารใหม่ (colostomy) มีแพทย์ผู้เชี่ยวชาญด้านศัลยกรรมลำไส้ใหญ่และทวารหนัก จำนวน 5 คน ผู้ปฏิบัติการพยาบาลขั้นสูง กลุ่มโรคลำไส้ใหญ่และทวารหนัก จำนวน 1 คน และพยาบาลวิชาชีพกรรมการทีมพัฒนาการดูแลผู้ป่วยกลุ่มโรคลำไส้ใหญ่และทวารหนัก ประจำหอผู้ป่วยละ 1 คน ร่วมให้การรักษาพยาบาลแบบทีมสหสาขาวิชาชีพ ตั้งแต่แรกรับกระทั่งติดตามหลังจำหน่ายออกจากโรงพยาบาล การดูแลผู้ป่วยอย่างต่อเนื่องและการพัฒนาคุณภาพการดูแลอย่างยั่งยืน จำเป็นต้องใช้ข้อมูลการรักษาของผู้ป่วยเป็นพื้นฐานในการวางแผนการดูแล ทีมพัฒนาคุณภาพการดูแลผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก (QIT colorectal) จึงได้กำหนดตัวชี้วัดที่ใช้ในการติดตาม ประเมินผลลัพธ์การรักษา พยาบาลประจำหอผู้ป่วยเป็นบุคลากรที่ให้บริการใกล้ชิดกับผู้ป่วยมากที่สุดจึงเป็นผู้ทำหน้าที่รวบรวมข้อมูลสุขภาพของผู้ป่วยโรคลำไส้ใหญ่และทวารหนักทุกรายที่เข้ารับการรักษา และส่งข้อมูลให้ผู้ปฏิบัติการพยาบาลขั้นสูงเป็นผู้ตรวจสอบความถูกต้อง วิเคราะห์ผลลัพธ์การรักษาพยาบาล เพื่อรายงานให้ทีมรับทราบทุกเดือน และนำเสนอในที่ประชุม QIT ประจำเดือน เพื่อร่วมกันวางแผนพัฒนาอย่างต่อเนื่อง

โครงสร้างการบริหาร



แผนภาพที่1 แสดงโครงสร้างการบริหาร คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช (คณะแพทยศาสตร์วชิรพยาบาล, 2563)

แผนภาพที่ 2 แสดงโครงสร้างการบริหาร ฝ่ายการพยาบาล คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช (ฝ่ายการพยาบาลโรงพยาบาลวชิรพยาบาล, 2563)

บทที่ 3
หลักเกณฑ์วิธีการปฏิบัติงาน

หลักเกณฑ์การปฏิบัติงาน

หลักเกณฑ์การปฏิบัติงานในการจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนัก เป็นรวบรวมข้อมูลการรักษา ตั้งแต่รับผู้ป่วยเข้ารักษาในโรงพยาบาล จนถึงติดตามหลังจำหน่ายผู้ป่วยออกจากโรงพยาบาล ประกอบด้วยข้อมูลปัญหาสุขภาพ ข้อมูลตัวชี้วัด ข้อมูลผลลัพธ์ทางการพยาบาล และข้อมูลภาวะแทรกซ้อน โดยมีการกำหนดขั้นตอนการรวบรวมอย่างเป็นระบบเพื่อความครบถ้วนและถูกต้องของการจัดเก็บข้อมูล และประยุกต์ใช้เว็บแอพลิเคชั่นเพื่อความรวดเร็วในการวิเคราะห์ข้อมูล มีหลักเกณฑ์ในการปฏิบัติงาน ดังนี้

1. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ (ฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์วชิรพยาบาล, 2561) เป็นนโยบายเพื่อให้ระบบสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาลเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง ดังนี้

1.1 การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (access control) ผู้ดูแลระบบจะต้องอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล ตามความจำเป็นต่อการใช้งานเท่านั้น และต้องกำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น อ่านอย่างเดียว ป้อนข้อมูล และแก้ไข เป็นต้น และแบ่งประเภทของข้อมูล จัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล เพื่อรักษาความปลอดภัยต่อเอกสารที่สำคัญไว้

1.2 การบริหารจัดการเข้าถึงของผู้ใช้งาน (user access management) ผู้ดูแลระบบต้องตรวจสอบสิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และทบทวนสิทธิ์การใช้งานอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

1.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) ผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่ายให้ผู้อื่นล่วงรู้รหัสผ่าน (password) และไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่ โดยต้องใช้วิธีการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล

1.4 การบริหารจัดการสินทรัพย์ (assets management) ผู้ใช้งานต้องไม่คัดลอกสำเนาแฟ้มข้อมูลก่อนได้รับอนุญาต และต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูลก่อนกำจัดอุปกรณ์ดังกล่าว เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ เช่น กระดาษ ทำลายด้วยเครื่องหั่นทำลายเอกสาร และ flash drive/hard disk ทำลายด้วยการทุบหรือบดให้เสียหาย เป็นต้น

1.5 การควบคุมการเข้าถึงเครือข่าย (network access control) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ มีการกำหนดการเชื่อมต่อกับระบบเครือข่ายที่ชัดเจนและต้องทบทวนการกำหนดค่า parameter ต่าง ๆ เช่น IP address เป็นต้น อย่างน้อยปีละ 1 ครั้ง โดยการเปลี่ยนแปลงค่าต่าง ๆ ต้องแจ้งบุคคลที่เกี่ยวข้องทราบทุกครั้ง

1.6 การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) ผู้ใช้งานต้องตั้งค่าถนอมหน้าจอ (screen saver) เพื่อทำการล๊อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน (password) และผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของตนในการเข้าถึงเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

1.7 การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (application and information access control) ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ แอพพลิเคชั่น (application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติหน้าที่ เพื่อใช้ตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล และยกเลิกรหัสผ่านเมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง

1.8 การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (software licensing and intellectual propertyand preventing malware) ผู้ใช้งานซอฟต์แวร์สามารถขอใช้งานได้ตามหน้าที่ความจำเป็น ห้ามทำการถอดถอน เปลี่ยนแปลง แก้ไขหรือสำเนาเพื่อนำไปใช้งานที่อื่น ๆ สำหรับข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆที่เป็นสินทรัพย์ของหน่วยงาน ผู้ใช้งานห้ามทำสำเนา เปลี่ยนแปลง ลบทิ้ง ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงาน และห้ามทำการติดตั้งซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ ผู้ใช้งานต้องทำการปรับปรุงข้อมูลและระบบปฏิบัติการ (update patch) ให้ใหม่เสมอ รวมถึงต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา หากพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

1.9 การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ผู้ใช้งานต้องผ่านการพิสูจน์ตัวตน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น รวมถึงต้องมีการตรวจสอบว่าอุปกรณ์ซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

1.10 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless lan access control) ผู้ใช้งานที่เข้าถึงระบบเครือข่ายไร้สาย ต้องทำการลงทะเบียนและได้รับอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

1.11 การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (firewall control) ผู้ใช้งานอินเตอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (login) ก่อนการใช้งานทุกครั้ง

1.12 การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-mail) ผู้ใช้งานต้องยื่นคำขอกับเจ้าหน้าที่หน่วยงานเพื่อขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ และไม่บันทึกรหัสผ่าน (password) ไว้ในระบบคอมพิวเตอร์ เมื่อใช้งานระบบเสร็จสิ้นต้องลงบันทึกออก (logout) ทุกครั้ง และห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่านหรือส่งข้อความยกเว้นได้รับการยินยอมจากเจ้าของผู้ใช้งาน

1.13 การควบคุมการใช้อินเตอร์เน็ต (internet) ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์ (web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และใช้งานผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น proxy, firewall, IPS-IDS เป็นต้น เมื่อใช้งานระบบอินเตอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการใช้งานโดยบุคคลอื่น ๆ

1.14 การใช้เครื่องคอมพิวเตอร์ส่วนบุคคล ผู้ใช้งานมีหน้าที่รับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ และต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (E-mail) ก่อนใช้งาน

1.15 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา โปรแกรมที่ได้ถูกติดตั้งบนเครื่องคอมพิวเตอร์ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดี และทำการสำรองข้อมูลไว้ในสถานที่ที่เหมาะสม

1.16 การตรวจจับการบุกรุก ต้องมีการตรวจสอบพฤติกรรมการใช้งาน การบันทึกปริมาณข้อมูลเข้าใช้เครือข่ายเป็นประจำ

1.17 การติดตั้งและกำหนดค่าของระบบ บริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ กำหนดชื่อผู้ใช้งาน และกำหนดค่าโปรแกรมฐานข้อมูลให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง

1.18 การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log) จัดเก็บข้อมูลไว้ในสื่อที่สามารถรักษาความครบถ้วน ถูกต้อง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และมีการบันทึกการปฏิบัติงานของผู้ใช้งานเพื่อใช้ตรวจสอบ รวมถึงต้องมีวิธีจำกัดสิทธิ์การเข้าถึงบันทึกให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

วิธีการปฏิบัติงาน

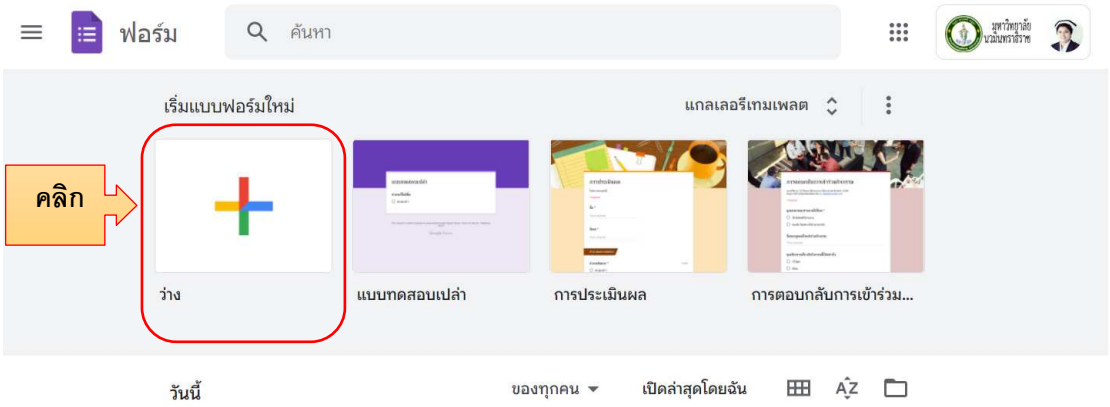
การจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนัก เป็นการรวบรวม ตรวจสอบ และวิเคราะห์ข้อมูลผลลัพธ์ทางการพยาบาลผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก โดยมีเป้าหมายเพื่อให้การจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพ สามารถนำผลการวิเคราะห์ไปวางแผนการดูแลรักษาต่อเนื่อง ซึ่งเป็นสิ่งสำคัญในการพัฒนาการพยาบาล หรือการดูแลรักษาได้อย่างถูกต้อง การจัดการข้อมูลตัวชี้วัดผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนัก มีวิธีปฏิบัติงาน ดังนี้

1. รวบรวมข้อมูลตัวชี้วัดผลลัพธ์ทางการพยาบาลทั้งหมดที่คณะกรรมการพัฒนาคุณภาพผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก (QIT colorectal) กำหนดไว้

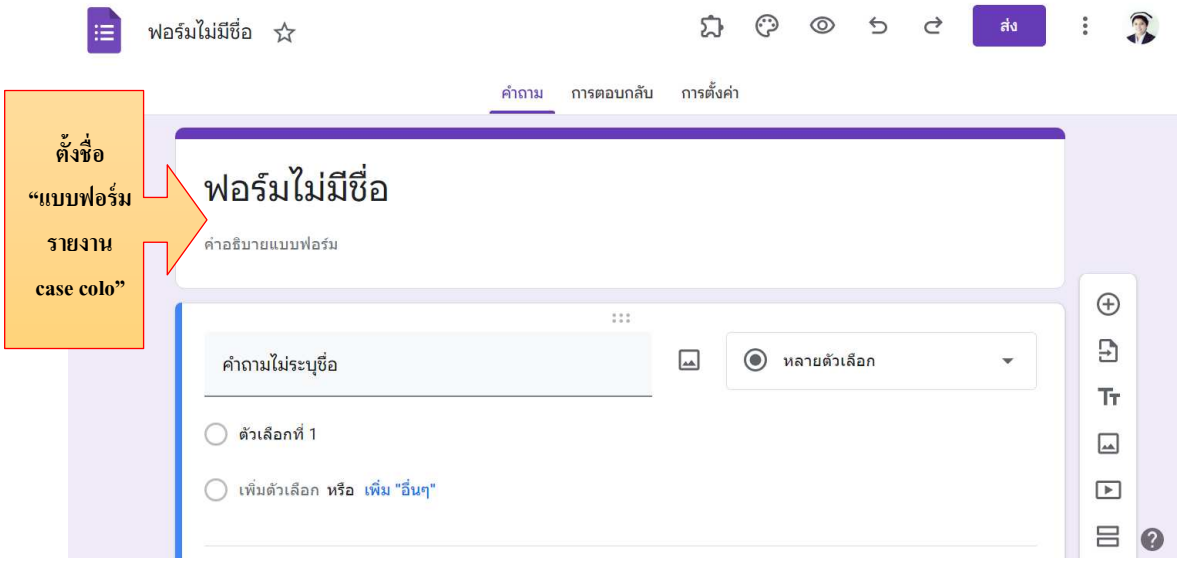
2. จัดทำเอกสารในรูปแบบไฟล์ (word) ของตัวชี้วัดได้แก่ 1) อัตราผู้ป่วยที่ได้รับการผ่าตัด colorectal แบบ elective case ที่มีแผลติดเชื้อ 2) อัตราผู้ป่วย colorectal disease ที่ได้รับการผ่าตัดซ้ำในการ admission เดียวกัน 3) อัตราผู้ป่วยที่รอการผ่าตัดภายหลังได้รับการยืนยันผลชิ้นเนื้อเกิน 30 วัน โดยที่ไม่มีข้อห้ามในการผ่าตัดและไม่ต้องได้รับการฉายแสงก่อนผ่าตัด 4) อัตราผู้ป่วยที่ได้รับการพักฟื้นในโรงพยาบาลหลังผ่าตัดลำไส้แบบส่องกล้องเกิน 10 วัน 5) อัตราการแก้ไข colostomy ใน admission ครั้งเดียวกัน 6) อัตราแผลผ่าตัดติดเชื้อ 7) อัตราติดเชื้อระบบทางเดินปัสสาวะ 8) อัตราเกิดภาวะเส้นเลือดดำอุดตัน DVT 9) อัตราเกิดภาวะลำไส้รั่ว 10) ภาวะทุพโภชนาการของผู้ป่วยระดับรุนแรงระดับ 3 และระดับ 4 11) คุณภาพชีวิตของผู้ป่วยมะเร็งลำไส้ใหญ่ 1 ปี หลังได้รับการรักษาโดยการผ่าตัด 12) อัตราการเกิดภาวะ colostomy retraction 13) อัตราการเกิดภาวะ colostomy bleeding ที่จำเป็นต้องผ่าตัด 14) อัตราการเกิดภาวะ colostomy necrosis15) อัตราการเกิดภาวะ colostomy infection 16) อัตราการเกิดภาวะ colostomy mucocutaneous fistula เพื่อนำลง “แบบฟอร์มรายงาน case colo”

3. สร้าง google form โดย เข้าสู่ระบบ Gmail ที่เว็บไซต์https://www.google.com/gmail/ (หรือพิมพ์ค้นหาใน Google ว่า “Gmail”) และเข้าไปที่เว็บไซต์ https://goo.gl/hTn9FK (หรือพิมพ์ค้นหาใน Google ว่า “Google Form”) และคลิก ไปที่ Google ฟอร์ม จากนั้นลงข้อมูล ดังนี้

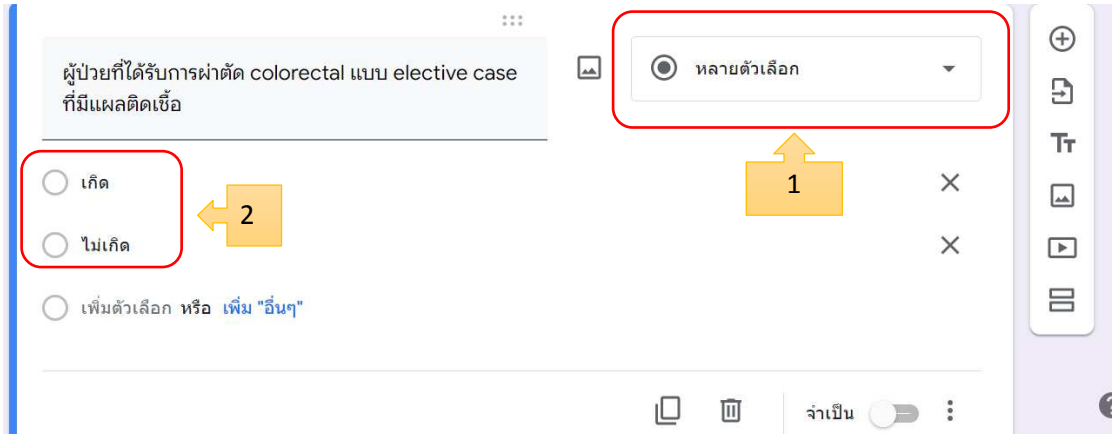
3.1 คลิก “ว่าง” เพื่อเริ่มแบบฟอร์มใหม่



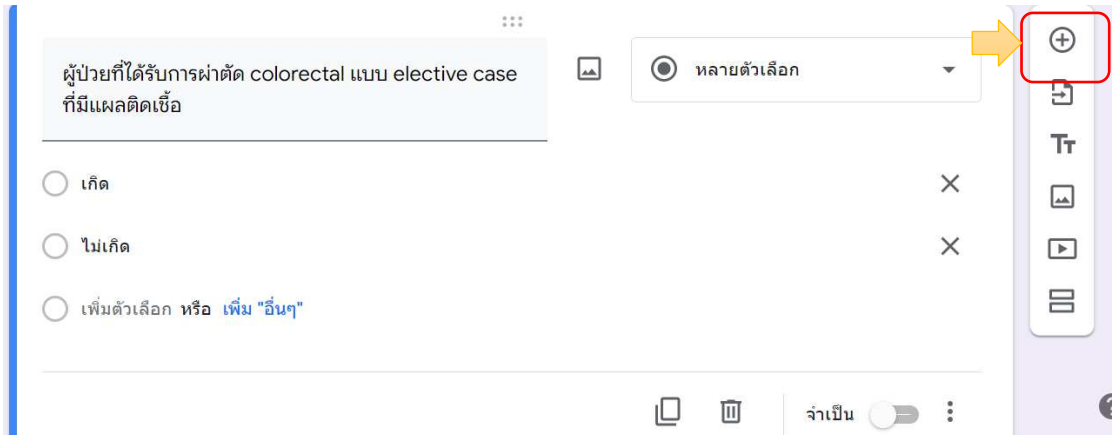
3.2 หลังจากเข้าสู่หน้าต่างแบบฟอร์มว่างแล้ว ให้ตั้งชื่อแบบฟอร์ม และใส่คำอธิบาย



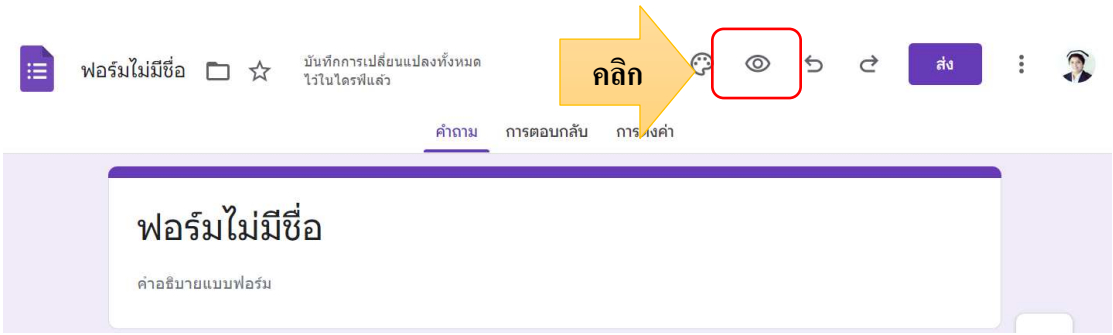
3.4 กำหนดลักษณะคำตอบแบบ หลายตัวเลือก (หมายเลข 1)และบันทึกข้อความทางเลือก (หมายเลข 2)



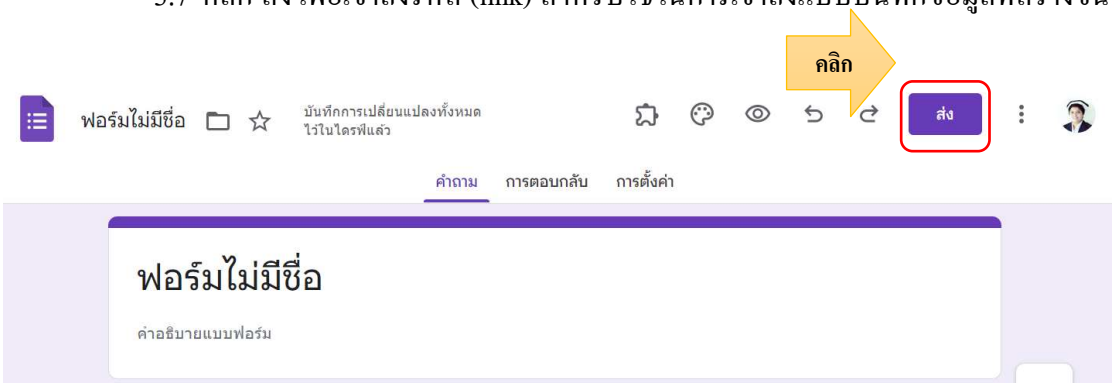
3.5 คลิกเพื่อเพิ่มคำถามข้อถัดไป กระทั่งบันทึกตัวชี้วัดครบตามต้องการ



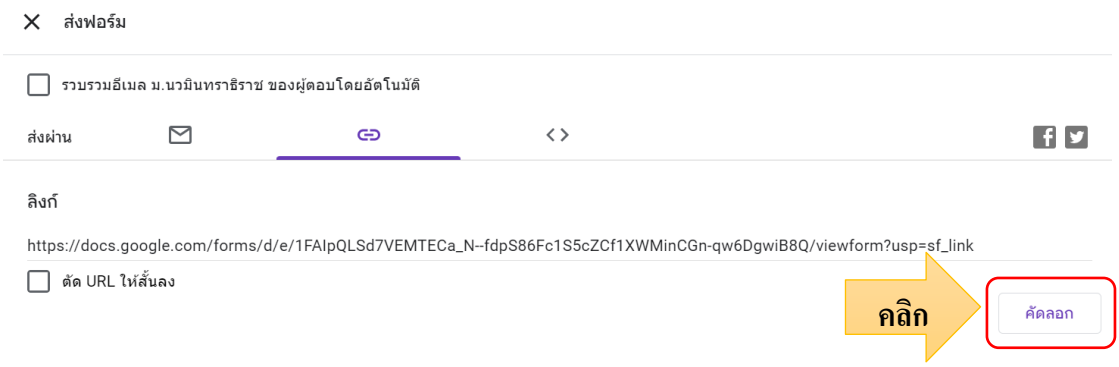
3.6 คลิก เพื่อดูการแสดงผลและการใช้งานแบบฟอร์มเสมือนจริงในมุมมองของผู้ตอบแบบฟอร์ม โดยสามารถคลิก  เพื่อกลับมาแก้ไขแบบฟอร์ม



3.7 คลิก ส่ง เพื่อเข้าถึงรหัส (link) สำหรับใช้ในการเข้าถึงแบบบันทึกข้อมูลที่สร้างขึ้น



3.8 คลิก “คัดลอก” เพื่อนำรหัส (link) ส่งให้คณะกรรมการสำหรับลงข้อมูลตัวชี้วัดที่กำหนด



4. นำรหัส (link) ส่งให้คณะกรรมการพัฒนาคุณภาพผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก เพื่อใช้ในการจัดส่งข้อมูลตามหน้าที่ที่ได้รับมอบหมาย และจำกัดสิทธิ์การเข้าถึงเมื่อคณะกรรมการมีการโอนย้าย ลาออกจากหน่วยงาน

5. อธิบายความหมายของตัวชี้วัดต่าง ๆ ให้กับคณะกรรมการพัฒนาคุณภาพผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก เพื่อสร้างความเข้าใจที่ถูกต้อง ก่อนการบันทึกข้อมูลของตัวชี้วัดทุกตัว และฝึกปฏิบัติการใช้รหัส (link) เพื่อเข้าสู่ไฟล์แบบบันทึกข้อมูลตามเนื้อหาในคู่มือการจัดเก็บและบันทึกข้อมูลตัวชี้วัด

6. กำหนดให้พยาบาลผู้ปฏิบัติการพยาบาลขั้นสูง กลุ่มโรคลำไส้ใหญ่และทวารหนัก หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติงานแทน เป็นผู้ติดตาม และตรวจสอบความถูกต้อง (re-check) การลงบันทึกข้อมูลตัวชี้วัดทุกเดือน ด้วยการทบทวนเวชระเบียนย้อนหลังของผู้ป่วยโรคลำไส้ใหญ่และทวารหนักทุกราย ก่อนนำเข้าสู่การรวบรวม วิเคราะห์ข้อมูล และจัดทำแบบรายงานผลลัพธ์ฯ เพื่อนำเสนอต่อคณะกรรมการพัฒนาคุณภาพผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก ในที่ประชุมประจำเดือนและรวบรวมเป็นข้อมูลประจำปีเพื่อใช้ในการวางแผนการพัฒนาระบบงานอย่างต่อเนื่อง รวมถึงการขอรับรองมาตรฐานเฉพาะโรคมะเร็งลำไส้ใหญ่และลำไส้ตรง (Disease Specific Certification: DSC) ของสถาบันรับรองคุณภาพสถานพยาบาล

เงื่อนไข/ข้อสังเกต/ข้อควรระวัง/สิ่งที่ควรคำนึงถึงในการปฏิบัติงาน

การจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่นในกลุ่มผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก สิ่งสำคัญที่สุดคือการรวบรวมข้อมูลผู้ป่วยโรคลำไส้ใหญ่และทวารหนักที่ครบถ้วน ถูกต้อง และลงรหัสเข้าไฟล์ (link) บันทึกในเว็บแอพลิเคชั่นภายในวันที่ 30 ของทุกเดือน ซึ่งสิ่งที่ควรคำนึงถึงในการปฏิบัติงานคือการประเมินผู้ป่วยให้ถูกต้อง และบันทึกข้อมูลผ่านระบบที่มีความปลอดภัย เกี่ยวกับ

1. การเตรียมข้อมูล คณะกรรมการพัฒนาคุณภาพผู้ป่วยโรคลำไส้ใหญ่และทวารหนักที่ได้รับมอบหมายให้บันทึกข้อมูล ต้องได้รับการสอน และแนะนำการเลือกข้อมูลการรักษาพยาบาล รวมถึงตัวชี้วัดผลลัพธ์ทางการพยาบาลที่กำหนด โดยข้อมูลต่าง ๆ ต้องได้รับการยืนยันจากแพทย์เจ้าของไข้ร่วมกับมีการบันทึกในแฟ้มประวัติ

2. ข้อมูลภาวะแทรกซ้อนต่าง ๆ ของผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก ต้องมีผลตรวจทางห้องปฏิบัติการยืนยัน ร่วมกับได้รับการประเมินและวินิจฉัยจากแพทย์เจ้าของไข้

3. การบันทึกข้อมูล ต้องปฏิบัติการผ่านเครื่องคอมพิวเตอร์ที่โรงพยาบาลจัดเตรียมให้ประจำหน่วยงาน ใช้สัญญาณอินเตอร์เน็ตของมหาวิทยาลัยนวมินทราธิราชผ่าน (LAN) และลงชื่อเข้า

ใช้ google form ผ่านชื่อบัญชีผู้ใช้งาน (username) ของจดหมายอิเล็กทรอนิกส์ที่ได้รับอนุญาตจากมหาวิทยาลัยนวมินทราธิราช (E-mail@nmu.ac.th) เท่านั้น โดยข้อมูลต้องเป็นข้อมูลที่ถูกต้องตามอาการของผู้ป่วย ตรงกับบันทึกในเวชระเบียน

แนวคิดที่ใช้ในการจัดทำคู่มือการปฏิบัติงาน

ผู้จัดทำใช้แนวปฏิบัติการพยาบาลผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ ในการจัดทำคู่มือปฏิบัติการ ดังนี้

1. แนวปฏิบัติการพยาบาลผู้ป่วยโรคลำไส้ใหญ่และทวารหนัก เป็นแนวทางในการให้การพยาบาลผู้ป่วยตั้งแต่เข้ารับการรักษาจนจำหน่ายกลับบ้าน (อรอนงค์ทัพสุวรรณ์, 2557)

1.1 การพยาบาลระยะก่อนผ่าตัดรักษาโรคลำไส้ใหญ่และทวารหนัก

1.2 การพยาบาลระยะหลังผ่าตัดโรคลำไส้ใหญ่และทวารหนัก

2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์ (ฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์วชิรพยาบาล, 2561)

2.1 การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (access control)

2.2 การบริหารจัดการเข้าถึงของผู้ใช้งาน (user access management)

2.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

2.4 การบริหารจัดการสินทรัพย์ (assets management)

2.5 การควบคุมการเข้าถึงเครือข่าย (network access control)

2.6 การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

2.7 การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (application and information access control)

2.8 การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (software licensing and intellectual propertyand preventing malware)

2.9 การปฏิบัติงานจากภายนอกสำนักงาน (teleworking)

2.10 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless Lan access control)

2.11 การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (firewall control)

2.12 การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)

2.13 การควบคุมการใช้อินเตอร์เน็ต (internet)

2.14 การใช้เครื่องคอมพิวเตอร์ส่วนบุคคล

2.15 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

2.16 การตรวจจับการบุกรุก

2.17 การติดตั้งและกำหนดค่าของระบบ

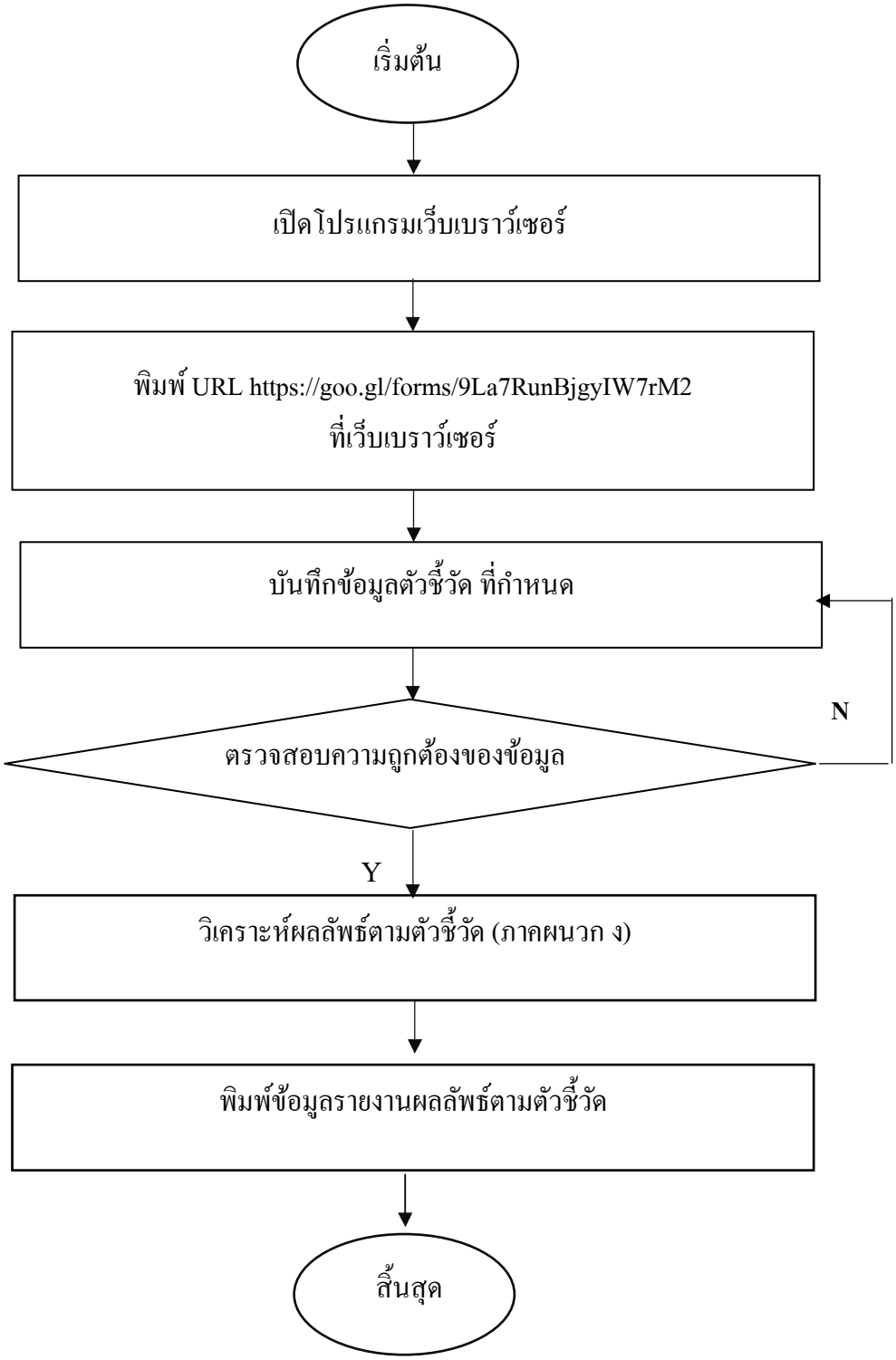
2.18 การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log)

บทที่ 4
เทคนิคการปฏิบัติงาน

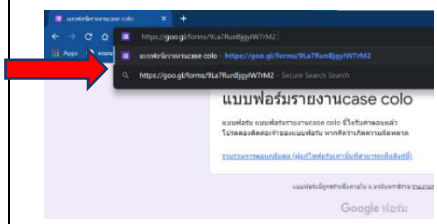
แผนกลยุทธ์ในการปฏิบัติงาน

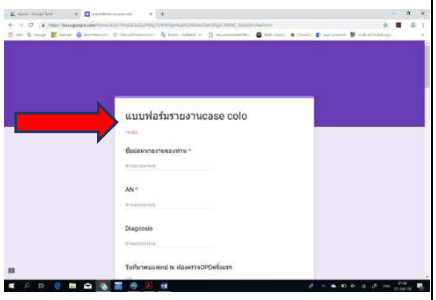
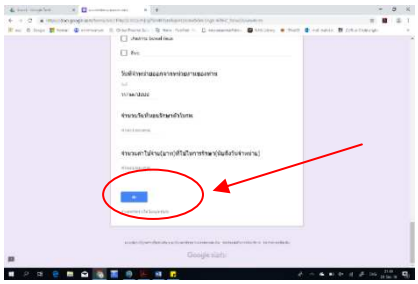
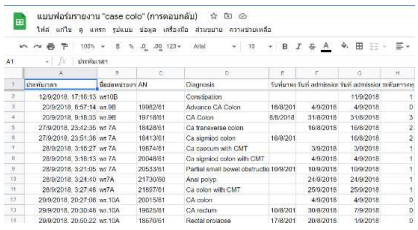
เพื่อพัฒนาระบบการจัดการข้อมูลผลลัพธ์ทางการพยาบาล ปัจจุบันพยาบาลสามารถสร้างฐานข้อมูลสำหรับใช้รวบรวมข้อมูล และจัดเก็บอย่างเป็นระบบมีการประยุกต์ใช้แอปพลิเคชั่นหรือโปรแกรมคอมพิวเตอร์พื้นฐาน เช่น Excel, Access, SPSS และ Word ที่สามารถสร้างฐานข้อมูลและวิเคราะห์ข้อมูลง่ายขึ้น สามารถลดระยะเวลาในการจัดการข้อมูล โดยเฉพาะการเก็บรวบรวมข้อมูลในลักษณะการติดตามผู้ป่วยในหลายหน่วยงาน และการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน สามารถลดความซ้ำซ้อน และลดระยะเวลาในการสื่อสาร เนื่องจากองค์กรสนับสนุนเครือข่ายอินเตอร์เน็ตที่ครอบคลุมบุคลากรทุกคนสามารถเข้าถึงโปรแกรมออนไลน์ได้สะดวก ผ่านระบบที่องค์กรสนับสนุนให้ใช้งานร่วมกัน ได้แก่ G Suite หรือชื่อเดิม คือ google apps เป็นบริการ application บน googleที่สามารถใช้งานได้หลากหลาย ไม่ว่าจะเป็นการใช้งานอีเมล (@nmu)การแชร์ไฟล์หรือเอกสารที่สามารถกระทำได้อย่างรวดเร็ว นอกจากนี้ยังสามารถทำงานแบบ real time ได้เช่นการนำ google sheet, google doc, google form มาใช้ในการส่งข้อมูล เป็นต้น การประยุกต์ใช้แอบพลิเคชั่น และการพัฒนาการจัดการข้อมูลนี้จึงสอดคล้องกับแผนยุทธศาสตร์ของคณะแพทยศาสตร์วชิรพยาบาล A-E-I-O-U ปี พ.ศ.2562-2565 ที่ผู้บริหารกำหนดไว้ ในประเด็น O:Organizational Strength องค์กรเข้มแข็งในยุคดิจิทัลให้มีความยั่งยืน และยังสะท้อนความก้าวหน้าทางเทคโนโลยีของวิชาชีพพยาบาล

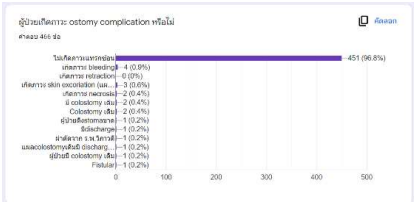
ขั้นตอนการปฏิบัติงาน

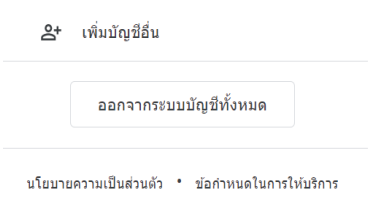


ขั้นตอนการปฏิบัติงานตามกระบวนการ

ลำดับที่	ผังกระบวนการ	ระยะเวลา (นาที)	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
1	เปิดโปรแกรมเว็บบราว์เซอร์	1-2	เปิดโปรแกรมเว็บบราว์เซอร์ Google Chrome โดยการคลิกที่รูปบนหน้าจอคอมพิวเตอร์ 	พยาบาลวิชาชีพ/หัวหน้าทีม	คอมพิวเตอร์หน่วยงาน
2	พิมพ์URL https://goo.gl/forms/9La7RunBjgyIW7rM2 ที่เว็บเบราว์เซอร์	2-5	พิมพ์ข้อมูลที่อยู่ของไฟล์ออนไลน์ในช่องที่อยู่เว็บ ดังนี้ https://goo.gl/forms/9La7RunBjgyIW7rM2 จากนั้นจะพบหน้า“แบบฟอร์มรายงาน case colo” 	พยาบาลวิชาชีพ/หัวหน้าทีม	คอมพิวเตอร์หน่วยงาน

ลำดับที่	ผังกระบวนการ	ระยะเวลา (นาที)	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
3	บันทึกข้อมูลตัวชี้วัด ที่กำหนด	10-15	บันทึกข้อมูลที่รวบรวมไว้ลงในแบบฟอร์มและยืนยันข้อมูลโดยกด “ส่ง”เพื่อจัดเก็บข้อมูลไว้ในระบบแฟ้มข้อมูล  	พยาบาลวิชาชีพ	คอมพิวเตอร์หน่วยงาน
4	ตรวจสอบความถูกต้องของข้อมูล	30-45	ตรวจสอบความถูกต้องของข้อมูลโดยทบทวนแฟ้มประวัติ และเวชระเบียนกรณีพบข้อมูลไม่ถูกต้องจะทำการแก้ไขพร้อมลงวันที่กำกับ แต่เมื่อตรวจสอบข้อมูลถูกต้อง จะดำเนินการวิเคราะห์ข้อมูลต่อไป 	หัวหน้าทีม	คอมพิวเตอร์หน่วยงาน

ลำดับที่	ผังกระบวนการ	ระยะเวลา (นาที)	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
5	วิเคราะห์ผลลัพธ์ตามตัวชี้วัด	15-20	วิเคราะห์ผลลัพธ์ตามตัวชี้วัด (ภาคผนวก ข) ด้วยสถิติพื้นฐาน ประกอบด้วยจำนวน และร้อยละ 	หัวหน้าทีม	คอมพิวเตอร์ หน่วยงาน
6	พิมพ์ข้อมูลรายงานผลลัพธ์ตามตัวชี้วัด	15-20	จัดทำรายงานผลลัพธ์ และพิมพ์ข้อมูลในรูปแบบเอกสารภายในวันที่ 5 ของเดือนถัดไป เพื่อนำเสนอต่อคณะกรรมการในที่ประชุมคณะกรรมการพัฒนาคุณภาพศัลยกรรมลำไส้ใหญ่และทวารหนักประจำเดือน 	หัวหน้าทีม	คอมพิวเตอร์ หน่วยงาน

ลำดับที่	ผังกระบวนการ	ระยะเวลา (นาที)	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
7	สิ้นสุด	1-2	เมื่อสิ้นสุดการจัดการข้อมูลตามหน้าที่แล้ว ให้ออกจากระบบบัญชีทั้งหมดทุกครั้ง ก่อนปิดเครื่องคอมพิวเตอร์ 	พยาบาลวิชาชีพ/หัวหน้าทีม	คอมพิวเตอร์หน่วยงาน

วิธีการติดตามและประเมินผลการปฏิบัติงาน

คู่มือการจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนักนี้ เริ่มใช้ตั้งแต่วันที่ 1 มกราคม 2561ถึงวันที่ 31 ธันวาคม 2564 กำหนดให้คณะกรรมการพัฒนาคุณภาพผู้ป่วยโรคลำไส้ใหญ่และทวารหนักประจำหอผู้ป่วยได้แก่ หอผู้ป่วยเพชรรัตน์ 9B หอผู้ป่วยเพชรรัตน์ 10B หอผู้ป่วยเพชรรัตน์ 11B หอผู้ป่วยเพชรรัตน์ 9A และหอผู้ป่วยเพชรรัตน์ 10A เป็นผู้บันทึกข้อมูล ตัวชี้วัด (ภาคผนวก ข) โดยกำหนดให้ส่งข้อมูลในระบบก่อนวันที่ 30 ของทุกเดือน ผู้จัดทำคู่มือจะดำเนินการเก็บรวบรวม โดยการติดตามประเมินผลการใช้คู่มือในทีม QIT colorectal ทุก 1 เดือน โดยการประเมินด้านบุคลากร มีการเก็บข้อมูลบุคลากรโดยใช้คู่มือโดยใช้แบบประเมินผลบุคลากรในการใช้เว็บแอพลิเคชั่น (ภาคผนวก ค) ในประเด็นต่อไปนี้

1. ระยะเวลาการลงบันทึกข้อมูล หมายถึง ระยะเวลาที่บุคลากรลงข้อมูลผ่านระบบออนไลน์ครบถ้วน (หน่วยนับเป็นวัน) นับจากวันสุดท้ายของเดือนสิ้นสุดลง (เกณฑ์: ระยะเวลาลงบันทึกข้อมูลภายใน 5 วัน มากกว่าร้อยละ 80)

ผลลัพธ์ปี พ.ศ. 2561-2564 พบว่า บุคลากรสามารถลงข้อมูลภายใน 5 วัน ได้ร้อยละ 100 ทุกปี

2. ความครบถ้วนของการบันทึกข้อมูล หมายถึง การบันทึกข้อมูลลงในแบบ google form ครบตามตัวชี้วัดที่กำหนด โดยเกณฑ์การให้คะแนน คือ หากกรรมการบันทึกครบถ้วน

ทุกหัวข้อให้ 1 คะแนน และหากบันทึกไม่ครบถ้วนทุกหัวข้อให้ 0 คะแนน (เกณฑ์: อัตราการลงบันทึกข้อมูลครบถ้วน มากกว่าร้อยละ 80)

ผลลัพธ์ปี พ.ศ. 2561-2564 พบว่า อัตราการลงบันทึกข้อมูลครบถ้วนได้ร้อยละ 80, 87, 95 และ 100 ตามลำดับ

กรณีพบอุบัติการณ์ความเสี่ยงจากการรายงานข้อมูลตัวชี้วัด ปฏิบัติดังนี้

1. ในกรณีที่เกิดอุบัติการณ์ความเสี่ยง เช่น ตรวจสอบพบประเด็น/หัวข้อ ที่ลงข้อมูลไม่ครบถ้วน หัวหน้าทีมทำการแก้ไข พร้อมลงวันที่กำกับ เป็นต้น
2. หัวหน้าทีมแจ้งผู้บันทึกข้อมูล และร่วมกันทบทวน วิเคราะห์สาเหตุ รวมถึงปัจจัยที่ก่อให้เกิดความเสี่ยงการรายงานข้อมูลไม่ถูกต้อง
3. นำผลการทบทวนมาดำเนินการวางแผนการพยาบาลเพื่อดูแลแก้ไขไม่ให้เกิดซ้ำ
4. สื่อสารข้อมูลแก่ทีมกรรมการ เพื่อทุกคนทราบและร่วมมือปฏิบัติในรูปแบบเดียวกัน

จรรยาบรรณ/คุณธรรม/จริยธรรมในการปฏิบัติงาน

ผู้จัดทำได้ยึดหลัก จรรยาบรรณ คุณธรรม จริยธรรม ในการทำงาน เช่น ประเด็นความซื่อสัตย์ในการบันทึกข้อมูลอย่างถูกต้อง เป็นต้น โดยปฏิบัติตามสาระสำคัญของจรรณยาบรรณวิชาชีพพยาบาล (ข้อบังคับสภาการพยาบาลว่าด้วยการรักษาจริยธรรมแห่งวิชาชีพการพยาบาลและการผดุงครรภ์ พ.ศ.2550, 2550)ดังนี้

1. พยาบาลพึงให้บริการพยาบาลด้วยความเคารพในศักดิ์ศรี และความแตกต่างระหว่างบุคคล โดยไม่จำกัดในเรื่อง สถานภาพทางสังคม เศรษฐกิจ คุณสมบัติเฉพาะกิจหรือสภาพปัญหาทางด้านสุขภาพอนามัยของผู้ป่วย
2. พยาบาลพึงเคารพสิทธิส่วนตัวของผู้ป่วย โดยรักษาข้อมูลเกี่ยวกับผู้ป่วยไว้เป็นความลับ
3. พยาบาลพึงให้การปกป้องคุ้มครองแก่ผู้ป่วย สังคม ในกรณีที่มีการให้บริการสุขภาพอนามัยและความปลอดภัย ถูกกระทำที่อาจเกิดจากความไม่รู้ ขาดศีลธรรม จริยธรรม หรือการกระทำที่ผิดกฎหมายจากบุคคล
4. พยาบาลมีหน้าที่รับผิดชอบในการตัดสินใจและให้การพยาบาลแก่ผู้ป่วย
5. พยาบาลพึงดำรงไว้ซึ่งสมรรถนะในการปฏิบัติการพยาบาล
6. พยาบาลพึงตัดสินใจด้วยความรอบคอบถี่ถ้วนใช้ข้อมูลสมรรถนะและคุณสมบัติอื่น ๆ เป็นหลักในการขอคำปรึกษาหารือ ยอมรับในหน้าที่ความรับผิดชอบ รวมถึงการมอบหมายกิจกรรมการปฏิบัติการพยาบาลให้ผู้อื่นปฏิบัติ

7. พยาบาลพึงมีส่วนร่วมและสนับสนุนใจกิจกรรมการพัฒนาความรู้เชิงวิชาชีพ

8. พยาบาลพึงมีส่วนร่วมและสนับสนุนในการพัฒนาวิชาชีพและส่งเสริมมาตรฐานการปฏิบัติการพยาบาล

9. พยาบาลพึงมีส่วนร่วมในการที่จะกำหนดและดำรงไว้ซึ่งสถานะภาพของการทำงานที่จะนำไปสู่การปฏิบัติพยาบาลที่มีคุณภาพสูง

10. พยาบาลพึงมีส่วนร่วมในการปกป้อง คุ้มครอง สังคม จากการเสนอข้อมูลที่ผิดและดำรงไว้ซึ่งความสามัคคีในวิชาชีพ

11. พยาบาลพึงร่วมมือและเป็นเครือข่ายกับสมาชิกด้านสุขภาพอนามัยและบุคคลอื่น ๆ ในสังคมเพื่อส่งเสริมชุมชนและสนองตอบความต้องการด้านสุขภาพอนามัยของสังคมสำหรับสมาคมพยาบาลแห่งประเทศไทยได้กำหนดจรรยาบรรณวิชาชีพของสมาคม พ.ศ. 2528 มุ่งเน้นให้พยาบาลได้ประพฤติปฏิบัติหน้าที่ความรับผิดชอบ โดยกำหนดเป็นความรับผิดชอบต่อประชาชน ความรับผิดชอบต่อประเทศชาติ ต่อผู้ร่วมวิชาชีพและต่อตนเอง ดังนี้

จรรยาบรรณวิชาชีพการพยาบาลต่อประชาชน

1. ประกอบวิชาชีพด้วยประกอบด้วยความมีสติ ตระหนักในคุณค่าและศักดิ์ศรีของความเป็นมนุษย์

2. ปฏิบัติต่อประชาชนด้วยความเสมอภาคตามสิทธิมนุษยชน โดยไม่คำนึงถึง เชื้อชาติ ศาสนา และสถานภาพของบุคคล

3. ละเว้นการปฏิบัติที่มีอคติ และการใช้อำนานหน้าที่เพื่อผลประโยชน์ส่วนตน

4. พึงเก็บรักษาเรื่องส่วนตัวของผู้รับบริการไว้เป็นความลับ เว้นแต่ด้วยความยินยอมของผู้นั้นหรือเมื่อต้องปฏิบัติตามกฎหมาย

5. พึงปฏิบัติหน้าที่โดยใช้ความรู้ความสามารถอย่างเต็มที่ในการวินิจฉัยและการแก้ไขปัญหาสุขภาพอนามัยอย่างเหมาะสมแก่สภาพของบุคคล ครอบครัว และชุมชม

6. พึงป้องกันภยันตรายอันจะมีผลต่อสุขภาพอนามัยของประชาชน

จรรยาบรรณวิชาชีพการพยาบาลต่อวิชาชีพ

1. พึงตระหนักและถือปฏิบัติในหน้าที่ความรับผิดชอบตามหลักการแห่งวิชาชีพการพยาบาล

2. พัฒนาความรู้และวิธีปฏิบัติให้ได้มาตรฐานแห่งวิชาชีพ

3. พึงศรัทธาสนับสนุนและให้ความร่วมมือในกิจกรรมแห่งวิชาชีพ

4. พึงสร้างและธำรงไว้ซึ่งสิทธิอันชอบธรรม ในการประกอบวิชาชีพการพยาบาล

5. พึงเผยแพร่ชื่อเสียงและคุณค่าแห่งวิชาชีพให้เป็นที่ปรากฏแก่สังคม

จรรยาบรรณวิชาชีพการพยาบาลต่อตนเอง

1. ประพฤติตนและประกอบกิจแห่งวิชาชีพ โดยถูกต้องตามกฎหมาย
2. ยึดมั่นในคุณธรรมและจริยธรรมแห่งวิชาชีพ
3. ประพฤติปฏิบัติตนให้เป็นแบบอย่างที่ดี ทั้งในด้านการประกอบกิจแห่งวิชาชีพและส่วนตัว
4. ใฝ่รู้พัฒนาแนวคิดให้กว้าง และยอมรับการเปลี่ยนแปลง
5. ประกอบกิจแห่งวิชาชีพด้วยความเต็มใจ และเต็มกำลังความสามารถ
6. ปฏิบัติหน้าที่ด้วยความมีสติ รอบรู้ เชื่อมั่น และมีวิจารณญาณอันรอบคอบ

บทที่ 5
ปัญหาอุปสรรค แนวทางแก้ไขและข้อเสนอแนะ

ปัญหาอุปสรรค

จากการนำคู่มือคู่มือการปฏิบัติงาน เรื่อง การจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาล โดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนัก ตั้งแต่วันที่1 มกราคม พ.ศ. 2561 ถึงวันที่ 31 ธันวาคม 2564 พบปัญหาและอุปสรรคดังนี้

1. บุคลากรพยาบาลบางรายไม่ใช้อีเมลของมหาวิทยาลัยนวมินทราธิราช (@nmu.ac.th) ส่งผลให้ระบบไม่ยินยอมให้เข้าถึงไฟล์การบันทึกข้อมูล

2. มีการปรับเปลี่ยนคณะกรรมการใน QIT กลุ่มโรคลำไส้ใหญ่และทวารหนัก เนื่องจากมีบุคลากรพยาบาลวิชาชีพโอนย้าย ลาออก ทำให้การบันทึกไม่ครบถ้วน จึงต้องสอน สาธิตและฝึกทักษะการบันทึกข้อมูลใหม่

แนวทางแก้ไขและพัฒนา

1. ขอความร่วมมือกับกรรมการในทีมในการใช้อีเมลของมหาวิทยาลัยนวมินทราธิราช
2. ประสานงานกับหน่วยสารสนเทศเพื่อขอใช้ระบบ WIFI ให้กับกรรมการในทีม
3. จัดการนิเทศคณะกรรมการQITคนใหม่ในเรื่องการใช้คู่มือก่อนลงมือปฏิบัติงานจริงและกำกับการปฏิบัติตามคู่มืออย่างสม่ำเสมอ

ข้อเสนอแนะ

1. เพื่อให้การดูแลผู้ป่วยโรคลำไส้ใหญ่และทวารหนักเป็นไปอย่างมีประสิทธิภาพต้องมีการจัดหางบประมาณสำหรับดำเนินการ หรือการจัดหาการสนับสนุนอุปกรณ์ในการเชื่อมต่อ เช่น Tablet เป็นต้น

2. สนับสนุนให้มีการใช้คู่มือการจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาล โดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนัก

3. ควรมีการนิเทศติดตามและประเมินผลการปฏิบัติการพยาบาลของพยาบาลในหน่วย ฯ ให้ปฏิบัติตามคู่มือการจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนัก

4. บุคลากรพยาบาลที่รับผิดชอบต้องศึกษาและทบทวนองค์ความรู้ใหม่ ๆ ที่เกี่ยวข้องกับตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลเพื่อนำมาพัฒนาต่อไป

บรรณานุกรม

ข้อบังคับสภาการพยาบาลว่าด้วยการรักษาจริยธรรมแห่งวิชาชีพการพยาบาลและการผดุงครรภ์ พ.ศ. 2550. (2550,11 กรกฎาคม). *ราชกิจจานุเบกษา.* เล่ม 124 ตอนพิเศษ 83 ง. หน้า 56-60.

คณะแพทยศาสตร์วชิรพยาบาล. (2563). *รายงานประจำปี 2563.* กรุงเทพมหานคร: มหาวิทยาลัยนวมินทราธิราช.

ฝ่ายการพยาบาล โรงพยาบาลวชิรพยาบาล. (2563). *แผนปฏิบัติการประจำปี 2563.*กรุงเทพมหานคร: คณะแพทยศาสตร์วชิรพยาบาล.

ฝ่ายเทคโนโลยีสารสนเทศคณะแพทยศาสตร์วชิรพยาบาล. (2561). *แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาล.* กรุงเทพมหานคร: คณะแพทยศาสตร์วชิรพยาบาล.

รสสุคนธ์ วาริทสกุล. (2560). การจัดการข้อมูลในการบริการสุขภาพสำหรับกลุ่มผู้ป่วยโรคเรื้อรัง. *วารสารพยาบาลทหารบก, 18*(1), 6-14.

วรกาล ไชยศล. (2561). การจัดการข้อมูล. สืบค้น2 เมษายน 2561 จาก https://sites.google.com/site/pimwipatom11/home

อรอนงค์ ทัพสุวรรณ์. (2557). *คู่มือการพยาบาลผู้ป่วยมะเร็งลำไส้ใหญ่และทวารหนักที่ได้รับการรักษาโดยการผ่าตัด.*กรุงเทพมหานคร: บริษัท บียอนด์ เอ็นเทอร์ไพรซ์ จำกัด.

Paul, S. M. (1998). Data Management in Nursing Research. In V. K. Saba, D. B. Pocklington, & K. P. Miller (Eds.), *Nursing and Computers: An Anthology,* 1987–1996 (pp. 492-496). New York, NY: Springer New York.

Zhu, R., Han, S., Su, Y., Zhang, C., Yu, Q., & Duan, Z. (2019). The application of big data and the development of nursing science: A discussion paper. *International Journal of Nursing Sciences,* 6(2), 229-234. doi:https://doi.org/10.1016/j.ijnss.2019.03.001

ภาคผนวก

ภาคผนวก ก
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของคณะแพทยศาสตร์วชิรพยาบาล

ประกาศคณะแพทยศาสตร์วชิรพยาบาล
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์

เพื่อให้การดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ของคณะแพทยศาสตร์วชิรพยาบาล มีความมั่นคง ปลอดภัย เชื่อถือได้ และมีมาตรฐานเป็นที่ยอมรับในระดับสากล อันจะเป็นการป้องกันปัญหาที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและภัยคุกคามต่าง ๆ รวมทั้งเพื่อให้เป็นไปตามมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ จึงสมควรให้มีประกาศคณะแพทยศาสตร์วชิรพยาบาลว่าด้วยการนี้

อาศัยอำนาจตามความในมาตรา ๓๙ แห่งพระราชบัญญัติมหาวิทยาลัยนวมินทราธิราช พ.ศ. ๒๕๕๓ จึงออกประกาศไว้ ดังต่อไปนี้

๑. ประกาศนี้เรียกว่า "ประกาศคณะแพทยศาสตร์วชิรพยาบาล เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาล"

๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

๓. ในประกาศนี้

"คณะ" หมายความว่า คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช

"นโยบาย" หมายความว่า แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาล

"แนวปฏิบัติ" หมายความว่า แนวทางปฏิบัติ ข้อปฏิบัติ และหรือวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาล

คำนิยามที่มิได้กำหนดไว้ในประกาศนี้ให้นำคำนิยามในประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม มาใช้โดยอนุโลม

๔. บรรดาประกาศหรือคำสั่งอื่นใดที่ขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะมีวัตถุประสงค์ ดังนี้

๕.๑ เพื่อให้ระบบสารสนเทศของคณะเกิดความมั่นคง ปลอดภัย และเชื่อถือได้

๕.๒ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติแก่ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้คณะ และเผยแพร่ให้ผู้เกี่ยวข้องได้รับทราบ เข้าถึงและถือปฏิบัติตามนโยบายและแนวปฏิบัติอย่างเคร่งครัด โดยต้องมีการทบทวนนโยบายไม่น้อยกว่าปีละ ๑ ครั้ง

/๖. นโยบาย...

๖. นโยบายในการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะ ประกอบด้วย

๖.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control)

๖.๑.๑ การควบคุมเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งาน ให้มีกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๖.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิเท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน รวมทั้งต้องมีการทบทวนสิทธิการใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๖.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องกำหนดสิทธิในการเข้าถึงเครือข่าย ผู้จะเข้าใช้งานต้องลงบันทึกการเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ตโดยผ่านระบบรักษาความปลอดภัยของคณะ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งานเพื่อให้สามารถควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๖.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องกำหนดให้ผู้เข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนเข้าใช้งาน ต้องมีการกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เกิดการละเมิดสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๖.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น ต้องกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอพพลิเคชั่นต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าส่วนงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๖.๒ การจัดการระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องมีการจัดทำระบบสารสนเทศระบบสำรองข้อมูลที่เหมาะสมและอยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับจากมากไปหาน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูลและจัดทำแผนเตรียมความพร้อมฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

/๖.๓ ต้องตรวจสอบ.....

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาล

แนบท้ายประกาศคณะแพทยศาสตร์วชิรพยาบาล
เรื่อง นโยบายและแนวปฏิบัติในการรักษา
ความมั่นคงปลอดภัยด้านสารสนเทศ
ของคณะแพทยศาสตร์วชิรพยาบาล
ลงวันที่ ๖ ธันวาคม ๒๕๖๑

สารบัญ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาล

ตามประกาศคณะแพทยศาสตร์วชิรพยาบาล เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาล กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาล เพื่อให้ระบบเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์วชิรพยาบาลเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อคณะแพทยศาสตร์วชิรพยาบาลนั้น คณะแพทยศาสตร์วชิรพยาบาล จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

ข้อ ๑ คำนิยาม

"คณะ" หมายความว่า คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช

"หน่วยงาน" หมายถึง ภาควิชา ฝ่าย สำนักงาน งาน ศูนย์ และหน่วยงานที่มีฐานะเทียบเท่าที่อยู่ในสังกัดคณะแพทยศาสตร์วชิรพยาบาล

"ผู้ใช้งาน" หมายถึง พนักงานมหาวิทยาลัย ข้าราชการ ลูกจ้าง และพนักงานราชการ ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

"ผู้บริหาร" หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ คณะบดี รองคณบดี หรือเทียบเท่า ผู้อำนวยการ/หัวหน้าภาค/หัวหน้าฝ่าย/หัวหน้าสำนักงาน/หัวหน้างาน เป็นต้น

"ผู้บริหารระดับสูง" คณะบดีหรือเทียบเท่า

"ผู้ดูแลระบบ" (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูล ของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"สิทธิของผู้ใช้งาน" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่ เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

"สินทรัพย์" หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์สื่อสารที่สามารถ

๒

เชื่อมต่อกับระบบเครือข่าย อาทิเช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

"ระบบเครือข่าย" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN) เป็นต้น

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึง โดยมิชอบเอาไว้ด้วยก็ได้

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงาน ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"การพิสูจน์ตัวตน" หมายถึง กระบวนการยืนยันความถูกต้องของตัวตนว่าเป็นบุคคลที่ได้กล่าวอ้าง โดยในการพิสูจน์ตัวตนนั้น จะต้องมีขั้นตอนระบุตัวตนเพื่อแสดงตนว่าคือใคร เช่น ชื่อผู้ใช้งาน (Username) และขั้นตอนแสดงหลักฐานว่าเป็นบุคคลที่กล่าวอ้างจริง เช่น รหัสผ่าน(Password)

"ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย"หมายถึง สถานที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์/หรืออุปกรณ์บริหารจัดการเครือข่าย

หมวดที่ ๑

การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจของหน่วยงานของรัฐ

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น

ข้อ ๒. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงาน

ข้อ ๓. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

(๑.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข

- อนุมัติ
- ไม่มีสิทธิ์

(๑.๒) กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(๑.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(๒.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่น ข้อมูลผู้ป่วย ข้อมูลทางการแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

(๒.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๒.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด

๔

ความเสียหายอย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๒.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๒.๕) รูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น TEXT Format, Document Format, PDF Format (Portable Document Format)

- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ มีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

ข้อ ๔. ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ ๕. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๖. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๗. กำหนดเวลาการเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าได้ตลอดเวลา

(๒) ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในตามที่หน่วยงานกำหนด

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๘. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความ รับผิดชอบตามส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control) ข้อ ๓

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษร ให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๙. ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย(Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์ เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบ เป็นลายลักษณ์อักษร

ข้อ ๑๐. ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งาน อย่างสม่ำเสมอ อย่างน้อย ปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือ เมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน ๗ วัน

ข้อ ๓๓. การบริหารจัดการรหัสผ่าน

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๖) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๗) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๓๔. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการ เข้าถึงผ่านระบบงาน

(๒) กำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับ ความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(๗) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

ข้อ ๑๓. ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงานหรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างคณะหน่วยงานที่มาขอเชื่อมโยง

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๔. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน

(Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)

(๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

(๓) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

(๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๗) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดาและการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๑๘๐ วันหรือทุกครั้งที่มีการ แจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๑๕. การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการ รักษาความลับ ทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

ข้อ ๑๖. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้ เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๑๗. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของ หน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดี หรือเกิดจากความผิดพลาด ใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๑๐

(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที

ข้อ ๑๘. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของคณะ หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๙. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญหรืออยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลงทำซ้ำหรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๐. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของคณะ และข้อมูลของ ผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพรโดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๑. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลคลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๒๒. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร คณะจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใด ทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่คณะต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับคณะ ซึ่งคณะอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่าแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์(Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๔. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๕. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของคณะ

ข้อ ๒๖. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของคณะ

ข้อ ๒๗. ห้ามใช้สินทรัพย์ของคณะเพื่อประโยชน์ทางการค้า

ข้อ ๒๘. ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของคณะโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๒๙. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ ๓๐. ห้ามใช้ระบบสารสนเทศของคณะ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๑. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๒. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของคณะ โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๓๓. ผู้ใช้งานต้องไม่เข้าไปในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๔. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๕. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๓๖. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๓๗. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูลก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บ ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

๑๒

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้ เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อ ๓๘. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย

ข้อ ๓๙. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย

ข้อ ๔๐. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๔๑. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

ข้อ ๔๒. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อคณะ

ข้อ ๔๓. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตาม ข้อ ๔๒ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๔๓

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๔๔. มาตรการควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) และทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่ "

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่ " ให้ถูกต้องชัดเจน

(๓) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ ๔๕. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม "การขอเชื่อมต่อเครือข่าย" โดย ผ่านระบบพิสูจน์ตัวตนการใช้งาน Internet คณะ

ข้อ ๔๖. การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

ข้อ ๔๗. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๘. ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๔๔

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม "การขอเชื่อมต่อเครือข่าย" โดยผ่านระบบพิสูจน์ตัวตนการใช้งาน Intranet คณะ
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ ๔๙. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๕๐. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ ติดตั้งก่อนดำเนินการ

ข้อ ๕๑. กำหนดให้มีการจัดเก็บซอร์สโค้ดไลบรารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๕๒. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์ ๒๕๖๐

ข้อ ๕๓. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากหัวหน้าหน่วยงาน

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๓) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

(๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(๕) การเข้าสู่ระบบเครือข่ายภายใน และระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๕๔. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ ๕๕. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๕๖. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ ๕๗. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ ๕๘. IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ ๕๙. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๖๐. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการ ยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๖๑. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัส ผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

(๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

(๖) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(๗) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากหัวหน้าส่วนงาน

(๘) ซอฟต์แวร์ที่คณะใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

(๙) ซอฟท์แวร์ที่คณะจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

(๑๐) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของคณะ เพื่อประโยชน์ทางการค้า

(๑๑) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๑๒) ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๖๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๖๓. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งาน โปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถ

๑๘

ทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๑) การใช้งานโปรแกรมยูทิลิตี้ ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน

(๒) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

(๔) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

(๕) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

ข้อ ๖๔. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

(๑) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที

(๒) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง

ข้อ ๖๕. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

(๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด และกำหนดให้ใช้งานได้ตามช่วงเวลาการทำงานที่หน่วยงานกำหนดเท่านั้น

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๑๙

ส่วนที่ ๙ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ข้อ ๖๖. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๖๗. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์ เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๖๘. ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ ๖๙. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๗๐. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการส ารองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๗๑. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(๑) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่น ๆ

(๒) มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(๓) มีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น

ข้อ ๗๒. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and Intellectual property and Preventing Malware)

ข้อ ๗๓. คณะได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิด ลิขสิทธิ์ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๗๔. ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ ๗๕. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่ หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้า หน่วยงาน

ข้อ ๗๖. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบ ไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๗๗. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๗๘. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๗๙. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๘๐. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๔๑. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงาน สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญ ในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๔๒. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟแวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๘๓. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

ข้อ ๘๔. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

ข้อ ๘๕. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๘๖. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัว เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

ข้อ ๘๗. ต้องกำหนดขนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ ๘๘. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ ๘๙. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๙๐. ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า โดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งานและกำหนดให้ซ่อน SSID (Service Set Identifier)

ข้อ ๙๑. ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๙๒. ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะ

อนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๔๓. ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๔๔. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๔๕. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข้อ ๔๖. ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรืออาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบ เครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่ง รายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ ๔๗. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

ข้อ ๔๘. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของคณะ จะต้องทำการลงทะเบียน กับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

ข้อ ๔๙. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๕๐๐. หน่วยงานมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

ข้อ ๕๐๑. การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๕๐๒. ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเตอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall

ข้อ ๕๐๓. ผู้ใช้งานอินเตอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

ข้อ ๕๐๔. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall

ข้อ ๑๐๕. การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๑๐๖. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๑๐ วัน

ข้อ ๑๐๗. การกำหนดนโยบายในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากหน่วยงานก่อน

ข้อ ๑๐๘. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

ข้อ ๑๐๙. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ Firewall เป็นประจำทุกสัปดาห์ หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๑๑๐. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงานที่มีลักษณะที่เป็นอินทราเน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเตอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๑๑. หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๑๒. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานก่อน

ข้อ ๑๑๓. ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเตอร์เน็ตทันที

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

ข้อ ๑๑๔. ในการลงทะเบียนบัญชี ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยยื่นคำขอกับเจ้าหน้าที่หน่วยงาน

ข้อ ๑๑๕. รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น "x" หรือ "O" ในการพิมพ์แต่ละตัวอักษร

ข้อ ๑๑๖. เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้ เปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๑๑๙. ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน ๓ ครั้ง

ข้อ ๑๒๐. ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๑๒๑. เปลี่ยนรหัสผ่าน (Password) ทุก ๓ - ๖ เดือน

ข้อ ๑๒๐. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตน

ข้อ ๑๒๓. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๑๒๒. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล E-Mail ที่หน่วยงานกำหนดไว้ ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-Mail ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๑๒๓. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๑๒๔. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๑๒๕. ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ ๑๒๖. ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๒๗. ให้ระบุชื่อของผู้ส่งใน E-Mail ทุกฉบับที่ส่งไป

ข้อ ๑๒๘. ให้ทำการสำรองข้อมูล E-Mail ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าหน่วยงานจะทำการสำรองข้อมูล E-Mail ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้น E-Mail ที่เก่ามาก ๆ และ จำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

ข้อ ๑๒๙. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

ข้อ ๑๓๐. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๓๑. ผู้ใช้งานไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๒. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๓. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือ จดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๔. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ส่วนที่ ๑๓ การควบคุมการใช้อินเตอร์เน็ต (Internet)

ข้อ ๑๓๕. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ ๑๓๖. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ต ผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ ๑๓๗. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๑๓๘. ไม่ใช้ระบบอินเตอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๑๓๙. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

ข้อ ๑๔๐. ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเตอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๔๑. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๑๔๒. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ ๑๔๓. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

ข้อ ๑๔๔. หลังจากใช้งานระบบอินเตอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๑๔๕. หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๑๔๖. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ ๑๔๗. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับคณะหรือมหาวิทยาลัยนวมินทราธิราช เท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันแล้วเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

(๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

ข้อ ๑๔๘. การใช้รหัสผ่าน ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุตาม ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Resopnsibilities) คิดว่าสะกด Responsibilities

ข้อ ๑๔๙. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๑๕๐. การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญ

เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ ๑๕๑. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงาน ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหยุดมือ เป็นต้น

(๖) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือ ทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๘) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๙) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด

ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๐) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายในเป็นพิมพ์ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ ๑๕๒. ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ ๑๕๓. การควบคุมการเข้าถึงระบบปฏิบัติการ

(๑) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตาม ส่วนที่ ๓ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) ข้อ ๖๙

(๓) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลา ประมาณ ๑๕ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(๔) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ ๑๕๔. การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุตาม ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Resopnsibilities)

ข้อ ๑๕๕. การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยง

ต่อการรั่วไหลของข้อมูล

(๓) แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ ๑๖ การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS)

ข้อ ๑๕๖. IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๑๕๗. IDS/IPS Policy ครอบคลุมทุก โฮสต์ (Host) ในเครือข่ายของ หน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเตอร์เน็ตทุกเส้นทาง

ข้อ ๑๕๘. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๑๕๙. ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๑๖๐. โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการ บันทึกผลการตรวจสอบ

ข้อ ๑๖๑. ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

ข้อ ๑๖๒. ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๑๖๓. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๑๖๔. เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๒๕. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบพฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบทันทีที่ตรวจพบ ข้อ ๑๒๖. พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๒๗. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๒๘. ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๒๙. หน่วยงานมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๓๐. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของคณะ การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และ ทรัพยากรระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ ๑๓๑. การปรับปรุงระบบปฏิบัติการ (Operating System Update)

(๑) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

(๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)

(๔) กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name) / IP Address

(๕) ปรับปรุง / กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)

(๖) ติดตั้งโปรแกรม Antivirus / ปรับปรุง Virus Definition และกำหนดค่าการ ตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

ข้อ ๑๓๒. การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)

๓๔

(๑) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Adminstrator)

(๒) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิการเข้าใช้ระบบ

ข้อ ๓๓๓. การปรับปรุงการรักษาความปลอดภัย / Antivirus (System Security & Antivirus Update)

(๑) ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ

(๒) Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

(๓) ปรับปรุง / กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา

(๔) ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(๕) ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์ เป็นประจำ

ข้อ ๓๓๔. ติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

(๑) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่หน่วยงานใช้

(๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นกำหนด

(๓) สร้าง และ กำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่นและสิทธิ์การใช้

(๔) ปรับปรุง / กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

ข้อ ๓๓๕. ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่าง ๆ / กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

(๑) ติดตั้ง โปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

(๒) กำหนดค่า หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด

(๔) แจ้งผู้ใช้งาน หรือเจ้าของระบบงาน ให้สามารถเริ่มใช้งานได้ โดยแจ้งรายชื่อรหัสผ่าน และ

สิทธิ์การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้

(๕) กำหนดเกณฑ์การสำรอง / สำเนา / ทดสอบกู้คืน (Restore Test)

(๖) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้าง / ปรับปรุง

ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ ๑๗๖. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

ข้อ ๑๗๗. ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ ๑๗๘. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๑๗๙. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ ๒

การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑. กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

(๑) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๒) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒.๒) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๓๙

(๒.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๓.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการพาณิชย์ที่ให้บริการ เช่น ข้อมูลดัชนีเศรษฐกิจการค้าข้อมูลการค้าระหว่างประเทศของไทย ข้อมูลเศรษฐกิจการค้าจังหวัด เป็นต้น

(๓.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๓.๕) การกำหนดเวลาที่ได้เข้าถึง

(๓.๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ ๒. ข้อมูล ข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการการรักษาความปลอดภัย

ข้อ ๓. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑ ข้อ ๑๒

ข้อ ๔. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้า ออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังต่อไปนี้

(๑) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกันหรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

(๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ

(๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

(๖) กำหนดสิทธิ์การเข้าถึงข้อมูล

(๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๓๔

(๔) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๖. พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ ๗. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ ๘. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการส ารองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาที่ข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบคำคอนฟิกูเรชันต่าง ๆ ของระบบการสำรองข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น

(๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลสำรองที่ได้สำรองเก็บไว้

ข้อ ๑๐. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ ๑๑. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ ๑๓. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

๔๓

ข้อ ๑๔. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อย ปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อ ๑. จัดลำดับความสำคัญของความเสี่ยง

ข้อ ๒. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๓. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๔. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ ๕. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

ข้อ ๖. มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหาร

จัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูล ล็อก แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงันหรือหยุดทำงาน และส่งผลให้ ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

(๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุดทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้าน สารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human error ลดน้อยลง

(๒) จัดทำหนังสือแจ้งเวียนหน่วยงานทั้งส่วนกลางและส่วนภูมิภาค เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่าง ถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเตอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนด แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย อุปกรณ์ตรวจจับควันจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสียงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนด แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(๒) ถอดเทป Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

(๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

หมวดที่ ๕

การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวปฏิบัติ

ข้อ ๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒. ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ต้องมีลักษณะ ดังนี้

(๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

(๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออก ของบุคคลเป็นจำนวนมาก

(๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๔) จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(๕) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจากบริเวณดังกล่าว

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศ จัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต

๔๑

รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการ กำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔. การควบคุมการเข้าออก อาคารสถานที่

(๑) กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ "พื้นที่ใช้งานระบบ" อย่างชัดเจน

(๒) การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้ มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

(๓) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

(๔) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(๕) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(๖) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๗) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไปเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๘) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

ที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๙. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูล สำคัญโดยผู้รับจ้างให้บริการจากภายนอก

(๙) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๐) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๑๒) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า- ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

(๑๓) จัดให้มีการดูแลและ เฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๔) จัดให้มีการทบทวนหรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณ

๕๐

(ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๕

การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ ๑. ระบบป้องกันผู้บุกรุก

(๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมี ดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อ ๒. ระบบไฟร์วอลล์

(๑) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

(๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

(๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต ภัยคุกคามทางอินเตอร์เน็ต หรือ มัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์

(๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในคณะไปยังภายนอกหรือไม่

(๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจาย อยู่ในเครือข่ายของคณะ

(๓) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

หมวดที่ ๖

การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของคณะ

๒ .เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อ ๑. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อ ๓. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการ ดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และ มีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ ๔. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อ ๖. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

ข้อ ๗. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ข้อ ๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของคณะหรือของมหาวิทยาลัยนวมินทราธิราช และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หาก

ผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ ๗

หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง คณบดี ผู้อำนวยการ หัวหน้าภาค หัวหน้าฝ่าย หัวหน้างาน เจ้าหน้าที่ ตลอดจนผู้ที่ ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ ๑. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CSO/CIO)
- หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือเทียบเท่าระดับหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

(๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบ คอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒. ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือ เทียบเท่าหัวหน้าฝ่าย

(๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อ ๓. ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

- ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการมหาวิทยาลัยนวมินทราธิราช เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่เครื่องคอมพิวเตอร์

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของ

๕๖

ฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(๓) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

(๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๖) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเตอร์เน็ต

(๗) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยนวมินทราธิราช

ภาคผนวก

๕๘

การจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๑.๑. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อย ครอบคลุมตามข้อ ๔

๑.๒. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อย ครอบคลุมตามข้อ ๕ – ๑๔

ข้อ ๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๒.๑. ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัยนานมีนทราธิราช

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๒.๒. ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

ข้อ ๓. มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๔. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยจัดทำข้อปฏิบัติสำหรับการควบคุมการเข้าถึงสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย โดยกำหนดสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ หลักการ "ตามความจำเป็นที่ต้องรู้"

ข้อ ๕. มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการถอดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๖. มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่าน

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ ๗. มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connection) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งาน เครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบน เครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๘. มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการ

ใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๙. มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (function) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้ กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๐. จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๓. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

(๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๔. ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ภาคผนวก ข

ข้อมูลตัวชี้วัดการพัฒนาคุณภาพหน่วยศัลยกรรมลำไส้ใหญ่และทวารหนัก

ข้อมูลตัวชี้วัดการพัฒนาคุณภาพหน่วยศัลยกรรมลำไส้ใหญ่และทวารหนัก

ข้อมูลตัวชี้วัดการพัฒนาคุณภาพหน่วยศัลยกรรมลำไส้ใหญ่และทวารหนัก					
ประจำเดือน ..... พ.ศ.					
ลำดับที่	ตัวชี้วัด	เกณฑ์	จำนวน	ร้อยละ	หมายเหตุ
1	อัตราผู้ป่วยที่ได้รับการผ่าตัด colorectal แบบ Elective case ที่มีแผลติดเชื้อ	5%			
2	อัตราผู้ป่วย colorectal disease ที่ได้รับการผ่าตัดซ้ำในการ admission ครั้งเดียวกัน	0%			
3	อัตราผู้ป่วยที่รอการผ่าตัดภายหลังได้รับการยืนยันผลชิ้นเนื้อเกิน 30 วัน	10%			
	โดยที่ไม่มีข้อห้ามในการผ่าตัด และไม่ต้องรับการฉายแสงก่อนผ่าตัด				
4	อัตราผู้ป่วยที่ได้รับการพักฟื้นในโรงพยาบาลหลังผ่าตัดลำไส้แบบส่องกล้องเกิน 10 วัน				
5	อัตราการแก้ไข colostomy ใน admission ครั้งเดียวกัน	10%			
6	ภาวะแทรกซ้อนหลังผ่าตัดลำไส้				
	- แผลผ่าตัดติดเชื้อ				
	- ติดเชื้อระบบทางเดินปัสสาวะ				
	- เกิดภาวะเส้นเลือดดำอุดตัน DVT				
	- เกิดการภาวะลำไส้รั่ว				
7	ภาวะทุพโภชนาการของผู้ป่วยระดับรุนแรงระดับ 3 และ ระดับ 4				
8	คุณภาพชีวิตของผู้ป่วยมะเร็งลำไส้ใหญ่ 1 ปีหลังได้รับการรักษาโดยการผ่าตัด				
9	ภาวะแทรกซ้อนจากการผ่าตัด Colostomy ใน admission ครั้งเดียวกัน				
	- retraction				
	- bleeding ที่จำเป็นต้องผ่าตัด				
	- necrosis				
	- infection				
	- mucocutaneous fistular				

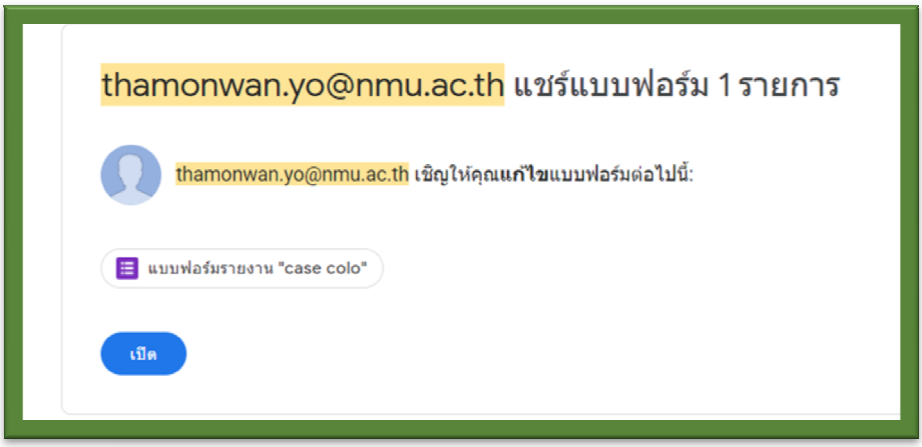
ภาคผนวก ค

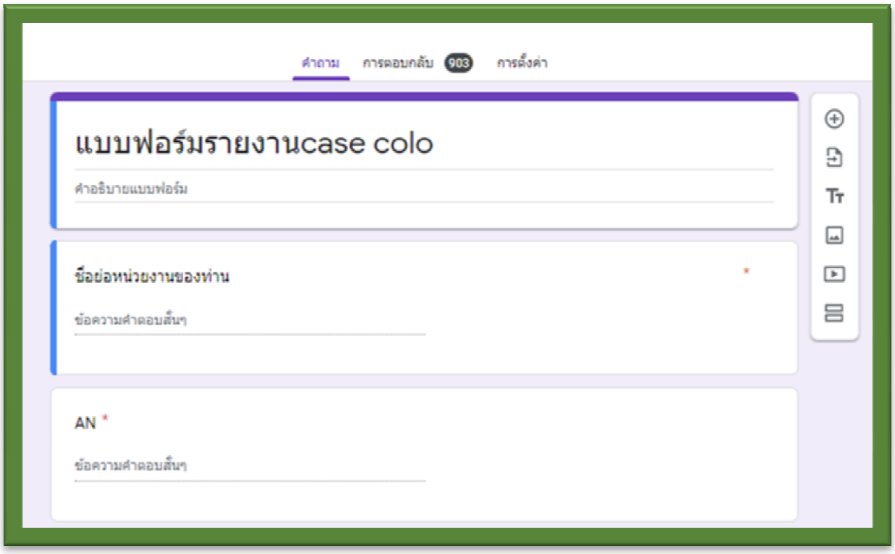
แบบประเมินผลบุคลากรในการใช้เว็บแอพลิเคชั่น

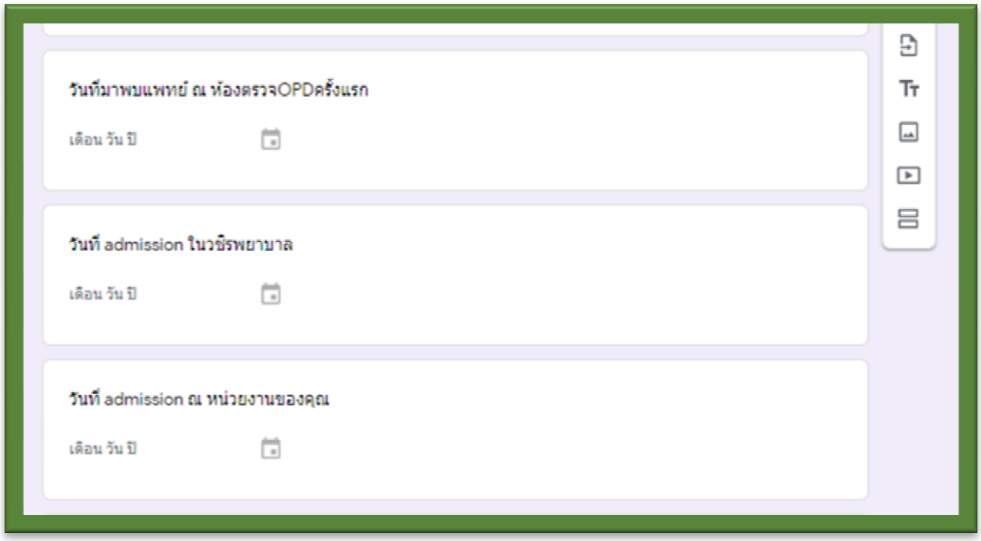
แบบประเมินผลบุคลากรในการใช้เว็บแอพลิเคชั่น

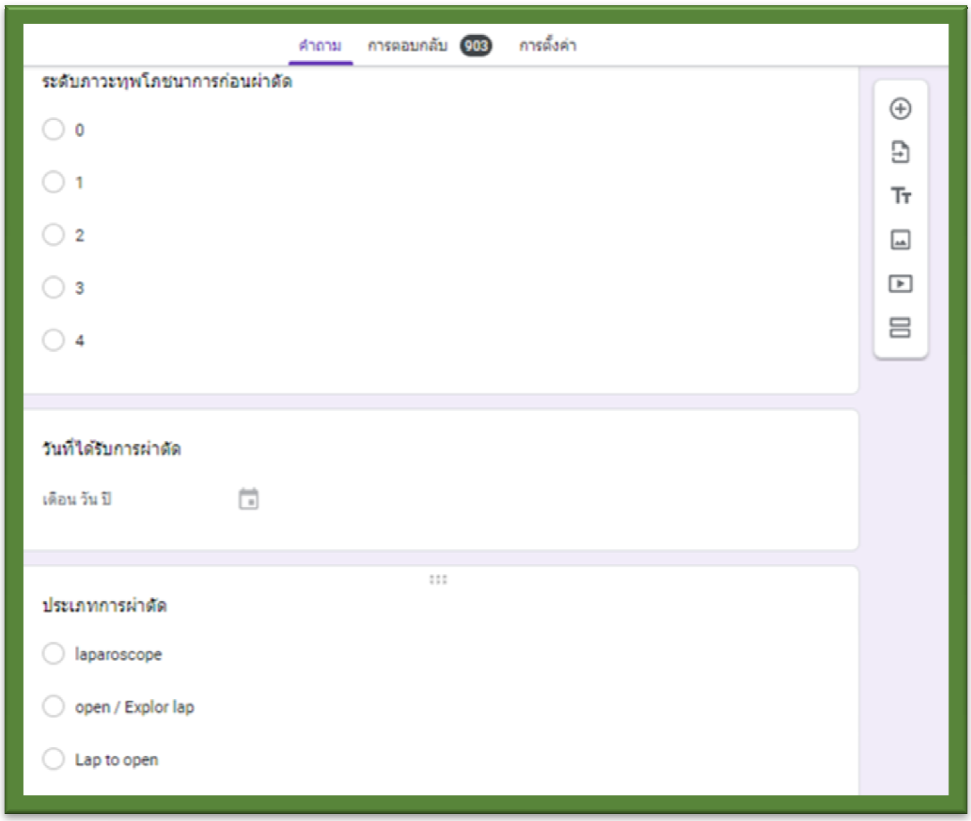
ชื่อกรรมการ	ความครบถ้วน	ความตรงต่อเวลา	ความพึงพอใจ	หมายเหตุ
คนที่ 1				
คนที่ 2				
คนที่ 3				
คนที่ 4				
คนที่ 5				
.				
.				
.				
.				
คนที่ 15				
รวม				
เฉลี่ย				
SD				

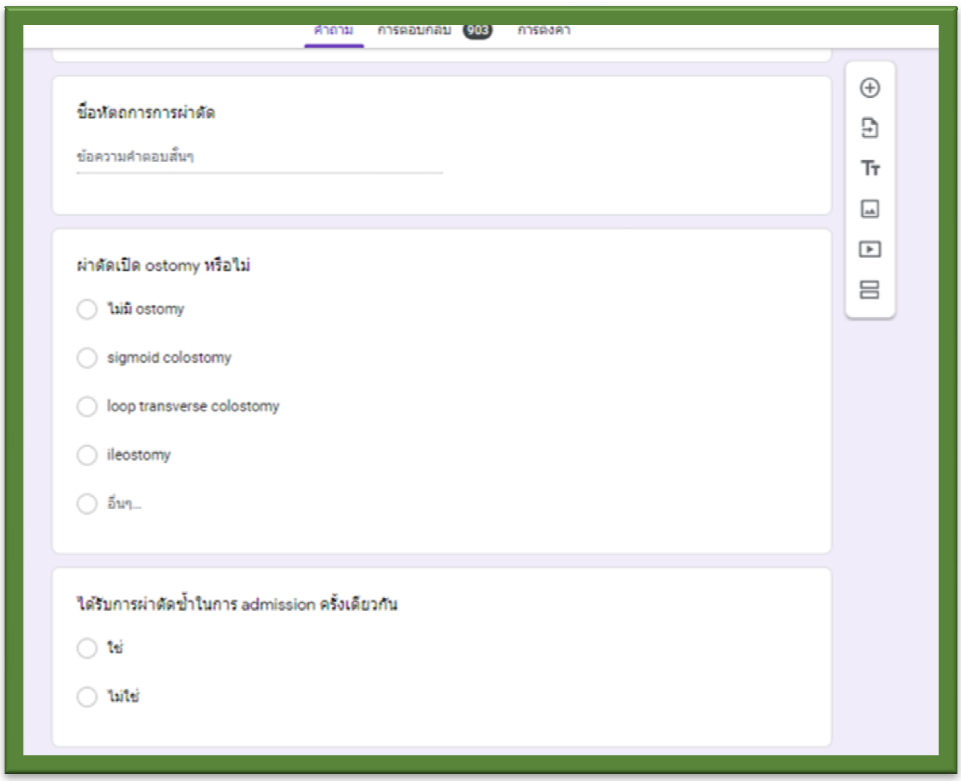
ภาคผนวก ง
ฐานข้อมูลแอพลิเคชั่น

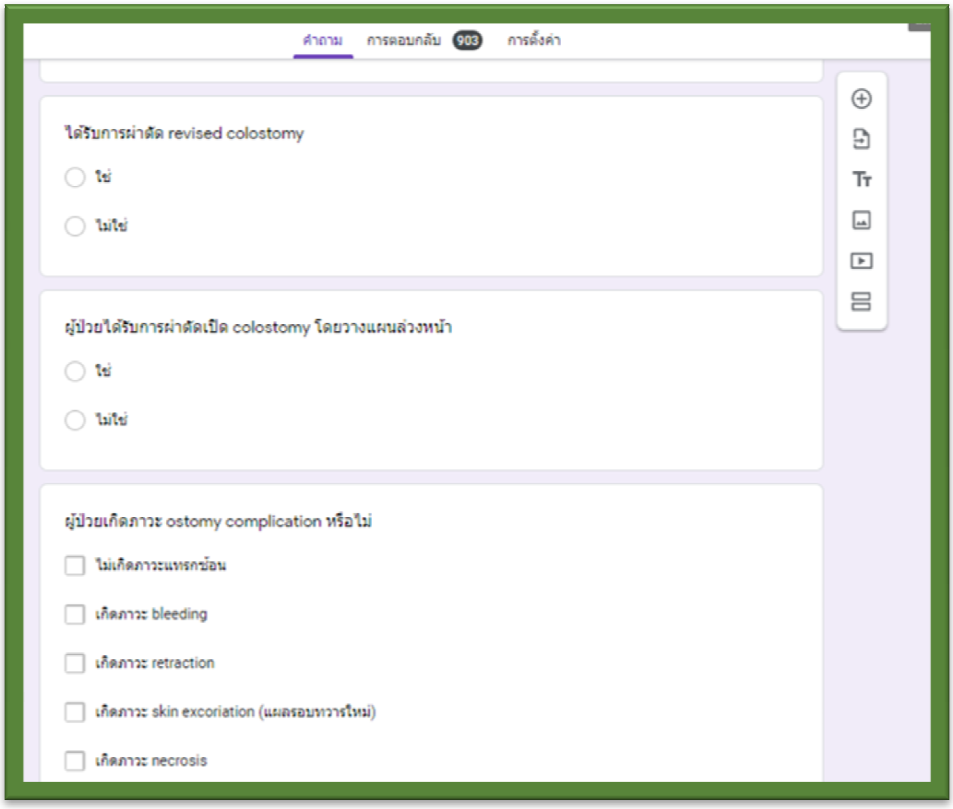

thamonwan.yo@nmu.ac.th แชร์แบบฟอร์ม 1 รายการ
thamonwan.yo@nmu.ac.th เชิญให้คุณแก้ไขแบบฟอร์มต่อไปนี้:
แบบฟอร์มรายงาน "case colo"
เปิด

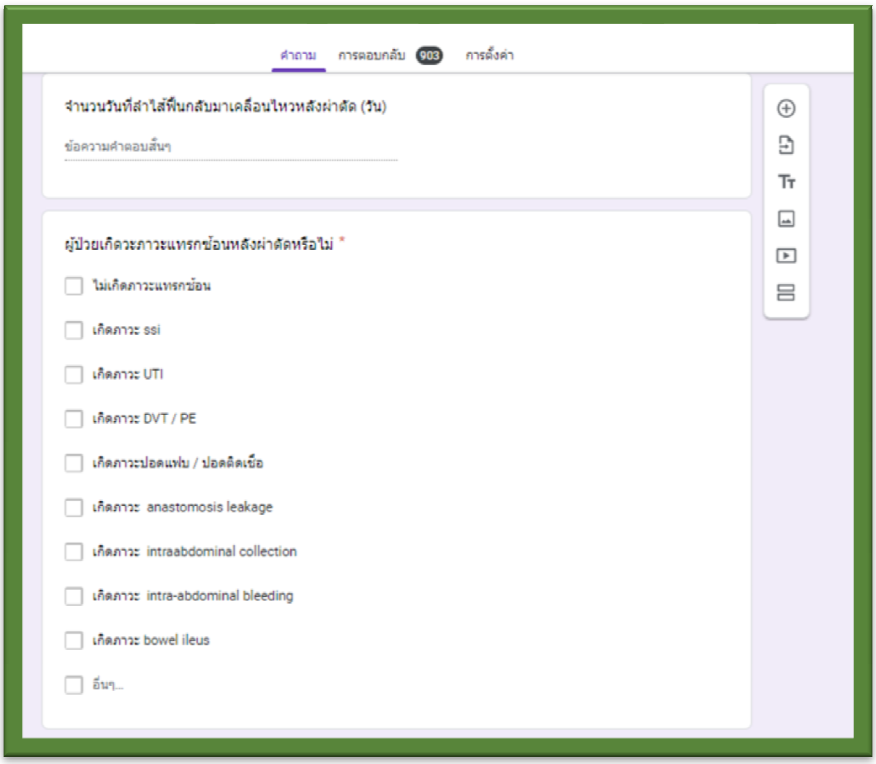

คำถาม
การตอบกลับ 903
การตั้งค่า
แบบฟอร์มรายงานcase colo
คำอธิบายแบบฟอร์ม
ชื่อย่อหน่วยงานของท่าน *
ข้อความคำตอบสั้นๆ
AN *
ข้อความคำตอบสั้นๆ

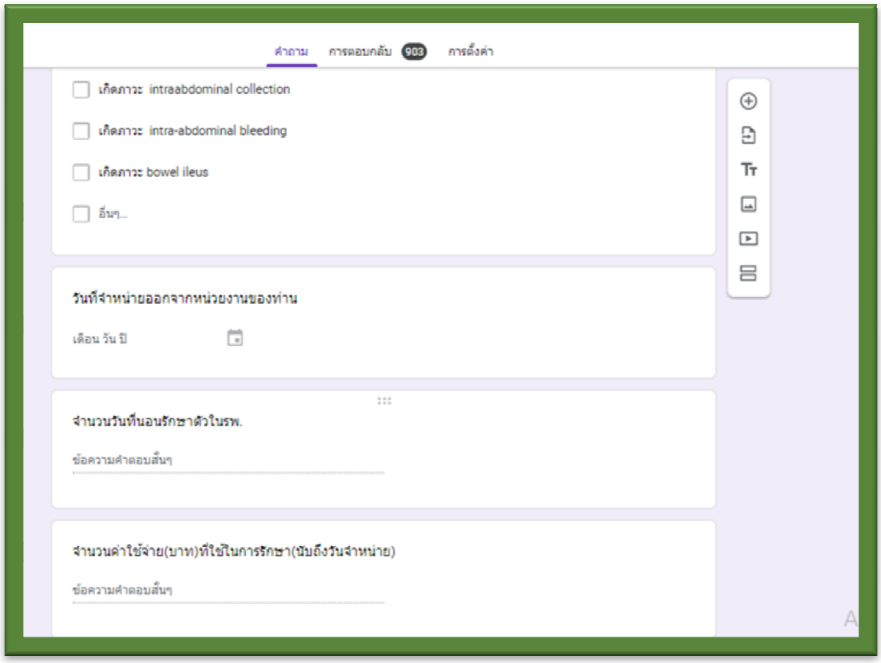

วันที่มาพบแพทย์ ณ ห้องตรวจOPDครั้งแรก
เดือน วัน ปี
วันที่ admission ในวชิรพยาบาล
เดือน วัน ปี
วันที่ admission ณ หน่วยงานของคุณ
เดือน วัน ปี

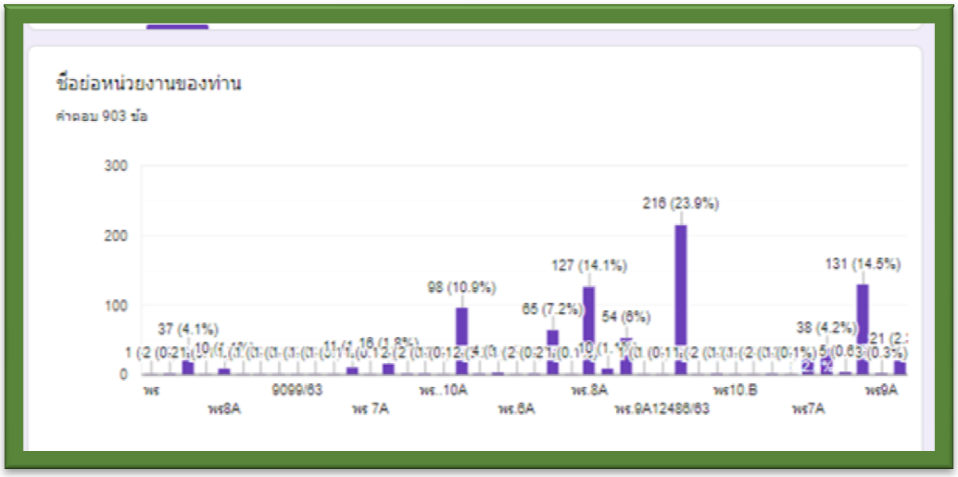

คำถาม
การตอบกลับ 903
การตั้งค่า
ระดับภาวะทุพโภชนาการก่อนผ่าตัด
0
1
2
3
4
วันที่ได้รับการผ่าตัด
เดือน วัน ปี
ประเภทการผ่าตัด
laparoscope
open / Explor lap
Lap to open


คำถาม
การตอบกลับ 903
การตั้งค่า
ชื่อหัตถการการผ่าตัด
ข้อความคำตอบสั้นๆ
ผ่าตัดเปิด ostomy หรือไม่
ไม่มี ostomy
sigmoid colostomy
loop transverse colostomy
ileostomy
อื่นๆ...
ได้รับการผ่าตัดซ้ำในการ admission ครั้งเดียวกัน
ใช่
ไม่ใช่

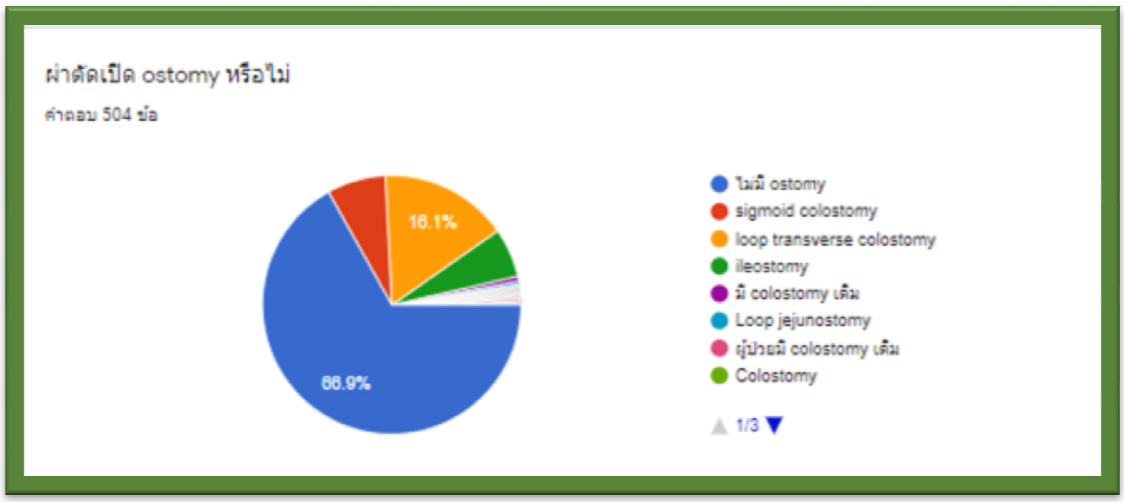

คำถาม
การตอบกลับ 903
การตั้งค่า
ได้รับการผ่าตัด revised colostomy
ใช่
ไม่ใช่
ผู้ป่วยได้รับการผ่าตัดเปิด colostomy โดยวางแผนล่วงหน้า
ใช่
ไม่ใช่
ผู้ป่วยเกิดภาวะ ostomy complication หรือไม่
ไม่เกิดภาวะแทรกซ้อน
เกิดภาวะ bleeding
เกิดภาวะ retraction
เกิดภาวะ skin excoriation (แผลรอบทวารใหม่)
เกิดภาวะ necrosis

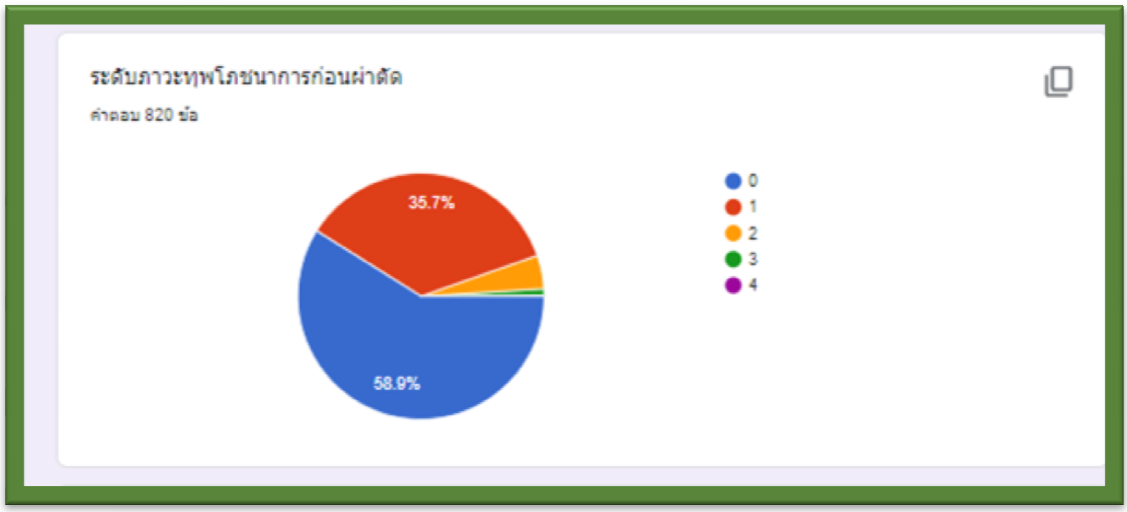

คำถาม
การตอบกลับ 903
การตั้งค่า
จำนวนวันที่สำไส้ฟื้นกลับมาเคลื่อนไหวหลังผ่าตัด (วัน)
ข้อความคำตอบสั้นๆ
ผู้ป่วยเกิดวะภาวะแทรกซ้อนหลังผ่าตัดหรือไม่ *
ไม่เกิดภาวะแทรกซ้อน
เกิดภาวะ ssi
เกิดภาวะ UTI
เกิดภาวะ DVT / PE
เกิดภาวะปอดแฟบ / ปอดติดเชื้อ
เกิดภาวะ anastomosis leakage
เกิดภาวะ intraabdominal collection
เกิดภาวะ intra-abdominal bleeding
เกิดภาวะ bowel ileus
อื่นๆ...

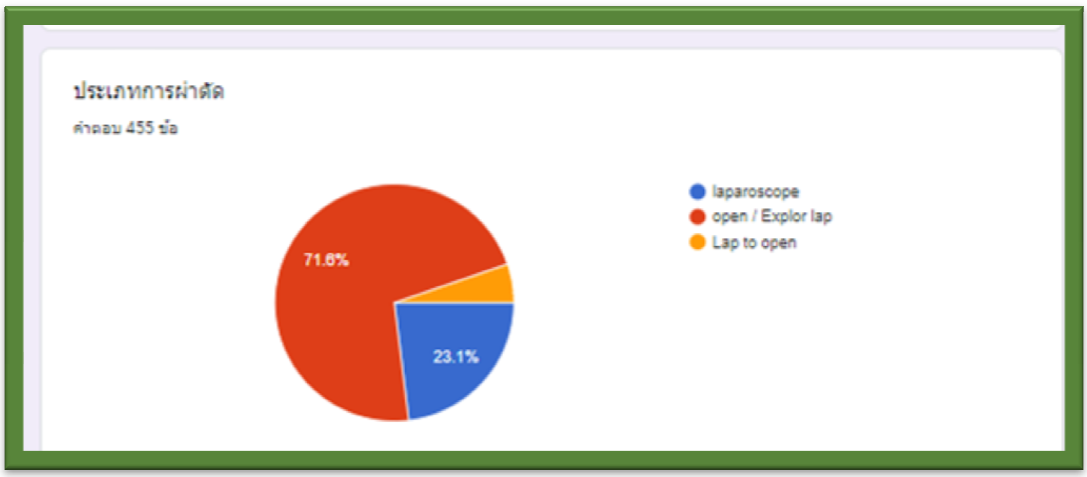

คำถาม
การตอบกลับ 903
การตั้งค่า
เกิดภาวะ intraabdominal collection
เกิดภาวะ intra-abdominal bleeding
เกิดภาวะ bowel ileus
อื่นๆ...
วันที่จำหน่ายออกจากหน่วยงานของท่าน
เดือน วัน ปี
จำนวนวันที่นอนรักษาตัวในรพ.
ข้อความคำตอบสั้นๆ
จำนวนค่าใช้จ่าย(บาท)ที่ใช้ในการรักษา(นับถึงวันจำหน่าย)
ข้อความคำตอบสั้นๆ

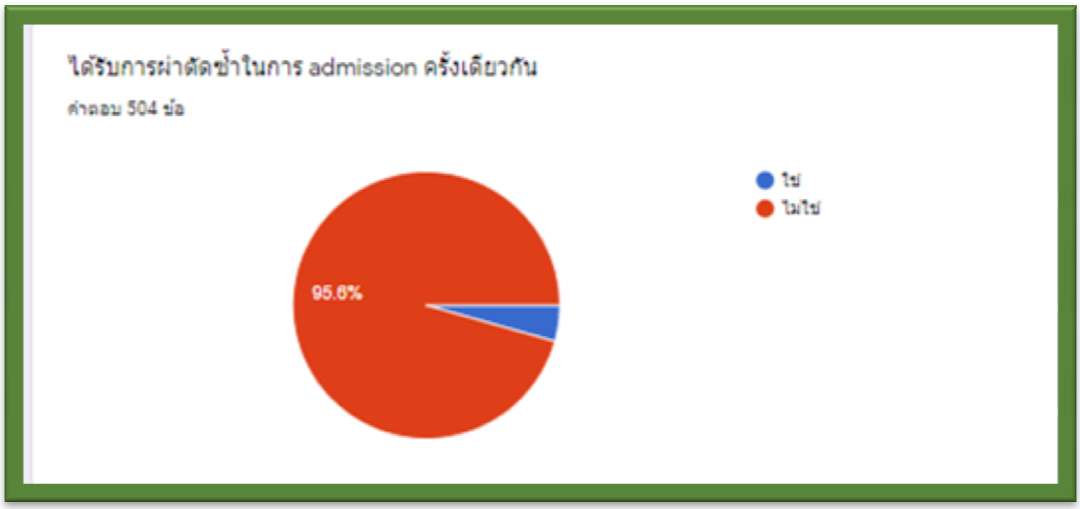

ชื่อย่อหน่วยงานของท่าน
ค่าตอบ 903 ข้อ
300
200
100
0
37 (4.1%)
98 (10.9%)
65 (7.2%)
127 (14.1%)
54 (6%)
216 (23.9%)
38 (4.2%)
131 (14.5%)
พร
พร8A
9099/63
พร 7A
พร..10A
พร.8A
พร.8A
พร.9A12486/63
พร10.B
พร7A
พร9A

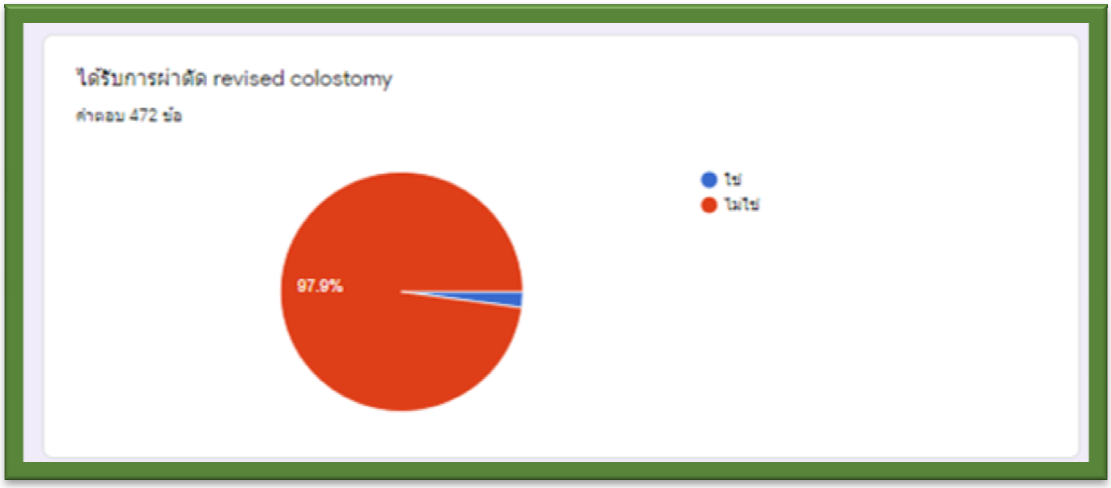

AN
ค่าตอบ 903 ข้อ
24122/61
8126/62
21224/61
20491/61
21846/61
718/62
8558/63
18300/62
13056/63

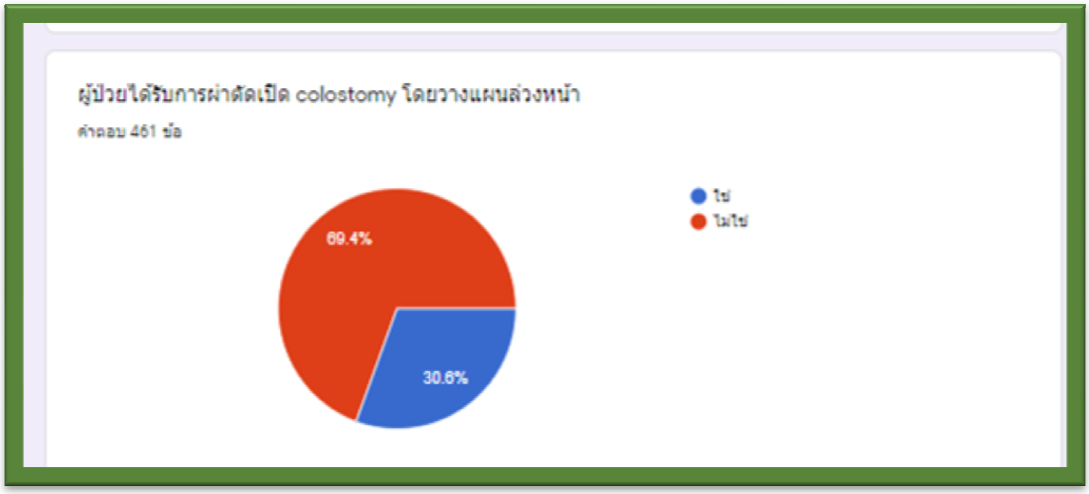

ผ่าตัดเปิด ostomy หรือไม่
ค่าตอบ 504 ข้อ
16.1%
66.9%
ไม่มี ostomy
sigmoid colostomy
loop transverse colostomy
ileostomy
มี colostomy เดิม
Loop jejunostomy
ผู้ป่วยมี colostomy เดิม
Colostomy
1/3

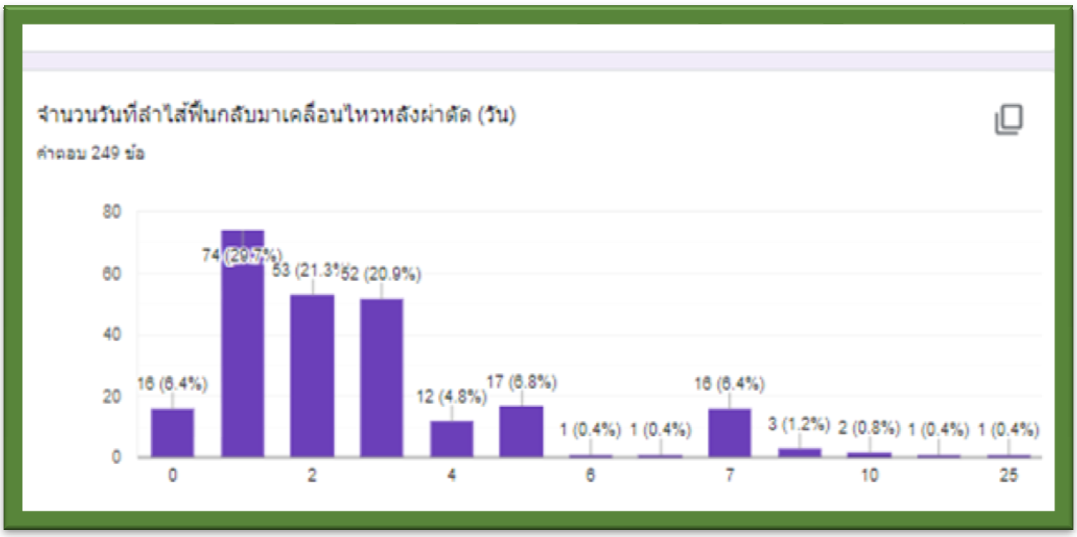

ระดับภาวะทุพโภชนาการก่อนผ่าตัด
ค่าตอบ 820 ข้อ
35.7%
58.9%
0
1
2
3
4

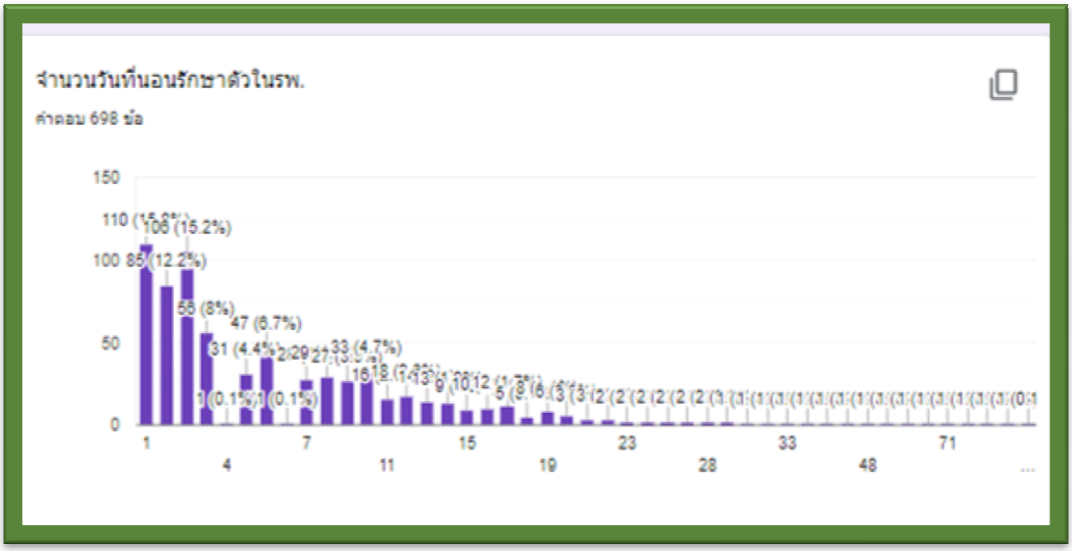

ประเภทการผ่าตัด
ตอบ 455 ข้อ
71.6%
23.1%
laparoscope
open / Explor lap
Lap to open


ได้รับการผ่าตัดซ้ำในการ admission ครั้งเดียวกัน
ตอบ 504 ข้อ
95.6%
ใช่
ไม่ใช่


ได้รับการผ่าตัด revised colostomy
คำตอบ 472 ข้อ
ใช่
ไม่ใช่
97.9%


ผู้ป่วยได้รับการผ่าตัดเปิด colostomy โดยวางแผนล่วงหน้า
คำตอบ 461 ข้อ
ใช่
ไม่ใช่
69.4%
30.6%


จำนวนวันที่สำไส้ฟื้นกลับมาเคลื่อนไหวหลังผ่าตัด (วัน)
ค่าตอบ 249 ข้อ
80
60
40
20
0
74 (29.7%)
53 (21.3%)
52 (20.9%)
16 (6.4%)
12 (4.8%)
17 (6.8%)
1 (0.4%)
1 (0.4%)
16 (6.4%)
3 (1.2%)
2 (0.8%)
1 (0.4%)
1 (0.4%)
0
2
4
6
7
10
25


จำนวนวันที่นอนรักษาตัวในรพ.
ค่าตอบ 698 ข้อ
150
110
100
50
0
106 (15.2%)
85 (12.2%)
55 (8%)
47 (6.7%)
31 (4.4%)
33 (4.7%)
1
4
7
11
15
19
23
28
33
48
71

ภาคผนวก จ
หนังสือรับรองการนำคู่มือการปฏิบัติงานมาใช้จริงในหน่วยงาน

บันทึกข้อความ

ส่วนงาน ฝ่ายการพยาบาล โรงพยาบาลวชิรพยาบาล (ผู้ปฏิบัติการพยาบาลขั้นสูง โทร. ๓๐๗๖)
ที่ **วันที่** ๑๒ ธันวาคม ๒๕๖๒
เรื่อง ขอรับรองการนำคู่มือการปฏิบัติงานมาใช้จริงในหน่วยงาน

เรียน หัวหน้าฝ่ายการพยาบาล

ด้วย ข้าพเจ้านางสาวธมลวรรณ ยอดกลกิจ ได้จัดทำคู่มือการปฏิบัติงาน เรื่อง "การจัดการข้อมูลตัวชี้วัดเชิงผลลัพธ์ทางการพยาบาลโดยใช้เว็บแอพลิเคชั่นในกลุ่มโรคลำไส้ใหญ่และทวารหนัก" เพื่อพัฒนาการสื่อสารส่งต่อข้อมูลตัวชี้วัดทางการพยาบาลของบุคลากรพยาบาล ให้มีการสื่อสารข้อมูลที่ถูกต้อง รวดเร็ว ครบถ้วน และต่อเนื่องลดการใช้ทรัพยากร โดยการใช้หลักแนวคิด LEAN ที่ครอบคลุมความปลอดภัย พิทักษ์สิทธิ์ทั้งผู้ป่วยและบุคลากรผู้ดูแลผู้ป่วย ทั้งนี้ได้เริ่มดำเนินการจัดทำคู่มือและนำคู่มือมาใช้ในทีมพัฒนาคุณภาพการดูแลผู้ป่วยกลุ่มโรคลำไส้ใหญ่และทวารหนัก ตั้งแต่วันที่ ๑ มกราคม ๒๕๖๑ เป็นต้นมา และในขณะนี้ยังคงใช้คู่มือปฏิบัติงานนี้อยู่

ดังนั้น ข้าพเจ้าจึงมีความประสงค์ขอคำรับรองว่า คู่มือการปฏิบัติงานดังกล่าวนี้ได้นำมาใช้จริงในหน่วยงาน เพื่อใช้ประกอบการขอประเมินเพื่อแต่งตั้งให้ดำรงตำแหน่งพยาบาลวิชาชีพชำนาญการพิเศษ

จึงเรียนมาเพื่อโปรดพิจารณา

(นางสาวธมลวรรณ ยอดกลกิจ)
พยาบาลวิชาชีพชำนาญการ
ฝ่ายการพยาบาล โรงพยาบาลวชิรพยาบาล
คณะแพทยศาสตร์วชิรพยาบาล

(นางสาวดวงเนตร์ ภู่วัฒนวนิชย์)
พยาบาลวิชาชีพชำนาญการพิเศษ
หัวหน้าฝ่ายการพยาบาล
โรงพยาบาลวชิรพยาบาล

ประวัติผู้เขียน

ประวัติผู้เขียน

ชื่อสกุล	นางสาวธมลวรรณ ยอดกลกิจ
วัน เดือน ปี เกิด	31 ตุลาคม 2520
สถานที่เกิด	จังหวัดกรุงเทพมหานคร
สถานที่อยู่ปัจจุบัน	5/696 หมู่10 ตำบล บางตลาด อำเภอ ปากเกร็ด จังหวัด นนทบุรี
ตำแหน่งและประวัติการทำงาน	
พ.ศ. 2541-2548	พยาบาลวิชาชีพ 3-6 (ด้านการพยาบาล)ฝ่ายการพยาบาล วิทยาลัยแพทยศาสตร์กรุงเทพมหานครและวชิรพยาบาล สำนักการแพทย์
พ.ศ. 2548-2555	พยาบาลวิชาชีพ 6 ว – 7 วช (ด้านการพยาบาล)ฝ่ายการพยาบาล โรงพยาบาลวชิรพยาบาล คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยกรุงเทพมหานคร
พ.ศ.2555-2561	พยาบาลวิชาชีพ 7 วช ฝ่ายการพยาบาล คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช
พ.ศ.2561-ปัจจุบัน	ผู้ปฏิบัติการพยาบาลขั้นสูง ฝ่ายการพยาบาล โรงพยาบาลวชิรพยาบาล คณะแพทยศาสตร์วชิรพยาบาล มหาวิทยาลัยนวมินทราธิราช
ประวัติการศึกษา	
พ.ศ. 2541	พยาบาลศาสตรบัณฑิต วิทยาลัยพยาบาลเกื้อการุณย์ (มหาวิทยาลัยมหิดล) (ประเทศไทย)
พ.ศ. 2548	วิทยาศาสตรมหาบัณฑิต(สุขศึกษา) มหาวิทยาลัยศรีนครินทรวิโรฒ ประสานมิตร
พ.ศ. 2560	ผู้ปฏิบัติการพยาบาลขั้นสูง ระดับวุฒิบัตร การพยาบาลผู้ใหญ่และผู้สูงอายุ แขนงโรคเรื้อรัง (สภาการพยาบาล ประเทศไทย)