แนวปฏิบัติการจัดการด้านความปลอดภัย ความเสี่ยงของระบบฐานข้อมูล และเครือข่ายเทคโนโลยีสารสนเทศ คณะทันตแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ ปี ๒๕๖๘

สารบัญ

ความเป็นมา

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ มีความมั่นคงปลอดภัย เชื่อถือได้ งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ คณะทันตแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ จึงได้กำหนดนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยสามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่าง ๆ ตลอดจนการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง

๒. วัตถุประสงค์

งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ คณะทันตแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ กำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๒. เพื่อให้เกิดความเชื่อมั่นด้านความปลอดภัย การใช้ระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพและประสิทธิผล

๒.๓. เพื่อเผยแพร่แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ทุกระดับ นักศึกษา - และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร มีความรู้ ความเข้าใจและถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด

๒.๔. เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของงานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศมีรายละเอียดดังต่อไปนี้

๓.๑. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของคณะทันตแพทยศาสตร์

๓.๒. เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๓. เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับที่เกี่ยวข้อง

๓.๔. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๔. องค์ประกอบของแนวปฏิบัติ

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องและเป็นไปตามแนวปฏิบัติที่กำหนดไว้ โดยมีรายละเอียดดังต่อไปนี้

ส่วนที่ ๑ แนวปฏิบัติควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของคณะทันตแพทยศาสตร์
๒. การบริหารจัดการบัญชีผู้ใช้และการเข้าถึงของผู้ใช้งาน
๓. การควบคุมการเข้าถึงระบบเครือข่าย
๔. การใช้งานอินเทอร์เน็ต
๕. การบริหารจัดการคอมพิวเตอร์แม่ข่าย
๖. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
๗. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ
๘. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ
๙. การตรวจสอบความถูกต้องของข้อมูล

ส่วนที่ ๒ แนวปฏิบัติการบำรุงการรักษาคอมพิวเตอร์อุปกรณ์และการจัดการข้อมูลในเครื่องคอมพิวเตอร์

ส่วนที่ ๓ แนวปฏิบัติการปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์

ส่วนที่ ๔ แนวปฏิบัติการจัดทำระบบสำรองสารสนเทศ

ส่วนที่ ๕ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

ส่วนที่ ๖ แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๗ แนวปฏิบัติการแก้ไขปัญหาระบบสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน

ส่วนที่ ๘ แนวการจัดการผู้ใช้ควบคุมการเข้าถึงระบบกล้องวงจรปิด

ส่วนที่ ๑
แนวปฏิบัติควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของคณะ

๒. เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจและปฏิบัติตามขั้นตอนโดยเคร่งครัด

ผู้รับผิดชอบ

๑. งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕

๒. สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของคณะทันตแพทยศาสตร์

๑.๑. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน

๑.๑.๑. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

๑.๒. กำหนดสิทธิ์การเข้าถึงข้อมูลและสารสนเทศของคณะ ดังนี้

๑.๒.๑. ไม่มีสิทธิ์

๑.๒.๒. อ่านได้อย่างเดียว

๑.๒.๓. สร้างข้อมูล

๑.๒.๔. ป้อนข้อมูล

๑.๒.๕. แก้ไขข้อมูล

๑.๒.๖. ลบข้อมูล

๑.๒.๗. อนุมัติการใช้ข้อมูล

๑.๓. กำหนดประเภทข้อมูลของคณะ

๑.๓.๑. ข้อมูลนักศึกษา

๑.๓.๒. ข้อมูลบุคลากร

๑.๓.๓. ข้อมูลการเงินและบัญชี

๑.๓.๔. ข้อมูลพัสดุ

๑.๓.๕. ข้อมูลการบริหาร

๑.๓.๖. ข้อมูลผู้ป่วย

๑.๔. เกณฑ์ในการกำหนดระดับชั้นความลับของข้อมูลและสารสนเทศของคณะ

๑.๔.๑. ลับ รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง

๑.๔.๒. ใช้ภายในเท่านั้น เป็นข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างภายในหน่วยงาน หรือข้อมูลเผยแพร่เฉพาะภายในเท่านั้น

๑.๔.๓. ส่วนบุคคล ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลนั้น

๑.๔.๔. เปิดเผยได้ เป็นข้อมูลที่เปิดเผยได้ทั้งภายได้ทั้งภายในและภายนอกคณะ

๑.๕. กำหนดระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของคณะ

๑.๕.๑. การเข้าถึงสำหรับผู้บริหาร

๑.๕.๒. การเข้าถึงสำหรับผู้ปฏิบัติงานตามภาระหน้าที่

๑.๕.๓. การเข้าถึงสำหรับผู้ดูแลระบบ

๑.๕.๔. การเข้าถึงสำหรับบุคคล

๑.๖. เกณฑ์การแบ่งระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของคณะ

๑.๖.๑. ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น

๑.๖.๒. ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย

๑.๖.๓. ผู้ดูแลระบบ มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่

๑.๖.๔. บุคคล เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้อนุญาตให้เข้าถึงได้

๑.๖.๕. การกำหนดสิทธิ์พิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูลเท่านั้น

๑.๖.๖. การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิ์หรือหน่วยงานหลักเท่านั้น

๑.๗. กำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศของคณะในแต่ละประเภทดังนี้

๑.๗.๑. ข้อมูลนักศึกษา หน่วยงานหลักคือ งานการศึกษา

๑.๗.๒. ข้อมูลบุคลากร หน่วยงานหลักคือ หน่วยอำนวยการและบริหารทรัพยากรบุคคล

๑.๗.๓. ข้อมูลพัสดุ ครุภัณฑ์ การเงิน บัญชี หน่วยงานหลักคือ งานคลังและพัสดุ และหน่วยเงินรายได้ดูแลในส่วนของเงินรายได้ที่เกิดจากโรงพยาบาลทันตกรรม

๑.๗.๔. ข้อมูลทางการบริหาร หน่วยงานหลัก คือ

(๑) งานยุทธศาสตร์และบริหารทรัพยากรบุคคล ดูแลข้อมูลการบริหารจัดการ แผนยุทธศาสตร์ บุคลากร งบประมาณ และอัตรากำลัง

(๒) งานพัฒนางานวิจัยและนวัตกรรม ดูแลพัฒนางานวิจัย ปฏิบัติการเครื่องมือวิจัย

(๓) สำนักงานจริยธรรมดูแลโครงการวิจัยที่ดำเนินการเกี่ยวข้องกับมนุษย์

(๔) งานคลังและพัสดุ ดูแลในส่วนของการจัดการงบประมาณทั้งหมดภายในคณะ

(๕) งานอาคาร วิศวกรรมและซ่อมบำรุง ดูแลในส่วนระบบกล้องวงจรปิด รักษาความปลอดภัยในส่วนภาพรวมของคณะ

๑.๗.๕. ข้อมูลผู้ป่วย หน่วยงานหลักคือ โรงพยาบาลทันตกรรม

รายละเอียดช่องทางการติดต่อหน่วยงานผู้ดูแลข้อมูลแต่ละประเภท แสดงดังภาคผนวก ก

๑.๘. การควบคุมการเปลี่ยนแปลง

๑.๘.๑. การเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ให้ดำเนินการ ดังนี้

(๑) พิจารณาวางแผนดำเนินการเปลี่ยนแปลง รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการเปลี่ยนแปลง

(๒) แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการเปลี่ยนแปลงนั้น ๆ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลง

(๓) ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลง

๑.๘.๒. จัดเก็บซอร์สโค้ดและไลบรารี่ของระบบสารสนเทศทั้งเวอร์ชั่นปัจจุบันและ เวอร์ชั่นเก่าไว้ในสถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็น

๑.๙. การกำหนดการใช้งานตามภารกิจ

๑.๙.๑. การควบคุมการเข้าถึงระบบสารสนเทศ

(๑) นักศึกษา จะให้สิทธิ์เมื่องานการศึกษาได้ทำหนังสือแจ้งมาทางงานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ และจะหมดสิทธิ์เมื่อจบการศึกษาหรือพ้นสภาพการเป็นนักศึกษา

(๒) บุคลากร จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นบุคลากร

(๓) ผู้บริหาร จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นผู้บริหาร

(๔) บุคคลภายนอก ได้รับอนุญาตเฉพาะระบบและช่วงเวลาที่กำหนด

๑.๙.๒. ข้อจำกัดในการเข้าถึง

(๑) นักศึกษา เข้าถึงได้เฉพาะระบบที่ได้รับอนุญาต

(๒) บุคลากร เข้าถึงได้ตามสิทธิ์เบื้องต้นและภารกิจที่ได้รับมอบหมาย

(๓) ผู้บริหาร เข้าถึงตามสิทธิ์และภารกิจที่ได้รับมอบหมาย

(๔) บุคคลภายนอก เข้าถึงได้ตามสิทธิ์ที่ได้รับอนุญาต

๑.๑๐. ระยะเวลาการใช้งาน

ระยะเวลาการเข้าถึงและการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศ ผู้ใช้งานจะเข้าถึงและใช้งานได้ตลอด ๒๔ ชั่วโมงโดยมีข้อมูลที่บริการทั้งบนระบบอินเทอร์เน็ตและระบบอินทราเน็ตที่จำกัดขอบเขตกลุ่มผู้ใช้งานโดยอนุญาตให้ผู้มีสิทธิเข้าใช้งาน คือ สมาชิกภายในองค์กรเท่านั้น

๑.๑๑. การหมดสิทธิ์การเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ

๑.๑๑.๑. บัญชีผู้ใช้หมดอายุ

๑.๑๑.๒. เมื่อมีการเปลี่ยนแปลงสิทธิ์การเข้าถึง

๑.๑๑.๓. ถูกระงับสิทธิ์

๑.๑๒. การทบทวนและการตรวจสอบสิทธิ์การเข้าถึงและการใช้งานข้อมูล สารสนเทศ และระบบสารสนเทศ

๑.๑๒.๑. ทบทวนและตรวจสอบสิทธิ์การเข้าถึงและใช้งานระบบสารสนเทศ โดยหน่วยอำนวยการและบริหารทรัพยากรบุคคล และงานการศึกษา จะส่งรายชื่อที่ลาออก จบการศึกษาหรือมีการเปลี่ยนแปลงไปยังหน่วยงานที่เกี่ยวข้อง

๑.๑๒.๒. หน่วยงานผู้ขอสิทธิ์แจ้งกลับผู้ดูแลระบบเพื่อดำเนินการแก้ไขให้ถูกต้อง

๑.๑๒.๓. หน่วยงานที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิ์ของผู้ใช้อย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องดำเนินการแจ้งผู้ดูแลระบบเพื่อดำเนินการเปลี่ยนแปลงสิทธิ์ให้สอดคล้องกับระดับชั้นการเข้าถึงทันที

๑.๑๓. ช่องทางการเข้าถึง

๑.๑๓.๑. เครือข่ายภายใน

๑.๑๓.๒. เครือข่ายภายนอก

๑.๑๓.๓. เข้าถึงโดยผ่านระบบที่จัดไว้ให้

๒. การบริหารจัดการบัญชีผู้ใช้และการเข้าถึงของผู้ใช้งาน

๒.๑. การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งาน

๒.๑.๑. การอบรมผู้ใช้งาน

(๑) ระบบสารสนเทศและข้อมูลสารสนเทศทั่วไป มีการอบรมการใช้งานระบบ ตามแผนการอบรมคอมพิวเตอร์ประจำปี รวมทั้งกรณีการส่งมอบระบบที่งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศได้พัฒนาขึ้น

(๒) ระบบสารสนเทศและข้อมูลสารสนเทศทางด้านการเรียนการสอน การประเมินผลการศึกษา และระบบฐานข้อมูลผู้ป่วย โดยหลังจากอบรมจะมีการวัดผลประเมินผลการเข้าร่วมอบรม ด้วยข้อสอบที่งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศจัดทำขึ้น มีการรายงานผลการสอบไปยังหน่วยงานต้นสังกัด ในกรณีนักศึกษา จะรายงานผลไปยังหน่วยทะเบียนและประเมินผลการศึกษา หรือหน่วยบัณฑิตศึกษา และมีการทวนอบรมซ้ำทุกปี เพื่อผู้ใช้งานทราบถึงนโยบายและขั้นตอนการบันทึกข้อมูลทางสารสนเทศที่เป็นปัจจุบัน

๒.๑.๒. การจัดทำคู่มือการใช้งานระบบ เพื่อผู้ใช้งานสามารถทวนศึกษาวิธีการใช้งานระบบได้ด้วยตนเอง

๒.๒. การแบ่งกลุ่มบัญชีผู้ใช้งาน

๒.๒.๑. นักศึกษา

๒.๒.๒. บุคลากรภายในคณะ

๒.๒.๓. ผู้บริหาร

๒.๒.๔. บุคคลภายนอก เช่น อาจารย์พิเศษ ทันตแพทย์คลินิกนอกเวลา ผู้ช่วยทันตแพทย์รายคาบ

๒.๓. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๒.๓.๑. ระบบสารสนเทศสนับสนุนงานสำนักงานเลขานุการ และระบบสารสนเทศสนับสนุนการเรียนการสอน มีระบบแสดงตัวตน โดยใช้ login ของ PSU Passport แบบเดียวกับมหาวิทยาลัย

๒.๓.๒. ระบบสารสนเทศโรงพยาบาล จะมีการตั้งค่าให้ระบบป๊อปอัพเตือนผู้ใช้งานตั้งรหัสผ่านใหม่ ซึ่งห้ามซ้ำกับรหัสผ่านเดิมทุก ๆ ๙๐ วัน และผู้ใช้งานจะต้องลงชื่อเข้าใช้ระบบใหม่หากเปิดระบบค้างไว้เกิน ๑๘๐ นาที โดยมีขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยดังนี้

(๑) **<u>รูปแบบของรหัสผ่านจะต้องมีอย่างน้อย ๔ หลัก</u>** ประกอบด้วย

- ตัวอักษรพิมพ์ใหญ่อย่างน้อย ๑ ตัว
- ตัวอักษรพิมพ์เล็กอย่างน้อย ๑ ตัว
- ตัวเลข หรือสัญลักษณ์ อย่างใดอย่างหนึ่งก็ได้ มีหรือไม่มีก็ได้

(๒) ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราว โดยการกำหนดรหัสผ่านให้มีความยากต่อการคาดเดาและกำหนดให้แตกต่างกัน ซึ่งรูปแบบของรหัสผ่านชั่วคราวประกอบด้วย รหัสตัวอักษรที่ตั้งขึ้นโดยแบ่งตามกลุ่มผู้ใช้งาน และรหัสบัตรประชาชน ๔ หลักสุดท้ายของผู้ใช้งาน

(๓) ผู้ดูแลระบบจัดส่งรหัสผ่านให้ผู้ใช้งานโดยตรง โดยกำหนดให้ผู้ใช้งานกรอกแบบฟอร์มขอรหัสผู้ใช้งาน พร้อมรายละเอียดข้อมูลส่วนบุคคล และจัดส่งให้ผู้ใช้งานโดยตรงทางอีเมล์ที่ระบุมาในแบบฟอร์ม

(๔) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากได้รับรหัสผ่านชั่วคราว ซึ่งผู้ดูแลระบบจัดทำแบบฟอร์มแจ้งรหัสผู้ใช้ และวิธีการเปลี่ยนรหัสผ่านให้แก่ผู้ใช้งานผ่านทางอีเมล์ (ระบบไม่มีให้ตั้งค่าเปลี่ยนรหัสทันที จึงทำเป็นข้อบังคับผ่านแบบฟอร์มแจ้งรหัสผู้ใช้แทน)

(๕) กรณีผู้ใช้ลืมรหัสผ่าน ต้องดำเนินการกรอกฟอร์ม E-request เพื่อให้งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศตั้งค่ารหัสผ่านให้ใหม่

๒.๔. การบริหารจัดการการเข้าถึงข้อมูลผู้ป่วย

๒.๔.๑. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลผู้ป่วยภายในระบบตามบทบาทหน้าที่ของผู้ใช้งาน

๒.๔.๒. ผู้ดูแลระบบต้องกำหนดแนวทางการส่งออก ข้อมูลผู้ป่วยภายในระบบตามบทบาทหน้าที่ของผู้ใช้งาน

การส่งออกข้อมูลมีหลายวัตถุประสงค์ ดังนี้

(๑) การขอข้อมูลเพื่อรายงานและ/หรือ ช่วยในการตัดสินใจของผู้บริหาร ผู้ขอข้อมูลกรอกฟอร์มผ่านระบบ E-Request

(๒) การขอข้อมูลเพื่อการวิจัย

(๓) การขอข้อมูลเพื่อประกอบการเรียนการสอน

ทั้งนี้ ได้มีการกำหนดแนวปฏิบัติในข้อ (๒) และ (๓) ดังแผนภาพด้านล่างนี้

แนวปฏิบัติการบริหารจัดการรหัสผู้ใช้งาน
ในระบบฐานข้อมูลโรงพยาบาลทันตกรรม (HOSxPXE)

แผนภาพที่ ๑ แนวปฏิบัติการบริหารจัดการรหัสผู้ใช้งาน ในระบบ HOSxPXE

แนวปฏิบัติการขอใช้ข้อมูลเพื่อการวิจัย
ในระบบฐานข้อมูลโรงพยาบาลและระบบการประเมินผลคลินิก

ผู้วิจัยยื่น

๑. กรอกรายละเอียดในแบบคำร้อง E-Request พร้อมแนบหลักฐานต่อไปในรูปแบบ electronic file ส่งผ่านระบบ E-Doc มายังงานไอที
๒. หนังสือรับรองโครงการวิจัยจากคณะกรรมการจริยธรรมการวิจัย คณะทันตแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์
๓. เอกสารโครงการวิจัย
๔. เอกสารแสดงรายละเอียดถึงวิธีการจัดการข้อมูลวิจัยให้ปลอดภัย ซึ่งได้รับความเห็นชอบจากคณะกรรมการจริยธรรมวิจัย หากเป็นการขอข้อมูล identified data (ระบุตัวตน) จะต้องมีหนังสือแสดงความยินยอมจากอาสาสมัครวิจัย
๕. บันทึกข้อความขออนุเคราะห์ดำเนินการวิจัย ซึ่งได้รับการเห็นชอบจากรองคณบดีฝ่ายโรงพยาบาล / รองคณบดีฝ่ายการศึกษาและวิเทศสัมพันธ์
๖. แบบบันทึกข้อมูลสำหรับการวิจัย หรือแบบฟอรมข้อมูลสถิติทางการแพทย์ (ถ้ามี)
๗. รายละเอียดแสดงชนิดของข้อมูล / ตัวแปรต่าง ๆ ที่ต้องการบันทึกใน Excel file

↓

ค่าบริการเตรียมข้อมูลเพื่อการวิจัย

สำหรับ : บุคลากร/หน่วยงานภายในคณะทันตฯ

รูปแบบรายงานละ ๖๐๐ - ๑,๐๐๐ บาท/ช.ม.
การดึงข้อมูลขั้นต่ำ ๑,๐๐๐ บาท ข้อมูลไม่เกิน ๑,๐๐๐ รายการ
ข้อมูลที่ ๑,๐๐๑ Record ขึ้นไป
คิดค่าดำเนินการ ๑.๕ บาท/รายการ

สำหรับ : บุคลากร/หน่วยงานภายนอกคณะทันตฯ

รูปแบบรายงานละ ๙๐๐ - ๑,๕๐๐ บาท/ช.ม.
การดึงข้อมูลขั้นต่ำ ๑,๕๐๐ บาท ข้อมูลไม่เกิน ๑,๐๐๐ รายการ
ข้อมูลที่ ๑,๐๐๑ Record ขึ้นไป
คิดค่าดำเนินการ ๒ บาท/รายการ
(ข้อมูลอ้างอิง : รายละเอียดค่าบริการของสำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ (ศูนย์คอมฯ) แนบท้ายประกาศสำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ (ศูนย์คอมฯ) ฉบับลงวันที่ ๓๑ ก.ค. ๖๒) (https://www.cc.psu.ac.th/pdf/ccpsu-services2019.pdf)

หมายเหตุ กรณีที่ผู้วิจัยเป็นบุคลากรหรือหน่วยงานภายในคณะฯ ไม่ได้รับทุนวิจัยสนับสนุนหรือรับทุนสนับสนุนจากกองทุนวิจัย คณะทันตฯ ให้ยื่นคำร้องขอยกเว้นค่าบริการเตรียมข้อมูลเพื่อการวิจัย โดยผ่านความคิดเห็นของผู้บังคับบัญชาต้นสังกัด

↓

ชำระเงิน ตามอัตราค่าบริการได้ที่งานคลัง ชั้น ๓ อาคาร ๓ คณะทันตแพทยศาสตร์ นำใบเสร็จแสดงหลักฐานการชำระค่าบริการ ยื่นที่งานเทคโนโลยีสารสนเทศ → ข้อมูลที่จัดเตรียมจะสามารถเข้าถึงได้โดยผ่านระบบอินทราเน็ต เจ้าหน้าที่ IT จัดเตรียม file ให้ในรูปแบบ excel file โดยใช้ password ที่กำหนดให้ ซึ่งมีระยะเวลาในการเข้าถึงข้อมูล ๙๐ วัน หลังจากนั้นจะถูกทำลาย หากผู้วิจัยต้องการข้อมูลเดิมอีกภายหลังจาก ๙๐ วันจะต้องยื่นคำขอและมีค่าบริการใหม่

แผนภาพที่ ๒ แนวปฏิบัติการขอใช้ข้อมูลเพื่อการวิจัย ในระบบ HOSxPXE และระบบการประเมินผลคลินิก

๓. การควบคุมการเข้าถึงระบบเครือข่าย

๓.๑. การเข้าใช้งานระบบเครือข่าย

๓.๑.๑. การเข้าถึงระบบเครือข่ายจะต้องพิสูจน์ตัวตนผู้ใช้งานด้วยบัญชีผู้ใช้ที่มหาวิทยาลัยออกให้ทุกครั้งก่อนใช้งาน

๓.๑.๒. การเข้าถึงระบบเครือข่ายจากภายนอกต้องมีการพิสูจน์ตัวตน

๓.๑.๓. จะต้องใช้ชุด IP Address ที่มหาวิทยาลัยเป็นผู้กำหนดให้เท่านั้น

๓.๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๓.๒.๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายจะต้องทำการลงทะเบียนกับผู้ดูแลระบบ (สำหรับผู้ที่ยังไม่มี PSU Passport จะต้องให้ผู้ดูแลระบบลงทะเบียนด้วยบัตรประชาชนก่อน)

๓.๒.๒. ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้

(๑) ลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นำมาใช้ในระบบเครือข่ายไร้สาย

(๒) ควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณเพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๓) ทำการเปลี่ยนค่า SSID เป็นตามมหาวิทยาลัย

(๔) เปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตี ไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย

(๕) เข้ารหัสข้อมูลระหว่าง wireless LAN client และอุปกรณ์กระจายสัญญาณ ด้วยวิธีที่มีความประสิทธิภาพไม่ด้อยกว่าวิธี WPA2 (Wi-Fi Protected Access) เพื่อให้ยากต่อการดักจับข้อมูล และทำให้ปลอดภัยมากขึ้น

(๖) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย รวมไปถึงคอยตรวจสอบผู้ใช้ที่มีการใช้งานเครือข่ายมากผิดปกติ

(๗) มีการใช้ Label เพื่อให้ง่ายต่อการตรวจสอบ ทั้งเป็นการติดที่ตัว Hardware และระบุใน Software Controller

(๘) หากมีการติดตั้งอุปกรณ์กระจายสัญญาณเพิ่มเติม จะต้องเป็นรุ่นที่มีความเข้ากันได้กับระบบและ Software ที่ใช้งานอยู่ในปัจจุบันเป็นหลักเท่านั้น

๓.๓. การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนเครือข่าย

๓.๓.๑. อุปกรณ์ที่นำมาเชื่อมต่อได้รับหมายเลขไอพีแอดเดรสตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

๓.๓.๒. เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการ และกำหนดค่าหมายเลขไอพีแอดเดรสบน DHCP Server

๓.๓.๓. มีการแบ่ง Zoning ของ IP Address เพื่อให้ง่ายต่อการ Tracking หรือในบาง Zoning จะมีการระบุ IP Address ของ Device ก่อนการใช้งาน

๓.๓.๔. ในจุดที่มีห้ามนำอุปกรณ์อื่นมาต่อพ่วงเพิ่ม จะมีการ ป้องกันการจ่าย IP มากกว่า 1 Address / จุด

๓.๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๓.๔.๑. ควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

๓.๔.๒. กำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

๓.๔.๓. ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกมหาวิทยาลัย แต่ให้เชื่อมต่อผ่านช่องทางที่ปลอดภัยที่มหาวิทยาลัยกำหนด เช่น VPN เป็นต้น

๓.๔.๔. อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความปลอดภัย

๓.๔.๕. ต้องปิดพอร์ตหรือปิดบริการ บนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๓.๔.๖. ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งาน

๓.๕. การแบ่งแยกเครือข่าย

๓.๕.๑. จัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๕.๒. แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้ และระบบงานต่าง ๆ

๓.๕.๓. สร้าง VLAN เพื่อแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ

๓.๕.๔. มีการตั้งค่า ACL ของเครือข่ายแต่ละเครือข่ายให้เข้าถึง/ไม่สามารถเข้าถึง อีกเครือข่ายได้ เพื่อรักษาความปลอดภัยให้กับเครือข่ายภายในบางเครือข่าย

๓.๕.๕. ใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงาน ซึ่งสอดคล้องกับแนวปฏิบัติควบคุมการเข้าถึงและการใช้งานบริการเครือข่ายของหน่วยงาน

๓.๕.๖. มี อุปกรณ์ Firewall กั้นระหว่างเครือข่ายที่ใช้ Internet และเครือข่ายระบบโรงพยาบาลเพื่อรักษาความปลอดภัยของเครือข่ายเพิ่มขึ้น

๓.๖. การควบคุมการเชื่อมต่อทางเครือข่าย

๓.๖.๑. อนุญาตการเชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น

๓.๖.๒. ในกรณีที่ผู้ดูแลระบบตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติต่อระบบเครือข่ายหลัก จะทำการหยุดให้บริการโดยการตัดการเชื่อมต่อกับระบบเครือข่าย โดยไม่มีการแจ้งให้ทราบล่วงหน้า จนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

๓.๗. การควบคุมการจัดเส้นทางบนเครือข่าย

๓.๗.๑. อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด

๓.๗.๒. ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

๓.๗.๓. ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการ ติดตั้งเครือข่ายแบบไร้สายด้วย (Wireless Network) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่คอมพิวเตอร์ หรือผู้ที่ได้รับมอบหมายจากผู้ดูแลระบบ เท่านั้น

๓.๗.๔. ควบคุมการใช้งานเครือข่ายทั้งขาเข้าและขาออกโดย Firewall เพื่อ Monitor Threat ที่สุ่มเสี่ยงต่อความปลอดภัยของ Server และ ผู้ใช้ภายในคณะ

๔. การใช้งานอินเทอร์เน็ต

๔.๑. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้ตามสิทธิ์ที่ได้รับ

๔.๒. ห้ามใช้อินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

๔.๓. ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย เป็นต้น

๔.๔. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๔.๕. ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน และระบบของมหาวิทยาลัยมีการจัดสรร Bandwidth Management ให้จำกัด เพื่อไม่ให้กระทบกับการใช้งานของผู้อื่น

๔.๖. ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

๔.๗. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๔.๘. หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ที่ใช้งาน และออกจากการเครือข่ายอินเทอร์เน็ตด้วยการ Logout จากการ Authentication เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๔.๙. มีการเก็บ Traffic Log โดยมหาวิทยาลัย

๕. การบริหารจัดการคอมพิวเตอร์แม่ข่าย

๕.๑. กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง

๕.๒. มีขั้นตอน/กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย

๕.๓. ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐาน (time.psu.ac.th) ที่มหาวิทยาลัยใช้อ้างอิง

๕.๔. เปิดใช้บริการเท่าที่จำเป็นเท่านั้น โดยต้องมีมาตรการป้องกันเพิ่มเติมสำหรับบริการที่มีความเสี่ยงต่อระบบรักษาความปลอดภัยด้วย

๕.๕. ปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่ออุดช่องโหว่ต่าง ๆ

๕.๖. ทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๕.๗. มีการตรวจระดับทรัพยากรที่ใช้งานและทรัพยากรคงเหลืออย่างสม่ำเสมอ (Resource Usage)

๕.๘. มีการตรวจสอบดูแลด้าน Hardware อย่างสม่ำเสมอ

๖. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๖.๑. กำหนดผู้มีสิทธิ์ตามตำแหน่ง และกำหนดจำนวนผู้มีสิทธิ์ในการเข้าถึง

๖.๒. ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้งานระบบ

๖.๓. ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๖.๔. จำกัดการเข้าถึงตัวเครื่อง โดยให้สิทธิ์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น และห้องคอมพิวเตอร์แม่ข่ายจะต้องมีการป้องกันการเข้าถึงโดยง่าย

๗. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ

๗.๑. การจำกัดการเข้าถึงของผู้ใช้งานตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

๗.๒. การแบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศเป็น ๓ กลุ่ม คือ ผู้ดูแลระบบ ผู้พัฒนาระบบงาน และผู้ใช้งานระบบ โดยกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจน

๗.๓. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศโรงพยาบาล ต้องบันทึกข้อมูลพฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศดังนี้

๗.๓.๑. ชื่อบัญชีผู้ใช้

๗.๓.๒. วันเวลาที่เข้าถึงระบบ

๗.๓.๓. วันเวลาที่ออกจากระบบ

๗.๓.๔. เหตุการณ์สำคัญที่เกิดขึ้น เช่นการสั่งยา หัตถการ การออกใบเสร็จ การยกเลิกใบเสร็จ เป็นต้น

๗.๓.๕. แสดงการใช้สิทธิ์ เช่น สิทธิ์ของผู้ดูแลระบบ

๗.๓.๖. หมายเลขไอพีแอดเดรสที่เข้าถึง

๗.๔. การควบคุมผู้รับเหมาช่วง (outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และ พัฒนาระบบสารสนเทศ

๗.๔.๑. มีกระบวนการคัดเลือกผู้รับเหมาช่วงโดยเฉพาะ และต้องกำหนดคุณสมบัติของผู้รับเหมาช่วงที่ชัดเจน เช่น ต้องมีประสบการณ์ มีลูกค้าอ้างอิงน่าเชื่อถือ หรือมีใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยี ของการรับเหมาช่วงทั้งในส่วนของ ฮาร์ดแวร์และซอฟท์แวร์รวมถึงระบบสนับสนุน อื่น ๆ เพื่อให้ได้ผู้รับเหมาช่วงที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ

๗.๔.๒. มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาช่วง และต้องกำหนดขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และผู้รับเหมาช่วงต้องนำเสนอรายละเอียดงานขอบเขตงานอย่างครบถ้วน

๗.๔.๓. หน่วยงานต้องเข้าไปตรวจสอบรายละเอียดของการปฏิบัติงานของผู้รับเหมาช่วงได้ เช่น ร่วมกำหนดวิธีการทำงาน การตรวจติดตามคุณภาพของผู้รับเหมาช่วงเป็นระยะ ๆ ตามที่กำหนดไว้หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ

๗.๔.๔. มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาช่วงที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๘. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ

๘.๑. ผู้ดูแลระบบ แบ่งออกเป็น ๓ กลุ่ม

๘.๑.๑. ผู้ดูแลระบบเครือข่าย

๘.๑.๒. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย

๘.๑.๓. ผู้ดูแลระบบสารสนเทศและผู้ดูแลเว็บไซต์

(๑) ระบบสารสนเทศงานเพื่อบริหารจัดการ

(๒) ระบบสารสนเทศงานโรงพยาบาล

(๓) ระบบสารสนเทศงานการเรียนการสอน

(๔) ระบบสารสนเทศข้อมูลวิจัยคณะทันตแพทยศาสตร์ และระบบสารสนเทศยื่นจริยธรรมวิจัยในมนุษย์

(๕) เว็บไซต์คณะฯ และหน่วยงานภายใน

๘.๒. ดูแลระบบเครือข่าย มีหน้าที่และความรับผิดชอบดังนี้

๘.๒.๑. ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอและปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๘.๓. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่และความรับผิดชอบดังนี้

๘.๓.๑. ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข

๘.๓.๒. ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่ายให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๘.๓.๓. ติดตั้งโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดีต่าง ๆ ให้เหมาะสม

๘.๓.๔. ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

๘.๓.๕. กรณีให้บริการ Service http และ กำหนด Policy การเข้าถึงแบบ Worldwide จะต้องแก้ไขและส่ง Audit Security ตามมาตรฐานของ DiiS

๘.๔. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเว็บไซต์มีหน้าที่และความรับผิดชอบในแต่ละระบบดังนี้

๘.๔.๑. ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๘.๔.๒. ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้นให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

๘.๔.๓. การดึงรายงานเพื่อพัฒนางานหรือเพื่อประกอบการตัดสินใจการบริหารองค์กร สามารถดึงผ่านระบบสารสนเทศ โดยหน่วยงานที่รับผิดชอบข้อมูล หากรายงานที่ต้องการไม่อยู่ในรายการที่ระบุไว้ ให้เขียนคำร้องมายังงานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ โดยผ่านความคิดเห็นของผู้บังคับบัญชาต้นสังกัด แสดงในภาคผนวก ข

๘.๔.๔. ผู้ดูแลเว็บไซต์ดูแลเนื้อหา ปรับปรุงเนื้อหาให้ถูกต้องและปัจจุบันเสมอ

๘.๕. หลักธรรมาภิบาลของผู้ดูแลระบบ

๘.๕.๑. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานโดยไม่มีเหตุผลอันสมควร

๘.๕.๒. ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๘.๕.๓. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๙. การตรวจสอบความถูกต้องของข้อมูล

มีแนวทางในการตรวจสอบความถูกต้องของระบบสารสนเทศ ดังนี้

๙.๑. ระบบสารสนเทศสนับสนุนงานสำนักงานเลขานุการ

๙.๑.๑ ข้อมูลพื้นฐานของบุคลากร และนักศึกษา มีการเชื่อมโยงกับระบบฐานข้อมูลสารสนเทศด้านบุคลากรและระบบฐานข้อมูลนักศึกษาซึ่งมีความถูกต้องตามมหาวิทยาลัย

๙.๑.๒ มอบหมายให้หน่วยงานที่รับผิดชอบข้อมูลสารสนเทศ เป็นผู้ดูแลข้อมูลในการบันทึกแก้ไขข้อมูลให้มีความถูกต้อง ครบถ้วน ทันสมัย และแม่นยำ หากพบว่าข้อมูลคลาดเคลื่อน ไม่ถูกต้อง และไม่ทันสมัย สามารถแจ้งเจ้าหน้าที่ที่เป็นเจ้าของข้อมูลเพื่อปรับปรุงแก้ไข

๙.๒. ระบบสารสนเทศงานโรงพยาบาล

๙.๒.๑ กำหนดข้อมูลพื้นฐาน เป็นตัวเลือกให้แก่ผู้ใช้ เพื่อลดข้อผิดพลาดจากการกรอกข้อมูลของผู้ใช้งาน

๙.๒.๒ ใช้เมนูสำหรับผู้ดูแลระบบ เพื่อกำหนดให้ระบบตรวจสอบและแสดงข้อความแจ้งเตือนก่อนผู้ใช้จะทำการบันทึกข้อมูลเข้าสู่ระบบ ในกรณีที่ผู้ใช้กรอกข้อมูลไม่ครบถ้วน หรือกรอกข้อมูลที่ผิดปกติ

๙.๒.๓ ผู้ดูแลระบบจัดทำรายงานทางสถิติ เพื่อให้ตัวแทนเจ้าหน้าที่ประจำหน่วยงาน ตรวจสอบความถูกต้องของข้อมูล โดยแบ่งเป็น รายงานรายคาบ รายวัน รายเดือน รายไตรมาส รายปี และรายปีงบประมาณ

๙.๓. สารสนเทศงานการเรียนการสอน

๙.๓.๑. มีระบบสารสนเทศตรวจสอบคะแนนสำหรับนักศึกษาทันตแพทย์ เพื่อตรวจสอบความถูกต้องของคะแนนกับอาจารย์แต่ละสาขา

๙.๓.๒. มีรายงานจากระบบคลินิกนักศึกษาเพื่อให้นักศึกษาทันตแพทย์ และอาจารย์ประจำสาขาวิชา ตรวจสอบความถูกต้องของข้อมูลร่วมกันก่อนออกเกรด และมีการเปรียบเทียบกับสมุดบันทึกการรักษาของนักศึกษาทันตแพทย์

๙.๓.๓. มีระบบสารสนเทศเพื่อให้นักศึกษาทันตแพทย์ ยื่นคำร้องขอแก้ไขคะแนนเพื่อให้ได้ข้อมูลที่ถูกต้อง

๙.๔. ระบบสารสนเทศข้อมูลวิจัยคณะทันตแพทยศาสตร์

๙.๔.๑. ข้อมูลวิจัยคณะ ฯ มีการเชื่อมโยงกับฐานข้อมูลวิจัยมหาวิทยาลัย (HRMIS)

๙.๔.๒. มอบหมายให้หน่วยส่งเสริมและพัฒนางานวิจัย ในการตรวจสอบความถูกต้องของข้อมูล หากพบว่าข้อมูลไม่ถูกต้องจะมีการแจ้งให้นักวิจัยที่เป็นเจ้าของข้อมูลเพื่อปรับปรุงแก้ไข

๙.๕. ระบบสารสนเทศยื่นจริยธรรมวิจัยในมนุษย์

๙.๕.๑. ข้อมูลโครงการวิจัยมีการเชื่อมโยงกับระบบบริหารงานวิจัยของมหาวิทยาลัยซึ่งมีความถูกต้องของข้อมูลตามมหาวิทยาลัย

๙.๕.๒. มอบหมายให้หน่วยงานสำนักจริยธรรมวิจัยในมนุษย์ เป็นผู้ดูแลข้อมูลในการตรวจสอบข้อมูล และปรับแก้สถานะของการยื่นเอกสารในการยื่นขอวิจัยในมนุษย์ให้เป็นปัจจุบัน หากพบว่าข้อมูลคลาดเคลื่อน ไม่ถูกต้อง สามารถแจ้งเจ้าหน้าที่ที่เป็นเจ้าของข้อมูลปรับปรุงแก้ไขข้อมูล

ส่วนที่ ๒

แนวปฏิบัติการบำรุงการรักษาคอมพิวเตอร์อุปกรณ์และการจัดการข้อมูลในเครื่องคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อควบคุมดูแล และบำรุงรักษาให้ทรัพยากรสารสนเทศของคณะทันตแพทยศาสตร์มีสภาพพร้อมใช้งานอยู่เสมอรวมถึงการแก้ไข ปรับปรุง เพื่อให้การใช้งานทรัพยากรสารสนเทศเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๒. ลดการติดขัดในการทำงาน สามารถทำงานได้อย่างต่อเนื่อง

๓. เพื่อบันทึก รวบรวมข้อมูลเกี่ยวกับอุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง

๔. เพื่อเป็นการป้องกันภัยคุกคามทางคอมพิวเตอร์และทางอินเทอร์เน็ต

๕. เพื่อให้การจัดการข้อมูลในคอมพิวเตอร์เป็นไปด้วยความเรียบร้อย

๖. ควบคุมข้อมูลคอมพิวเตอร์ไม่ให้รั่วไหลหรือนำไปใช้ต่อในทางไม่พึงประสงค์

๗. ลดปัญหาเรื่องข้อมูลสูญหาย

๘. ลดการติดขัดในการทำงาน หน่วยงานสามารถทำงานได้อย่างต่อเนื่อง

ผู้รับผิดชอบ

๑. งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ

๒. ผู้ดูแลทรัพยากรสารสนเทศ

๓. หน่วยงานที่ใช้ทรัพยากรสารสนเทศ

๔. เจ้าหน้าที่ของหน่วยงานที่ใช้งานทรัพยากรสารสนเทศ

อ้างอิงมาตรฐาน

๑. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

แนวปฏิบัติ

1. การบำรุงรักษาคอมพิวเตอร์อุปกรณ์

1.1 ถ่ายทอดความรู้และแนะนำการใช้งาน

1.1.1 สมรรถนะพื้นฐานทางด้านคอมพิวเตอร์ให้เหมาะสมกับลักษณะการปฏิบัติงานแสดงในภาคผนวก ค

1.1.2 การแก้ไขปัญหาเบื้องต้นในใช้งานทรัพยากรสารสนเทศของแต่ละหน่วยงาน

1.1.3 การใช้งานคอมพิวเตอร์และอุปกรณ์ Mobile

1.1.4 การติดตั้ง Software และการใช้งานระบบ

1.1.5 การเชื่อมต่อใช้งานอินเทอร์เน็ต

1.2 กระบวนการตรวจซ่อมคอมพิวเตอร์

1.2.1 ผู้ใช้แจ้งปัญหาผ่านระบบแจ้งซ่อมออนไลน์ หรือเจ้าหน้าที่ผู้ดำเนินการตรวจซ่อมโดยตรง

1.2.2 เจ้าหน้าที่ผู้ดำเนินการตรวจซ่อมรับทราบข้อมูลบันทึกในระบบและดำเนินการวิเคราะห์เบื้องต้น

1.2.3 หากปัญหาสามารถแก้ไขได้ เจ้าหน้าที่ผู้ดำเนินการตรวจซ่อมจะดำเนินการซ่อมแซมทันที

1.2.4 หากปัญหาเกิดจากระบบปฏิบัติการ Windows เสียหาย หรือปัญหาที่ต้องใช้เวลาในการตรวจซ่อมนาน ให้หน่วยงานยกอุปกรณ์มาที่งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ เพื่อดำเนินการซ่อมแซม

1.2.5 อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงที่อยู่ในระยะเวลารับประกัน หากเกิดปัญหา เสียหายหรือชำรุด เจ้าหน้าที่ฝ่ายซ่อมบำรุงคอมพิวเตอร์จะทำการตรวจเช็คพร้อมทั้งดำเนินการส่งเคลมและติดตามงานกับทางบริษัท และหากต้องใช้ อุปกรณ์สคอมพิวเตอร์สำรองให้ทางหน่วยงานมายืมเพื่อนำไปใช้งานชั่วคราวในขณะที่ดำเนินการส่งเคลม และเมื่ออุปกรณ์ซ่อมเสร็จ ทางหน่วยงานนำอุปกรณ์คอมพิวเตอร์ที่ยืมมาคืน

1.2.6 อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงที่หมดประกันหากเกิดปัญหา เสียหายหรือชำรุด ทางเจ้าหน้าที่ผู้ดูแลทรัพยากรสารสนเทศจะทำการตรวจเช็คแก้ไขปัญหาก่อนรายงานผล เพื่อให้ทางหน่วยงานส่งซ่อมกับทางพัสดุ และมีอุปกรณ์คอมพิวเตอร์สำรองให้ทางหน่วยงานมายืมเพื่อนำไปใช้งานชั่วคราวในขณะที่ดำเนินการส่งซ่อม และเมื่ออุปกรณ์ซ่อมเสร็จ ทางหน่วยงานนำอุปกรณ์คอมพิวเตอร์ที่ยืมมาคืน

1.2.7 ในการตรวจซ่อมคอมพิวเตอร์ในทุกกรณี ทางเจ้าหน้าที่ผู้ดำเนินการตรวจซ่อมจะไม่เข้าถึง แก้ไขเปลี่ยนแปลง หรือคัดลอกข้อมูลส่วนบุคคลของผู้ใช้งาน และไม่เข้าถึงระบบต่างๆ ที่ผู้ใช้งานมีสิทธิ์ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน เว้นแต่ผู้ใช้งานมีความประสงค์และยินยอม ในกรณีที่ต้องย้ายข้อมูลในกรณีที่อุปกรณ์จัดเก็บข้อมูลเกิดการชำรุดเสียหาย โดยทางเจ้าหน้าที่ผู้ตรวจซ่อมจะปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ อย่างเคร่งครัด

1.2.8 ทางเจ้าหน้าที่ผู้ดำเนินการตรวจซ่อม ทำการบันทึกประวัติการซ่อมบำรุงเพื่อใช้เป็นข้อมูลในการวิเคราะห์และปรับปรุงกระบวนการในอนาคต

1.3 การบำรุงรักษา

1.3.1 ตรวจเช็คอุปกรณ์คอมพิวเตอร์ และเครื่องสำรองไฟ (UPS) ที่ให้บริการส่วนกลางและเครื่องบริการนักศึกษา ให้มีสภาพใช้งานได้ทุกๆปี

1.3.2 อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ และแอนตี้ไวรัสให้เป็นเวอร์ชันล่าสุด เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางอินเทอร์เน็ต

1.3.3 เปลี่ยนอุปกรณ์ฮาร์ดแวร์ที่มีสัญญาณชำรุดหรือเสื่อมสภาพ

1.3.4 กรณีเครื่องคอมพิวเตอร์ที่หมดความจำเป็นใช้งาน มีเครื่องคอมพิวเตอร์ใหม่ทดแทนให้แล้ว หรืออุปกรณ์ที่เสื่อมสภาพ ไม่อนุญาตให้นำมาใช้งาน เนื่องจากจะมีผลต่อความปลอดภัยในการใช้งานระบบและ เป็นช่องโหว่ทำให้ถูกโจมตีจากภายนอกได้

1.4 การเปลี่ยนอุปกรณ์

1.4.1 เปลี่ยนอุปกรณ์คอมพิวเตอร์ที่มีอายุการใช้งานเกิน 5 ปี หรือที่มีต้นทุนการซ่อมสูงกว่าการเปลี่ยนใหม่

2. การจัดการข้อมูลในเครื่องคอมพิวเตอร์

2.1 กรณีอุปกรณ์ Harddisk เสียหาย

2.1.1 บุคลากรเจ้าของข้อมูลต้องทำการ Backup ข้อมูลไว้อุปกรณ์เก็บข้อมูลอื่น เช่น Handy Drive , External Harddisk หรือ บน Cloud Google Drive อยู่สม่ำเสมอเพื่อป้องกัน ข้อมูลเสียหายหรือสูญหาย

2.1.2 หากเป็น Harddisk ที่อยู่ในประกัน ทางเจ้าหน้าที่สารสนเทศ จะทำการส่งเคลม เพื่อนำ Harddisk ตัวใหม่มาเปลี่ยน หาก Harddisk หมดประกัน จะดำเนินการจัดหา Hard disk ใหม่ทดแทน

2.2 กรณีบุคลากรพ้นสภาพจากการเป็นพนักงาน (ลาออก เกษียณ ให้ออก) หรือ ลาศึกษาต่อ ย้ายสังกัดการปฏิบัติงานข้ามหน่วยงาน หรือหมดความจำเป็นใช้งาน

2.2.1 บุคลากรเจ้าของข้อมูลต้องดำเนินการจัดการข้อมูลส่วนตัวที่อยู่ในเครื่องคอมพิวเตอร์และลบข้อมูลส่วนตัวออก

2.2.2 บุคลากรเจ้าของข้อมูลต้องส่งมอบข้อมูลเกี่ยวกับงานในองค์กรให้กับหน่วยงานที่สังกัดเพื่อนำไปใช้ต่อ

2.2.3 เมื่อจัดการข้อมูลในเครื่องคอมพิวเตอร์ดังกล่าวเสร็จสิ้นแล้ว หน่วยงานเจ้าของเครื่องแจ้งเรื่องไปทางงานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศและต้องทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือและอุปกรณ์คอมพิวเตอร์อื่นๆคืนกับยังงานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศภายในระยะเวลาไม่เกิน 1 เดือน นับจากคำสั่งมีผลบังคับใช้ หรือ 1 เดือน หลังจากที่บุคลากรเจ้าของเครื่องสิ้นสุดเวลาการปฏิบัติงาน

2.2.4 ทางเจ้าหน้าที่งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ จะดำเนินการลบข้อมูลทั้งหมดที่อยู่ในเครื่องคอมพิวเตอร์ และติดตั้ง Software ใหม่ให้เพื่อดำเนินการจัดสรรให้ทางหน่วยงานนอื่นนำเครื่องคอมพิวเตอร์ไปใช้งานต่อ

2.3 กรณีบุคลากรเสียชีวิต

2.3.1 หน่วยงานที่บุคลากรสังกัดนำข้อมูลออกจากเครื่องคอมพิวเตอร์เพื่อนำไปใช้ต่อในองค์กร หากติดปัญหาให้แจ้งมายังเจ้าหน้าที่นวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ

2.3.2 หน่วยงานแจ้งเรื่องไปทางงานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ ทางเจ้าหน้าที่นวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ จะมาดำเนินการลบข้อมูลทั้งหมดที่อยู่ในเครื่องคอมพิวเตอร์ และติดตั้ง Software ใหม่ให้เพื่อหน่วยงานนำเครื่องคอมพิวเตอร์ไปใช้งานต่อ

2.3.3 เมื่อจัดการข้อมูลในเครื่องคอมพิวเตอร์ดังกล่าวเสร็จสิ้นแล้ว หน่วยงานเจ้าของเครื่องต้องทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์ หรือครุภัณฑ์ต่อพ่วงอื่น ๆ คืนกับยังงานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศภายในระยะเวลาไม่เกิน 1 เดือน นับจากคำสั่งมีผลบังคับใช้ หรือ 1 เดือน หลังจากที่บุคลากรเจ้าของเครื่องสิ้นสุดเวลาการปฏิบัติงาน

ส่วนที่ ๓
แนวปฏิบัติการปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อให้การปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์เป็นไปด้วยความเรียบร้อย
๒. เพื่อให้มีความเข้าใจตรงกันในกระบวนการการปรับปรุงสิ่งก่อสร้าง
๓. เพื่อลดความเสียหายจากการปรับปรุงสิ่งก่อสร้าง

ผู้รับผิดชอบ

๑. งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. มาตรฐานระบบเครือข่าย ที่กำหนดโดย IEEE

แนวปฏิบัติ

๑. กรอกฟอร์มขอใช้บริการจากระบบ E-request
๒. นัดหารือพูดคุยเกี่ยวกับการปรับปรุงสิ่งก่อสร้างที่เกี่ยวข้องระบบเครือข่าย เช่น สาย LAN, อุปกรณ์กระจายสัญญาณไร้สาย, เครื่องคอมพิวเตอร์ และเครื่องพิมพ์
๓. เจ้าหน้าที่นวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศเข้าไปสำรวจจุดเครือข่าย (Outlet) เดิม และอุปกรณ์ระบบเครือข่าย
๔. จุดเครือข่ายเดิม (Outlet) ให้ย้ายเก็บไว้ สำหรับนำมาใช้ได้อีก เพื่อประหยัดงบประมาณในการติดตั้งใหม่
๕. แนวทางการติดตั้งและการเพิ่มเติมอุปกรณ์เครือข่ายต้องเป็นไปตาม TOR ที่เจ้าหน้าที่นวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ กำหนด

ส่วนที่ ๔
แนวปฏิบัติการจัดทำระบบสำรองสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของคณะมีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง

๒. เพื่อกำหนดแนวปฏิบัติการทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบสารสนเทศระบบงานสำนักงานเลขานุการระบบงานโรงพยาบาล และระบบสารสนเทศงานการเรียนการสอนถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีข้อมูลที่สำรองและสามารถกู้คืนข้อมูลได้ในเวลาที่กำหนด

ผู้รับผิดชอบ

๑. งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕

๒. สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

๑. ระบบสำรอง

๑.๑. จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศสำคัญและจำเป็นต้องมีระบบสำรอง แสดงดังภาคผนวก ง

๑.๒. ข้อมูลสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม

๑.๓. มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๒. การสำรองข้อมูล

๒.๑. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของระบบสารสนเทศ

๒.๒. กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ โดยวิธีการเขียนสคริปต์การสำรองข้อมูลอัตโนมัติ ควบคู่ไปกับการสำรองข้อมูลโดยเจ้าหน้าที่ในบางระบบ

๒.๓. กำหนดความถี่การสำรองข้อมูล โดยมีการสำรองฐานข้อมูลระบบสารสนเทศตามประเภทการไหลเวียนของข้อมูลในระบบ โดยแบ่งเป็น ทุกวัน วันละ ๑ ครั้ง สัปดาห์ละ ๑ ครั้ง หรือเดือนละครั้ง

๒.๔. จัดเก็บข้อมูลสำรองไว้ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก โดยมีการจัดเก็บข้อมูลไว้ที่ห้องระบบเครือข่าย (Network D) อาคาร 1 ชั้น 3 ซึ่งอยู่คนละพื้นที่กับระบบหลัก กรณีเกิดเหตุไม่คาดฝัน เช่น ไฟไหม้ ตึกถล่ม สามารถนำข้อมูลที่เก็บไว้อีกที่มาใช้ได้ โดยได้สำรองไว้ย้อนหลัง ๑ – ๓ เดือน โดยเก็บแยกออกจากเครื่องคอมพิวเตอร์แม่ข่ายระบบใช้งานจริง

๒.๕. ในส่วนของเครื่องแม่ข่ายได้ออกแบบไว้ 2 ชุด กรณีฉุกเฉินอุปกรณ์เครื่องแม่ข่ายมีปัญหาเครื่องแม่ข่ายอีกเครื่องสามารถทำงานแทนกันได้ทันที(Redundant) และส่วนของการเก็บข้อมูลมีการทำ Raid 6 คือ Hard disk เสียพร้อมกันได้ 2 ลูก เพื่อลดการสูญเสียของข้อมูล

๒.๖. สำหรับระบบ HRM และ HIS จะมีการใช้ Veeam Backup ในการช่วยสำรองข้อมูลเก็บไว้ในอุปกรณ์ NAS โดย จะมีความจุอยู่ที่ 40TB แบ่ง เป็น project ละ 50% ของพื้นที่ความจุ จะสามารถสำรองได้ 9 วัน สำหรับ HRM (Full Backup x 1 และ Incremental Backup x 2) และ 4 วันสำหรับ HIS (Full Backup ทุกวัน)

๓. การกู้คืนข้อมูล

๓.๑. จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

๓.๒. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ

๓.๓. ให้ใช้ข้อมูลทันสมัยที่สุด

๓.๔. ทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง

๔. การทดสอบสภาพพร้อมใช้งาน

๔.๑. ต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๕
แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายได้รับทราบถึงหน้าที่ ความรับผิดชอบ และความจำเป็นในการประเมินความเสี่ยงสารสนเทศ เพื่อหาแนวทางป้องกันภัยคุกคามและการโจมตีต่าง ๆ

ผู้รับผิดชอบ

๑. งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕
๒. สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

๑. ต้องมีการตรวจสอบและป้องกันความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ
๒. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อประเมินความเสี่ยงนั้น
   ๒.๑. ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต
      ๒.๑.๑. มีการอัพเดทแพทช์ระบบปฏิบัติการของเครื่องแม่ข่าย
      ๒.๑.๒. มีการเปลี่ยนพาสเวิร์ดของเครื่องแม่ข่ายอย่างน้อยปีละ ๒ ครั้ง
      ๒.๑.๓. มีการติดตาม (monitor) log file ของเครื่องแม่ข่าย อย่างน้อยสัปดาห์ละ ๑ ครั้ง
   ๒.๒. ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สาย
      ๒.๒.๑. มีการใช้งาน PSU Passport เพื่อป้องกันบุคคลภายนอก
      ๒.๒.๒. มีการตั้งค่าอุปกรณ์เครือข่ายที่ปลอดภัยตามมาตรฐานความปลอดภัยของเครือข่าย WPA2
   ๒.๓. ความเสี่ยงที่เกิดจากการลงบันทึกเข้าสารสนเทศที่สำคัญผ่านระบบเครือข่าย
      ๒.๓.๑. ตั้งค่าไม่ให้บันทึกรหัสผ่านบนเบราว์เซอร์เพื่อป้องกันไม่ให้บุคคลอื่นเข้าถึงสิทธิ์การใช้งานของผู้ใช้เฉพาะคอมพิวเตอร์บริการส่วนกลาง (เครื่องคอมพิวเตอร์ประจำยูนิตรักษาห้องปฏิบัติการคอมพิวเตอร์ และหน่วยส่งเสริมและพัฒนาการศึกษาด้วยตนเอง)
๓. ทำรายงานการวิเคราะห์และการประเมินความเสี่ยงประจำปีตามภาคผนวก ซ

ส่วนที่ ๖
แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อเผยแพร่แนวปฏิบัติให้กับผู้บริหาร บุคลากรและผู้เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

๑. งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕
๒. สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

๑. อบรมผู้ใช้งานและเจ้าหน้าที่ผู้เกี่ยวข้อง ให้มีความรู้ความเข้าใจ เกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการใชงานสารสนเทศโดยไม่ระมัดระวัง
๒. อบรมการใช้งานสารสนเทศให้กับหน่วยงาน
๓. จัดทำคู่มือการใช้งานระบบสารสนเทศ
๔. ประชาสัมพันธ์แจ้งข่าวสาร

ส่วนที่ ๗
แนวปฏิบัติการแก้ไขปัญหาระบบสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของคณะทันตแพทยศาสตร์
๒. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของระบบสารสนเทศของคณะทันตแพทยศาสตร์
๓. เพื่อให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และสามารถตอบสนองสถานการณ์ได้อย่างทันท่วงที

ผู้รับผิดชอบ

๑. งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ
๒. ผู้ดูแลระบบสารสนเทศ เจ้าหน้าที่ระบบเครือข่ายที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕
๒. สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

๑. ติดต่อประสานงาน โทร. ๗๕๔๐
๒. ระบบเครือข่ายและเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงขัดข้อง ติดต่อหน่วยโครงสร้างพื้นฐานและบริการด้านดิจิทัล โทร. ๗๗๕๘
๓. ระบบสารสนเทศขัดข้องติดต่อหน่วยพัฒนาพัฒนานวัตกรรมดิจิทัลและจัดการข้อมูลสารสนเทศ

ระบบงานสารสนเทศ	ติดต่อ
สนับสนุนทรัพยากรองค์กร (HRM&ERP) / เว็บไซต์คณะฯและหน่วยงาน	๗๖๘๔
ระบบสารสนเทศโรงพยาบาล (HIS)	๗๕๔๑
ระบบสารสนับสนุนการเรียนการสอน/วิจัย (EDU&RDU)	๗๕๐๕

การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน จัดเตรียมทีมงาน และมอบหน้าที่ความรับผิดชอบ ตามทีมงานแผนดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan Team)

แผนกู้คืน Disaster Recovery Plan (DRP)

1. คู่มือการกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery)

2. คู่มือกู้คืนเครื่องสำรองไฟสำหรับ Data Center ขัดข้อง
3. แนวปฏิบัติระบบสารสนเทศโรงพยาบาลใช้งานไม่ได้
    - คู่มือการกู้คืนระบบสารสนเทศโรงพยาบาล (HOSxPXE)
    - คู่มือการกู้คืนระบบสารสนเทศ HIS ใหม่
4. คู่มือกู้คืนระบบสารสนเทศสำคัญอื่นๆ
    - คู่มือการกู้คืนเว็บไซต์
    - คู่มือการกู้คืน Dent Web Application
    - คู่มือการกู้คืนระบบสารสนเทศการศึกษา
5. คู่มือกู้คืนข้อมูลจากระบบสำรองข้อมูล

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์ฉุกเฉิน ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเป็นประจำทุกเดือน และรายงานการเกิดปัญหาและผลการแก้ไขให้ทราบทันที พร้อมทั้งปรับปรุงแนวปฏิบัติการจัดการด้านความ ปลอดภัย ความเสี่ยงของระบบฐานข้อมูลและเครือข่ายเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ เพื่อให้สามารถนำไปมาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติต่อไป

ส่วนที่ ๘

แนวการจัดการผู้ใช้ควบคุมการเข้าถึงระบบกล้องวงจรปิด

วัตถุประสงค์

1. ควบคุมการเข้าถึงระบบกล้องวงจรปิดขององค์กร
2. รักษาความปลอดภัยของข้อมูล
3. ป้องกันการใช้งานที่ไม่เหมาะสม

ผู้รับผิดชอบ

1. งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ
2. งานอาคาร วิศวกรรมและซ่อมบำรุง
3. เจ้าหน้าที่สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ

อ้างอิงมาตรฐาน

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
3. พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

การกำหนดสิทธิ์การเข้าถึง

การเข้าถึงระบบกล้องวงจรปิดได้กำหนดตามบทบาทและความรับผิดชอบของผู้ใช้
โดยแบ่งผู้ใช้งานและกำหนดสิทธิ์ดังนี้

	User	Account	privilege	Camera	View	Revert Event	Manage	Export
1	เจ้าหน้าที่ DIIS		guest	all			/	
2	เจ้าหน้าที่ บ.ACG		guest	all			/	
3	รปภ. คณะ		user	all	/	/		/
4	IT Support คณะ		admin	all	/	/	/	/
5	ผู้บริหารคณะ		user	all	/	/		
6	เจ้าหน้าที่ห้องสมุดคณะ		user	กล้องอาคาร 3 ชั้น5	/	/		

โดยสิทธิ์ที่เป็น Admin สามารถเข้าไปจัดการแก้ไข ตั้งค่าในโปรแกรมระบบกล้อง

สิทธิ์ที่เป็น User สามารถเข้าดูและย้อนกล้องได้ ไม่สามารถเข้าไปจัดการแก้ไขในระบบได้
สิทธิ์ที่เป็น Guest กำหนดให้สามารถเข้ามาจัดการในระบบในช่วงเวลาที่ได้รับอนุญาต

แนวปฏิบัติ

1. กำหนดสิทธิ์ Admin สำหรับเจ้าหน้าที่ฝ่ายซ่อมบำรุงคอมพิวเตอร์คณะ
   สำหรับเข้าไปจัดการตั้งค่าแก้ไขในโปรแกรมระบบกล้อง
2. กำหนดสิทธิ์ User สำหรับผู้บริหารคณะ เจ้าหน้าที่ห้องสมุด สามารถดูกล้องและย้อนเหตุการณ์ดูได้
   ส่วนผู้ใช้ระบบที่เป็น รปภ.และเจ้าหน้าที่ฝ่ายซ่อมบำรุงคอมพิวเตอร์คณะ สามารถ Export file image และ VDO เหตุการณ์ได้
3. กำหนดสิทธิ์ Guest สำหรับเจ้าหน้าที่สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะและเจ้าหน้าที่บริษัทภายนอก
   เพื่อสามารถเข้ามาตั้งค่าแก้ไข ตรวจเช็คความผิดปกติในระบบกล้องคณะในช่วงเวลาที่ได้รับอนุญาต

ภาคผนวก

ภาคผนวก ก

ตารางรายละเอียดช่องทางการติดต่อหน่วยงานผู้ดูแลข้อมูลแต่ละประเภท

ตารางที่ ๑ รายละเอียดช่องทางการติดต่อหน่วยงานผู้ดูแลข้อมูลแต่ละประเภท

ประเภทข้อมูล	หน่วยงาน	เบอร์โทรติดต่อ	อีเมล์
๑. ข้อมูลนักศึกษา	หน่วยทะเบียนและประเมินผลการศึกษา หน่วยกิจการนักศึกษา หน่วยบัณฑิตศึกษา - ระดับหลังปริญญา	๐๗๔-๒๘๗๕๒๙ ๐๗๔-๒๘๗๕๓๒ ๐๗๔-๒๘๗๕๒๙	dentpsu_registrar@hotmail.com dentpsu.studentaffairs@gmail.com dentpsu.grad@group.psu.ac.th
๒. ข้อมูลบุคลากร	หน่วยบริหารทรัพยากรบุคคล	๐๗๔-๒๘๗๕๑๘	saowanee.sa@psu.ca.th
๓. ข้อมูลการเงินและบัญชี	งานคลังและพัสดุ – บริหารจัดการข้อมูลการเงินและบัญชี การจัดการงบประมาณทั้งหมดภายในคณะฯ	๐๗๔-๒๘๗๕๒๔	supot.t@psu.ac.th
	หน่วยเงินรายได้ – บริหารจัดการข้อมูลการเงินและบัญชีด้านโรงพยาบาลทันตกรรม	๐๗๔-๒๘๗๖๓๕	chatmanee.s@psu.ac.th
๔. ข้อมูลการศึกษา	หน่วยทะเบียนและประเมินผลการศึกษา – ระดับปริญญาตรี	๐๗๔-๒๘๗๕๒๙	dentpsu_registrar@hotmail.com
	หน่วยบัณฑิตศึกษา - ระดับหลังปริญญา	๐๗๔-๒๘๗๕๓๑	dentpsu.grad@group.psu.ac.th
๕. ข้อมูลทางการบริหาร	หน่วยนโยบายและแผน ดูแลข้อมูลการบริหารจัดการ นโยบาย งบประมาณ และอัตรากำลัง	๐๗๔-๒๘๗๕๒๓	kanokwan.s@psu.ac.th
	หน่วยส่งเสริมและพัฒนางานวิจัย ดูแลฐานข้อมูลวิจัย	๐๗๔-๒๘๗๕๐๔	kemarajt.k@psu.ac.th
	สำนักงานจริยธรรมดูแลโครงการวิจัยที่ดำเนินการเกี่ยวข้องกับมนุษย์	๐๗๔-๒๘๗๕๓๓	tasawan.r@psu.ac.th
	หน่วยพัสดุ ดูแลในส่วนการจัดซื้อจัดจ้าง บริหารงานพัสดุ	๐๗๔-๒๘๗๕๒๖	kruawon.p@psu.ac.th pagrapruk.s@psu.ac.th
๖. ข้อมูลผู้ป่วย	โรงพยาบาลทันตกรรม	๐๗๔-๒๘๗๖๒๐	vorawan.s@psu.ac.th

ภาคผนวก ข

แบบฟอร์มขอใช้งาน E-Request

แบบฟอร์มขอพัฒนาระบบสารสนเทศ โทร. 7540
งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ คณะทันตแพทยศาสตร์ ม.อ.

ชื่อผู้ขอใช้บริการ..... **ภาควิชาหน่วยงาน/**.....

วันที่ขอ..... **โทรศัพท์**..... **อีเมล์**.....

มีความประสงค์ ☐ ต่อยอด ☐ ปรับปรุง แก้ไข/ ☐ พัฒนาระบบใหม่

ระบบที่ต้องการ.....

วัตถุประสงค์ ความต้องการระบบ/.....

.....

ผู้เกี่ยวข้องกับระบบ หน่วยงาน /.....

เอกสารสนับสนุนการพัฒนาระบบ

☐ เอกสารแสดงขั้นตอนการทำงาน และความเชื่อมโยงถึงส่วนต่าง ๆ ของระบบ

☐ แบบฟอร์มที่ต้องการ เช่นแบบฟอร์มการกรอกข้อมูล

☐ ฉบับร่างแบบรายงานที่ต้องการ

☐ ตัวแปรหรือข้อมูลที่ต้องการให้เก็บในฐานข้อมูล

☐ หากมีรูปภาพ ให้แนบ File .jpg / .gif

ระบุผู้ใช้งานระบบ ☐ **:** อาจารย์ ☐ บุคลากร ☐ นักศึกษา ☐ อื่นๆ

.....

กรณีต้องการประชุมกับเจ้าหน้าที่สารสนเทศ : วันที่ ...เวลา ...../...../.....ห้อง.....

สำหรับผู้ขอใช้บริการ	**เห็นควรอนุมัติ/คำสั่ง**	**สำหรับเจ้าหน้าที่ผู้ได้รับมอบหมาย**
ลงชื่อ.....ผู้ขอใช้บริการ (.....) ...../...../.....	☐ เห็นชอบ โดยมอบหมาย..... ☐ ไม่เห็นชอบ..... ลงชื่อ..... (นางสาวสุทิศา จรียานุวัฒน์) หัวหน้างานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ ...../...../.....	☐ รับทราบ..... ....
ลงชื่อ..... ผู้บังคับบัญชา (.....) ...../...../.....	☐ อนุมัติ ☐ ไม่อนุมัติ ..... ลงชื่อ..... (ผศ.ดร.ทพญ. สุภาวดี เนาว์รุ่งโรจน์) ผู้ช่วยคณบดีฝ่ายสารสนเทศ ...../...../.....	ลงชื่อ..... ( ) ...../...../.....

แบบฟอร์ม แจ้งปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ โทร. 7758
งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ คณะทันตแพทยศาสตร์ ม.อ.

ชื่อผู้ขอใช้บริการ..... **ภาควิชาหน่วยงาน/**.....

วันที่ขอ..... **โทรศัพท์**..... **อีเมล์**.....

มีความประสงค์ ☐ ปรับปรุงพื้นที่ ☐ ขอยืมอุปกรณ์เครือข่าย .....

พื้นที่ปรับปรุง.....

วัตถุประสงค์ ความต้องการ/.....

.....

.....

ผู้เกี่ยวข้องกับพื้นที่ปรับปรุง หน่วยงาน /.....

เอกสารสนับสนุนการปรับปรุงพื้นที่

☐ ผังปรับปรุงพื้นที่เดิม

☐ ผังปรับปรุงพื้นที่ใหม่

☐ แบบฟอร์ม แจ้งปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์

กรณีต้องการประชุมกับเจ้าหน้าที่สารสนเทศ : วันที่ ...เวลา ...../...../.....ห้อง.....

สำหรับผู้ขอใช้บริการ	**เห็นควรอนุมัติ/คำสั่ง**	**สำหรับเจ้าหน้าที่ผู้ได้รับมอบหมาย**
ลงชื่อ.....ผู้ขอใช้บริการ (.....) ...../...../.....	☐ เห็นชอบ โดยมอบหมาย..... ☐ ไม่เห็นชอบ..... ลงชื่อ..... (นางสาวสุทิศา จรียานุวัฒน์) หัวหน้างานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ ...../...../.....	☐ รับทราบ..... ....
ลงชื่อ..... ผู้บังคับบัญชา (.....) ...../...../.....	☐ อนุมัติ ☐ ไม่อนุมัติ ..... ลงชื่อ..... (ผศ.ดร.ทพญ. สุภาวดี เนาว์รุ่งโรจน์) ผู้ช่วยคณบดีฝ่ายสารสนเทศ ...../...../.....	ลงชื่อ..... ( ) ...../...../.....

ภาคผนวก ค

ตารางสมรรถนะพื้นฐานทางด้านคอมพิวเตอร์ให้เหมาะสมกับลักษณะการปฏิบัติงาน

ตารางที่ ๒ สมรรถนะพื้นฐานทางด้านคอมพิวเตอร์ให้เหมาะสมกับลักษณะการปฏิบัติงาน ให้คลอบคลุม Digital Literacy ๙ ด้าน

ตำแหน่ง	ทักษะทางด้านคอมพิวเตอร์
๑. อาจารย์/ทันตแพทย์	๑.๑ โปรแกรมพื้นฐานที่ต้องใช้ภายในสำนักงาน MS Office เช่น Word, Excel, Power Point ๑.๒ โปรแกรมสำหรับโต้ตอบ รับ-ส่งอีเมล์ การใช้อินเทอร์เน็ต ๑.๓ โปรแกรมใช้สำหรับงานประชุม การเรียนการสอนออนไลน์ เช่น ZOOM, Google Meet, Microsoft Teams, VPN และ อื่น ๆ ๑.๔ การใช้งานระบบสารสนเทศโรงพยาบาลทันตกรรม (ระบบ HOSxPXE และ ระบบ PACs) ตามบทบาทหน้าที่การปฏิบัติงานของตนเอง ๑.๕ ระบบสารสนเทศสำหรับบุคลากรของมหาวิทยาลัยฯ เช่น DSS, TOR Online ๑.๖ ระบบรองรับการประเมินผลการเรียน เช่น LMS ระบบคลินิกรวมนักศึกษา ๑.๗ สามารถแก้ไขปัญหาคอมพิวเตอร์เบื้องต้น เช่น การเปลี่ยนหมึกพิมพ์ แก้ไขปัญหากระดาษติด ปรับช่วงเครื่องพิมพ์แคร่กระดาษต่อเนื่อง
๒. บุคลากรในสังกัดภาควิชา และ สำนักงานเลขานุการ	๒.๑ โปรแกรมพื้นฐานที่ต้องใช้ภายในสำนักงาน MS Office เช่น Word, Excel, Power Point ๒.๒ โปรแกรมสำหรับโต้ตอบ รับ-ส่งอีเมล์ การใช้อินเทอร์เน็ต ๒.๓ โปรแกรมใช้สำหรับงานประชุม การเรียนการสอนออนไลน์ เช่น ZOOM, Google Meet, Microsoft Teams, VPN และ อื่น ๆ ๒.๔ ระบบสารสนเทศสำหรับบุคลากรของมหาวิทยาลัยฯ เช่น DSS, TOR Online ๒.๕ ระบบสารสนเทศสำหรับการปฏิบัติงานของบุคลากร เช่น แจ้งซ่อม ครุภัณฑ์ จองห้องประชุม เบิกวัสดุออนไลน์ ๒.๖ สามารถแก้ไขปัญหาคอมพิวเตอร์เบื้องต้น เช่น การเปลี่ยนหมึกพิมพ์ แก้ไขปัญหากระดาษติด ปรับช่วงเครื่องพิมพ์แคร่กระดาษต่อเนื่อง ๒.๗ สามารถสร้างข้อมูลประชาสัมพันธ์หน่วยงานและ/หรือผลงานของตนเองได้ ผ่านช่องทางต่าง ๆ เช่น เว็บไซต์หน่วยงาน เฟซบุ๊ก เป็นต้น
๓. บุคลากรในสังกัดโรงพยาบาลทันตกรรม	๓.๑ โปรแกรมพื้นฐานที่ต้องใช้ภายในสำนักงาน MS Office เช่น Word, Excel, Power Point ๓.๒ โปรแกรมสำหรับโต้ตอบ รับ-ส่งอีเมล์ การใช้อินเทอร์เน็ต ๓.๓ โปรแกรมใช้สำหรับงานประชุม การเรียนการสอนออนไลน์ เช่น ZOOM, Google Meet, Microsoft Teams, VPN และ อื่น ๆ ๓.๔ การใช้งานระบบสารสนเทศโรงพยาบาลทันตกรรม (ระบบ HOSxPXE และ ระบบ PACs) ตามบทบาทหน้าที่การปฏิบัติงานของตนเอง ๓.๕ ระบบสารสนเทศสำหรับบุคลากรของมหาวิทยาลัยฯ เช่น DSS, TOR Online ๓.๖ ระบบสารสนเทศสำหรับการปฏิบัติงานของบุคลากร เช่น แจ้งซ่อม ครุภัณฑ์ จองห้องประชุม เบิกวัสดุออนไลน์

ตำแหน่ง	ทักษะทางด้านคอมพิวเตอร์
	๓.๗ สามารถแก้ไขปัญหาคอมพิวเตอร์เบื้องต้น เช่น การเปลี่ยนหมึกพิมพ์ แก้ไขปัญหากระดาษติด ปรับช่วงเครื่องพิมพ์แคร่กระดาษต่อเนื่อง ๓.๘ สามารถสร้างข้อมูลประชาสัมพันธ์หน่วยงานและ/หรือผลงานของตนเองได้ ผ่านช่องทางต่าง ๆ เช่น เว็บไซต์หน่วยงาน เฟซบุ๊ก เป็นต้น
๔. นักศึกษาทันตแพทย์ และทันตแพทย์หลังปริญญา และนักศึกษาผู้ช่วยทันตแพทย์	๔.๑ โปรแกรมพื้นฐานที่ต้องใช้ภายในสำนักงาน MS Office เช่น Word, Excel, Power Point ๔.๒ โปรแกรมสำหรับโต้ตอบ รับ-ส่งอีเมล์ การใช้อินเทอร์เน็ต ๔.๓ โปรแกรมใช้สำหรับงานประชุม การเรียนการสอนออนไลน์ เช่น ZOOM, Google Meet, Microsoft Teams, VPN และ อื่น ๆ ๔.๔ การใช้งานระบบสารสนเทศโรงพยาบาลทันตกรรม (ระบบ HOSxPXE และ ระบบ PACs) ตามบทบาทหน้าที่การปฏิบัติงานของตนเอง ๔.๕ ระบบสารสนเทศสำหรับบุคลากรของมหาวิทยาลัยฯ เช่น DSS, TOR Online ๔.๖ ระบบรองรับการประเมินผลการเรียน เช่น LMS ระบบคลินิกรวมนักศึกษา ๔.๗ สามารถแก้ไขปัญหาคอมพิวเตอร์เบื้องต้น เช่น การเปลี่ยนหมึกพิมพ์ แก้ไขปัญหากระดาษติด ปรับช่วงเครื่องพิมพ์แคร่กระดาษต่อเนื่อง

ภาคผนวก ง

ตารางการสำรองข้อมูลและแผนปฏิบัติงานและตารางการบริหารความเสี่ยงระบบเครือข่าย เครื่องแม่ข่าย ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

ตารางที่ ๓ การสำรองข้อมูล

ระบบสารสนเทศ	ความถี่	ผู้รับผิดชอบ
ระบบสนับสนุนงานบริหารและเว็บไซต์		
- เว็บไซต์คณะฯ และหน่วยงานภายในคณะฯ - ระบบประเมินรายวิชาบัณฑิตศึกษา - ระบบติดตามและรายงานผลการดำเนินงานในระดับยุทธศาสตร์ และระดับแผนปฏิบัติการ (Strategic Organization Development – sodd) - ระบบการสืบค้นผลงานทรัพย์สินทางปัญญา - ระบบคลังภาพกิจกรรม - Equipment management and scientific instrument service - PDPA Agreement - ระบบขอใช้เครื่องมือวิทยาศาสตร์ - ระบบลงทะเบียนออนไลน์ - ระบบคลังข้อมูลรายงานผู้ป่วย - ระบบใบเสร็จ - ระบบสั่งซื้อวัสดุ/เวชภัณฑ์ยา โรงพยาบาลทันตกรรม - ระบบคลังพัสดุออนไลน์ - ระบบฐานข้อมูลสมัครอบรมออนไลน์ - ระบบฐานข้อมูลผลงานวิจัย - ระบบโครงการวิจัย (Dent-PRPM) - ระบบจัดการใบนำฝาก – ถอนธนาคาร - ระบบออกใบเสร็จ หน่วยเงินรายได้ - ระบบงานค่าตอบแทนคลินิกนอกเวลา - Endodontic Charting - ระบบลงคะแนนคลินิกผู้สูงอายุ ระบบ e-Report (Keyreport) - ระบบ e-TOR16 (ระบบภาระงานส่วนงานกำหนดสายสนับสนุน) - ระบบ e-Workload16 (ระบบภาระงานส่วนงานกำหนดวิชาการ) - ระบบ e-Maintenance (แจ้งซ่อมวัสดุ-ครุภัณฑ์) - ระบบ e-Request - ระบบ e-Room - ระบบ e-Zoom - ระบบ e-LineNotify	ทุกวัน	สุทิศา จรียานุวัฒน์
Database Server (Mysql)	ทุกวัน	สุทิศา จรียานุวัฒน์
Database Server (Oracle Link จากสำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ)	ในวันศุกร์ของทุกสัปดาห์	สุทิศา จรียานุวัฒน์

ระบบสารสนเทศ	ความถี่	ผู้รับผิดชอบ
ระบบสนับสนุนการเรียนการสอนและการประเมินผล		
- ระบบ e-Clinic (คลินิกรวมนักศึกษา) - ระบบยื่นคำร้องเพื่อปรับปรุงข้อมูลการประเมิน - ระบบรายงานการลงปฏิบัติงานในคลินิกของนักศึกษา	ทุกวัน	มงคล ทองเพชรคง
- ระบบ e-student	ทุกวันสุดท้ายของเดือน	
- ระบบจอง Unit - ระบบประเมินการปฏิบัติงานห้อง Lab นักศึกษาชั้นปีที่ ๓ - ระบบจองห้องบรรยายออนไลน์	ทุกวัน	
ระบบสนับสนุนงานโรงพยาบาลทันตกรรม (E-Hospital)		
- ระบบฐานข้อมูลโรงพยาบาลทันตกรรม (HOSxPXE)	ทุกวัน (Day Backup) เวลา ๒๒.๐๐ น. ทุกวันเสาร์ (Full Baclup) เวลา ๐๐.๐๐ น.	นพสิทธิ์ ไชยนนท์ อุมา เพ็ชรคง รัชดา โรจน์หัสดิน
- ระบบคัดกรองก่อนการรักษาทางทันตกรรม	ทุกวัน	
ระบบบัญชีเครือข่าย		
- DHCP-Server สำหรับ สนล. + รพ. + Wi-Fi และการอบรม	ทุกวัน เวลา ๒๒.๐๐ น.	รัชดา โรจน์หัสดิน
- Core-Switch	ทุกสิ้นเดือน	

ตารางที่ ๔ ตารางแผนปฏิบัติงานและการบริหารความเสี่ยงระบบเครือข่าย เครื่องแม่ข่าย ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

แผนบริหารความเสี่ยง	ความถี่	ผู้รับผิดชอบ
ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก		
1. อัพเดทแพทช์ระบบปฏิบัติการของเครื่องแม่ข่าย		
1.1 www.dent.psu.ac.th	1 ครั้ง /เดือน	สุทิศา จรียานุวัฒน์
1.2 sys.dent.psu.ac.th	1 ครั้ง /เดือน	สุทิศา จรียานุวัฒน์
1.3 app.dent.psu.ac.th	1 ครั้ง /เดือน	สุทิศา จรียานุวัฒน์
1.4 his.dent.psu.ac.th	1 ครั้ง /เดือน	รัชดา โรจนหัสดิน
1.5 vcenter-dent.psu.ac.th(Hospital)	1 ครั้ง/ปี	รัชดา โรจนหัสดิน
1.6 vcenter2-dent.psu.ac.th(Office)	1 ครั้ง/ปี	รัชดา โรจนหัสดิน
1.7 vcenter3-dent.psu.ac.th(PACs)	1 ครั้ง/ปี	รัชดา โรจนหัสดิน
1.8 DHCP-Server(Office)	1 ครั้ง/ปี	รัชดา โรจนหัสดิน
1.9 DHCP-Server(Wi-Fi)	1 ครั้ง/ปี	รัชดา โรจนหัสดิน
1.10 DHCP-Server(LAB3515)	1 ครั้ง/ปี	รัชดา โรจนหัสดิน
1.11 DHCP-Server(Hospital)	1 ครั้ง/ปี	รัชดา โรจนหัสดิน
2. เปลี่ยนพาสเวิร์ดของเครื่องแม่ข่าย และอุปกรณ์กระจายสัญญาณ	2 ครั้ง/ ปี	รัชดา โรจนหัสดิน
3. การติดตาม (monitor) log file ของเครื่องแม่ข่าย	1 ครั้ง / สัปดาห์	รัชดา โรจนหัสดิน
4. อัพเดทเวอร์ชั่นของ wordpress ของเว็บไซต์คณะฯ และหน่วยงานภายในคณะฯ	ทุกวันสุดท้ายของเดือน	สุทิศา จรียานุวัฒน์
5. อัพเดทปลั๊กอินเว็บไซต์คณะฯ และหน่วยงานภายในคณะฯ	ทุกวันที่ 15 และวันสุดท้ายของเดือน	สุทิศา จรียานุวัฒน์
6. อัพเดท Certificate Web Server (psu.ac.th)	1 ครั้ง /ปี	สุทิศา จรียานุวัฒน์
7. อัพเดทเวอร์ชั่นระบบโรงพยาบาล (HOSxPXE)	2 ครั้ง / ปี	นพสิทธิ์ ไชยนนท์ อุมา เพ็ชรคง
การดูแลอุปกรณ์ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง		
1. ตรวจเช็คคอมพิวเตอร์และอุปกรณ์ต่อพ่วง เครื่องส่วนกลางและเครื่องให้บริการนักศึกษา	1 ครั้ง / ปี	ธีรเดช เขมะธีรรัตน์ ธนาวุฒิ สงสุข

ภาคผนวก จ

แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม

แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม

กลุ่มผู้ใช้งาน	หน่วยงานรับผิดชอบ	ขั้นตอนการส่งเอกสารปรับสถานะผู้ใช้งาน	ขั้นตอนการทวนสอบข้อมูล	ช่วงเวลาดำเนินการทวนสอบข้อมูล	รูปแบบรหัสผู้ใช้งาน	
					ปฏิบัติงานในเวลา	ปฏิบัติงาน ค. นอกเวลาฯ
1. ทันตแพทย์						
1.1 อ. ทพ./ทพ. ***มีสัญญาจ้างกับคณะฯ**	ภาควิชา/ธุรการ รพ. (ขึ้นอยู่กับหน่วยงานที่สังกัด)	หน่วยงานที่รับผิดชอบ ⓿ ธุรการ รพ. ⓿ หน่วย IT ***แจ้ง Update ข้อมูลทันทีเมื่อได้รับอนุมัติให้ลาออก/ลาศึกษาต่อ**	หน่วยการเจ้าหน้าที่ ⓿ หน่วย IT ***ทวนสอบข้อมูลตามช่วงเวลาที่กำหนด**	หน่วยการเจ้าหน้าที่ส่งข้อมูลรายชื่อทันตแพทย์ ที่ได้รับการอัพเดทจากหน่วยงานต้นสังกัด มาตลอดปี มายังงาน IT ใน สัปดาห์ที่ 3 ของเดือน**ธันวาคม**ของทุกปี หน่วย IT ดำเนินการสัปดาห์สุดท้าย ในเดือน**ธันวาคม**ของทุกปี	ชื่อ.อักษรสกุลตัวแรก	ชื่อ.อักษรสกุลตัวแรก
1.2 อ.ทพ. พิเศษ	หน่วยทะเบียนและประเมินผลการศึกษา และ หน่วยบัณฑิตศึกษา				ชื่อ.อักษรสกุลตัวแรก	11ชื่อ.อักษรสกุลตัวแรก *ตัวอย่าง 11nittayo.t*
1.3 ทพ. นอกเวลา ***มีคำสั่งแต่งตั้งจากคณะฯ**	คลินิกบริการทันตกรรมนอกเวลา				✗	11ชื่อ.อักษรสกุลตัวแรก *ตัวอย่าง 11nittayo.t*

HOSxP Username request for DENTISTs

1 ผู้ใช้งาน กรอกข้อมูลขอรหัสผู้ใช้ ผ่านระบบ E-request
https://sys.dent.psu.ac.th/erequest/

2 ผู้ใช้งานตรวจสอบความสมบูรณ์ในการกรอกข้อมูล พร้อมแนบไฟล์คำสั่งแต่งตั้ง เลือกส่งคำร้องไปยังผู้บังคับบัญชา เพื่ออนุมัติคำร้องในระบบ

3 สำนักงานธุรการ รพ. เสนอเรื่องที่ได้รับอนุมัติคำร้องโดยผู้บังคับบัญชา ไปยังผู้บริหาร รพ. เพื่ออนุมัติดำเนินการในระบบ และส่งเรื่องต่อมายังงาน IT

4 เจ้าหน้าที่ IT ตรวจสอบข้อมูล ส่งเรื่องให้หัวหน้างาน และผช.สารสนเทศ พิจารณาอนุมัติ

5 เจ้าหน้าที่ IT ดำเนินการบริหารจัดการรหัสผู้ใช้งานในระบบฯ และส่งข้อมูลให้ทันตแพทย์ทางอีเมล์ที่กรอกมาในคำร้อง

6 ผู้ใช้ตรวจสอบอีเมล์ลิงค์เข้าทำแบบทดสอบ เมื่อได้คะแนน 80% ขึ้นไป งาน IT ส่งอีเมล์รหัสผู้ใช้งานเพื่อเข้าสู่ระบบฯ
ผู้ใช้ควรเปลี่ยนรหัสผ่านทันที

โปรดดำเนินการขอรหัสผู้ใช้งานล่วงหน้า

3 งาน IT ดำเนินการ นับจากเอกสารในระบบ E-request ผ่านการอนุมัติดำเนินการ

วันทำการ

แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม

กลุ่มผู้ใช้งาน	หน่วยงานรับผิดชอบ	ขั้นตอนการส่งเอกสารปรับสถานะผู้ใช้งาน	ขั้นตอนการทวนสอบข้อมูล	ช่วงเวลาดำเนินการทวนสอบข้อมูล	รูปแบบรหัสผู้ใช้งาน	
					ปฏิบัติงานในเวลา	ปฏิบัติงาน ค. นอกเวลาฯ
2. นักศึกษาทันตแพทย์						
2.1 ระดับปริญญาตรี ชั้นปีที่ 4-6	หน่วยทะเบียนและประเมินผลการศึกษา	หน่วยทะเบียนและประเมินผลการศึกษา ⬇ ธุรการ รพ. ⬇ หน่วย IT *แจ้ง Update ข้อมูลทันทีเมื่อได้รับอนุมัติสำเร็จการศึกษา/เหตุแห่งการพ้นสภาพ	หน่วยทะเบียนและประเมินผลการศึกษา ⬇ ธุรการ รพ. ⬇ งาน IT *ทวนสอบข้อมูลตามช่วงเวลาที่กำหนด	หน่วยงานที่รับผิดชอบส่งข้อมูลภายในสัปดาห์แรกของภาคการศึกษา งาน IT ดำเนินการสัปดาห์ที่ 2 ของภาคการศึกษา	รหัสนักศึกษา	X
2.2 ระดับปริญญาตรี เก็บเคส					33.รหัสนักศึกษา *ตัวอย่าง* *33.0123456789*	

หมายเหตุ ขั้นตอนการปรับสถานะผู้ใช้งาน

1. **กรณีรับนักศึกษาใหม่** หน่วยทะเบียนฯ ส่งไฟล์ข้อมูลรายชื่อ รหัสบัตรประชาชน พร้อมรหัสนักศึกษาในรูปแบบไฟล์ .xlsx ➲ ธุรการ รพ. ➲ งาน IT (ดำเนินการช่วงเดือน**สิงหาคม**ของทุกปี)
2. **กรณีจบการศึกษา** หน่วยทะเบียนฯ ส่งไฟล์ข้อมูลรายชื่อพร้อมรหัสนักศึกษาในรูปแบบไฟล์ .xlsx ➲ ธุรการ รพ. ➲ งาน IT (ดำเนินการทันที Update เป็นปัจจุบัน)
3. **กรณีนักศึกษาเก็บเคส** ส่งไฟล์ข้อมูลรายชื่อ รหัสบัตรประชาชน พร้อมรหัสนักศึกษาในรูปแบบไฟล์ .xlsx พร้อมระบุช่วงเวลาที่ต้องคงอยู่ในระบบฯ

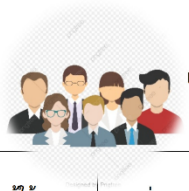
HOSxP Username request for Undergrad students

แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม

กลุ่มผู้ใช้งาน	หน่วยงานรับผิดชอบ	ขั้นตอนการส่งเอกสารปรับสถานะผู้ใช้งาน	ขั้นตอนการทวนสอบข้อมูล	ช่วงเวลาดำเนินการทวนสอบข้อมูล	รูปแบบรหัสผู้ใช้งาน	
					ปฏิบัติงานในเวลา	ปฏิบัติงาน ค. นอกเวลาฯ
3. ทันตแพทย์หลังปริญญา						
3.1 ทันตแพทย์หลังปริญญา	ภาควิชา และ หน่วยบัณฑิตศึกษา	หน่วยงานในสังกัด ⇩ หน่วยบัณฑิตศึกษา ⇩ ธุรการ รพ. ⇩ งาน IT ***แจ้ง Update ข้อมูลทันทีเมื่อได้รับอนุมัติสำเร็จการศึกษา/เหตุแห่งการพ้นสภาพ**	หน่วยงานในสังกัด ⇩ หน่วยบัณฑิตศึกษา ⇩ หน่วยการเจ้าหน้าที่ ⇩ ธุรการ รพ. ⇩ งาน IT ***ทวนสอบข้อมูลตามช่วงเวลาที่กำหนด**	หน่วยงานที่รับผิดชอบส่งข้อมูลภายในสัปดาห์แรกของภาคการศึกษา งาน IT ดำเนินการสัปดาห์ที่ 2 ของภาคการศึกษา	รหัสนักศึกษา	11ชื่อ.อักษรสกุลตัวแรก *ตัวอย่าง 11nittaya.t* (ดำเนินการทวนสอบเหมือน ข้อ 1.3 ทพ. ***ไม่มีสัญญาจ้างกับคณะฯ**)
3.2 ทันตแพทย์หลังปริญญาเก็บเคส				หน่วยงานต้นสังกัดรับผิดชอบส่งข้อมูล พร้อมระบุช่วงเวลาที่ต้องคงอยู่ในระบบฯ งาน IT ดำเนินการ 3 วันทำการ นับจากได้รับแจ้งเอกสารผ่านทางระบบ E-doc	66.รหัสนักศึกษา *ตัวอย่าง* *66.0123456789*	

หมายเหตุ ขั้นตอนการปรับสถานะผู้ใช้งาน

1. **กรณีรับนักศึกษาใหม่** หน่วยบัณฑิตรวบรวมข้อมูลจากภาควิชา นำส่งไฟล์ข้อมูลส่วนบุคคล รายละเอียดข้อมูลตามแบบฟอร์มขอ user HOSxP ส่งข้อมูลมาในรูปแบบไฟล์ .xlsx พร้อมบันทึกข้อความประหน้า ➲ ธุรการ รพ. ➲ งาน IT (ดำเนินการช่วงเดือน**สิงหาคม**ของทุกปี)
2. **กรณีจบการศึกษา** หน่วยบัณฑิตรวบรวมข้อมูลจาภาควิชา นำส่งไฟล์ข้อมูลส่วนบุคคล รายละเอียดข้อมูลตามแบบฟอร์มขอ user HOSxP ส่งข้อมูลมาในรูปแบบไฟล์ .xlsx พร้อมบันทึกข้อความประหน้า ➲ ธุรการ รพ. ➲ งาน IT (ดำเนินการทันที Update เป็นปัจจุบัน)
3. **กรณีนักศึกษาเก็บเคส** ภาควิชา ส่งไฟล์ข้อมูลรายชื่อ รหัสนักศึกษาในรูปแบบไฟล์ .xlsx พร้อมระบุช่วงเวลาที่ต้องคงอยู่ในระบบฯ ➲ หน่วยบัณฑิต ➲ ธุรการ รพ. ➲ งาน IT (หมายเหตุ หน่วยบัณฑิตสำเนาข้อมูลส่ง ➲ หน่วยการเจ้าหน้าที่ เพื่อ Update ข้อมูลเป็นปัจจุบัน)



แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม

กลุ่มผู้ใช้งาน	หน่วยงานรับผิดชอบ	ขั้นตอนการส่งเอกสารปรับสถานะผู้ใช้งาน	ขั้นตอนการทวนสอบข้อมูล	ช่วงเวลาดำเนินการทวนสอบข้อมูล	รูปแบบรหัสผู้ใช้งาน	
					ปฏิบัติงานในเวลา	ปฏิบัติงาน ค. นอกเวลาฯ
4. บุคลากร						
4.1 สังกัด รพ. ทันตกรรม ***มีสัญญาจ้างกับคณะฯ**	ธุรการ รพ./ คลินิกต่าง ๆ/ หน่วยการเจ้าหน้าที่ (ขึ้นอยู่กับหน่วยงานที่สังกัด)	หน่วยงานที่รับผิดชอบ ➲ ธุรการ รพ. ➲ หน่วยการเจ้าหน้าที่ ➲ งาน IT ***แจ้ง Update ข้อมูลทันทีเมื่อได้รับอนุมัติเข้าปฏิบัติงาน/ลาออก**	หน่วยการเจ้าหน้าที่ ➲ งาน IT ***ทวนสอบข้อมูลตามช่วงเวลาที่กำหนด**	หน่วยการเจ้าหน้าที่ส่งข้อมูลรายชื่อบุคลากร ที่ได้รับการอัพเดทจากหน่วยงานต้นสังกัด มาตลอดปีมายังงาน IT ใน สัปดาห์ที่ 3 ของเดือน**ธันวาคม** ของทุกปี งาน IT ดำเนินการสัปดาห์สุดท้ายของเดือน**ธันวาคม**ของทุกปี	ชื่อ.อักษรสกุลตัวแรก	ชื่อ.อักษรสกุลตัวแรก
4.1.1 เจ้าหน้าที่ รพ. ทั้งหมด						
4.1.2 เจ้าหน้าที่รายคาบ						
4.2 สังกัดสำนักงานเลขานุการ**	หน่วยการเจ้าหน้าที่					
4.3 เจ้าหน้าที่ ค. นอกเวลาฯ ***มีคำสั่งแต่งตั้งจากคณะฯ รวมถึง จนท. คณะฯ ที่ทำงานเสริม ณ ค. นอกเวลาฯ**	คลินิกบริการทันตกรรมนอกเวลา				✗	22ชื่อ.อักษรสกุลตัวแรก *ตัวอย่าง 22nittaya.t*
4.5 เจ้าหน้าที่งาน IT	งาน IT	ดำเนินการเหมือน 1.1 ทพ. สัญญาจ้าง Admin ระบบ HIS **ของงาน IT บริหารจัดการข้อมูลตามบทบาทหน้าที่ของเจ้าหน้าที่ในงาน**		สัปดาห์ที่ 3 ของเดือน**เมษายน** ของทุกปี งาน IT ดำเนินการสัปดาห์สุดท้ายของเดือน**เมษายน** ของทุกปี	ชื่อ.อักษรสกุลตัวแรก	✗
หมายเหตุ ข้อ 4.2 ขั้นตอนการปรับสถานะผู้ใช้งานดำเนินการดังนี้ หน่วยงานที่รับผิดชอบ ➲ หน่วยการเจ้าหน้าที่ ➲ ธุรการ รพ. ➲ งาน IT						

หมายเหตุ :

๑. กำหนดให้**<u>ไฟล์ข้อมูล</u>** การทวนสอบข้อมูลผู้ใช้ที่จะส่งมายังงานไอที **<u>เป็นไฟล์ Excel เท่านั้น</u>**

๒. **<u>การทวนสอบข้อมูล</u>**ผู้ใช้ของทุกหน่วยงาน**<u>จะต้องมีทั้งข้อมูลผู้ใช้งานที่ยังคงปฏิบัติงานอยู่</u>** และ**<u>ข้อมูลผู้ใช้งานที่พ้นสภาพ/ลาออกไปแล้ว</u>**ในรอบปีที่ทวนสอบข้อมูลพ้นสภาพ/ลาออกไปแล้วในรอบปีที่ทวนสอบข้อมูล

๓. กรณีผู้ใช้งานขอรหัสผู้ใช้งานให้หน่วยงานผู้รับผิดชอบแจ้งผู้ใช้กรอกข้อมูลในแบบฟอร์มขอ User HOSxPXE ของงาน IT อนุมัติโดยรองคณบดี/ผู้ช่วยคณบดีของหน่วยงาน นำเรื่องเข้าระบบ E-doc ส่งไปยังสำนักงานธุรการ รพ. เพื่อรับการอนุมัติจากผู้บริหารโรงพยาบาล และส่งเรื่องต่อ ให้งาน IT ดำเนินการต่อไป (ตาม Flow User Request for HOSxPXE ในแต่ละกรณีข้างต้น)

๔. ผู้ใช้งานระบบฯ ทุกท่านจะต้องได้รับการอบรมการใช้งานระบบฯ ตามบทบาทหน้าที่การปฏิบัติงานของตนเอง โดยงาน IT และทำแบบทดสอบความรู้ความเข้าใจในการใช้งานระบบฯ ผ่านอย่างน้อย ๘๐% ของคะแนนทดสอบ จึงจะเข้าใช้งานระบบฯได้

๕. ผู้ใช้งานระบบฯ ต้องทำการเปลี่ยน Password ใหม่ ทุก ๓ เดือน/๙๐ วัน ตามเงื่อนไขการตั้ง Password ใหม่ ดังนี้

๕.๑. ความยาวไม่น้อยกว่า ๔ หลัก

๕.๒. ประกอบด้วยตัวอักษรพิมพ์เล็กและพิมพ์ใหญ่อย่างน้อย ๑ ตัว

๕.๓. ตัวเลข สัญลักษณ์ มีหรือไม่มีก็ได้

๖. หากเปิดใช้งานระบบค้างไว้นานเกิน ๑๘๐ นาที/๓ ชั่วโมง ระบบจะทำการ Logout ผู้ใช้ทำการ Login เข้าใช้งานระบบใหม่

ภาคผนวก ฉ

บัญชีผู้ดูแลระบบ/ผู้ใช้งานระบบส่วนกลางมหาวิทยาลัย

ตารางที่ ๕ ระบบงานบริหารบุคคล การเงิน สำนักงาน

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
๑	MIS-DSS	ระบบการเจ้าหน้าที่	https://dss.psu.ac.th/dss_person	นางสุธาสินี ตั่นหุ้ย นางเสาวณี แซ่หลี นางสุทิศา จรียานุวัฒน์ นางทิชาภรณ์ รัตนะ นางสาวเพลินพิศ สิทธิจันทร์	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th suthisa.j@psu.ac.th tichaporn.r@psu.ac.th phleanphit.s@psu.ac.th
		ระบบขอลาหยุดราชการ		นางสุธาสินี ตั่นหุ้ย นางเสาวณี แซ่หลี นางสาวธัญพิชชา ชูโสต นางทิชาภรณ์ รัตนะ นางสาวเพลินพิศ สิทธิจันทร์	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th thanpitcha.s@psu.ac.th tichaporn.r@psu.ac.th phleanphit.s@psu.ac.th
		ระบบการจัดอบรมเพื่อพัฒนาบุคลากร		นางเสาวณี แซ่หลี นางทิชาภรณ์ รัตนะ นางสาวเพลินพิศ สิทธิจันทร์ นางสุริวัสสา จันทร์เขียว	saowanee.sa@psu.ac.th tichaporn.r@psu.ac.th phleanphit.s@psu.ac.th suriwatsa.j@psu.ac.th
๒	Resume	ระบบสมัครงานและรายงานตัวออนไลน์	https://resume.psu.ac.th	นางสุธาสินี ตั่นหุ้ย นางเสาวณี แซ่หลี	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th
๓	Fund	ระบบกองทุนสวัสดิการพนักงานมหาวิทยาลัย	https://fund.psu.ac.th	นายสุภัทร์ พงศาธิรัตน์ นางกวินทิพย์ ชูศรี	supat.p@psu.ac.th kavinthip.l@psu.ac.th
๔	PVD	ระบบกองทุนสำรองเลี้ยงชีพ	https://pvd.psu.ac.th	นายสุภัทร์ พงศาธิรัตน์ นางสุธาสินี ตั่นหุ้ย	supat.p@psu.ac.th sutasinee.n@psu.ac.th
๕	work.psu.ac.th	ระบบดูรายงานการลงเวลาปฏิบัติราชการบนเว็บของบุคลากรในหน่วยงาน	https://work.psu.ac.th	นางสุธาสินี ตั่นหุ้ย นางเสาวณี แซ่หลี	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th
๖	PSU Passport	ระบบจัดการบัญชีผู้ใช้งาน	https://adsadmin.psu.ac.th	นางสุธาสินี ตั่นหุ้ย	sutasinee.n@psu.ac.th

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
		ระบบสารสนเทศ			
๗	TOR Online	ระบบประเมินผลการปฏิบัติงาน	https://tor.psu.ac.th	นางสุธาสินี ตั่นหุ้ย นางเสาวณี แซ่หลี นางสาวนิตตยา ตรีสุวรรณ	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th nittaya.t@psu.ac.th
๘	Competency	ระบบประเมินสมรรถนะ	https://competency.psu.ac.th	นางสุธาสินี ตั่นหุ้ย นางเสาวณี แซ่หลี นางสุทิศา จรียานุวัฒน์	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th suthisa.j@psu.ac.th
๙	hrmis	ระบบผลงานวิชาการและภาระงาน	https://hrmis.psu.ac.th	นางสุธาสินี ตั่นหุ้ย นางสาวกนกวรรณ สุวรรณรัตน์ นายเขมรัฐ เขมวงศ์ นางสุทิศา จรียานุวัฒน์	sutasinee.n@psu.ac.th kanokwan.s@psu.ac.th kemarajt.k@psu.ac.th suthisa.j@psu.ac.th
๑๐	aod	ระบบบริการวิชาการ	https://aod.psu.ac.th	นางสุริวัสสา จันทร์เขียว	suriwatsa.j@psu.ac.th
๑๑	MOU	ระบบข้อตกลงความร่วมมือระหว่างมหาวิทยาลัยสงขลานครินทร์กับมหาวิทยาลัย/สถาบันต่างประเทศ	https://iao.psu.ac.th	นางสาวปวีณรัตน์ ณ พัทลุง	paweenrat.n@psu.ac.th
๑๒	epr	ระบบตะกร้าข้าว	https://epr.psu.ac.th	นางอัญชลี สุวรรณโร	aunchalee.su@psu.ac.th
๑๓	edoc	ระบบเอกสาร	https://edoc.psu.ac.th	นางนารี จันทรัตน์	naree.t@psu.ac.th
๑๔	emeeting	ระบบประชุม	http://meeting.dent.psu.ac.th/dentmeeting	นางสาวจรรยากร คงแก้ว นางทิชาภรณ์ รัตนะ	janyakorn.k@psu.ac.th tichaporn.r@psu.ac.th

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
๑๕	Management Accounting System (PSU-MAS)	ระบบสารสนเทศบัญชี-การเงิน		นายสุพจน์ ตรีรัญเพ็ชร นายสุภัทร์ พงศาธิรัตน์ นางสาวอรวรรณ เจริญวุฒิวงษา นางกวินทิพย์ ชูศรี นางสาวชื่นพจี เสน่หา นางกาญจนา กัลยาศิริ นางปิ่นประภา ทันหะวาส นางเสาวณี แซ่หลี นางสาวผกาพฤษ สีดำอ่อน นางสาวเครือวัลย์ พวงสอน นางสาวฉัตทริกา หลีเบ็นหมาน นางสาวปวริศา ณ พัทลุง นางวิภาดา อัครภา นางสาวปรียาภัทร์ ยอดทอง	supot.t@psu.ac.th supat.p@psu.ac.th orawan.ch@psu.ac.th kavinthip.l@psu.ac.th cheunpajee.s@psu.ac.th kanchana.ka@psu.ac.th pinprapa.k@psu.ac.th saowanee.sa@psu.ac.th pagrapruk.s@psu.ac.th kruawon.p@psu.ac.th chattarika.l@psu.ac.th pawarisa.n@psu.ac.th wipada.a@psu.ac.th peeyapat.y@psu.ac.th
๑๖	ALIST	ระบบห้องสมุดอัตโนมัติ		นางสาวสาวิตรี วงศ์สันติ	sawitree.w@psu.ac.th

ตารางที่ ๖ ระบบงานวิจัย

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
๑	prpm	ระบบบริหารงานวิจัย	https://prpm.psu.ac.th	นายเขมรัฐ เขมวงศ์ นางสาวปรียาภัทร์ ยอดทอง	kemarajt.k@psu.ac.th peeyapat.y@psu.ac.th
๒	hrmis	ระบบผลงานวิชาการและภาระ งาน	https://hrmis.psu.ac.th	นายเขมรัฐ เขมวงศ์ นางสาวปรียาภัทร์ ยอดทอง	kemarajt.k@psu.ac.th peeyapat.y@psu.ac.th
๓	NRIIS	ระบบข้อมูลสารสนเทศวิจัยและนวัตกรรมแห่งชาติ	http://nriis.nrct.go.th	นายเขมรัฐ เขมวงศ์ นางสาวปรียาภัทร์ ยอดทอง	kemarajt.k@psu.ac.th peeyapat.y@psu.ac.th

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
๔	Article Reward Online : ARO	ระบบรางวัลบทความตีพิมพ์ของมหาวิทยาลัยสงขลานครินทร์	https://aro.psu.ac.th/arotest	นางสาวปรียาภัทร์ ยอดทอง	peeyapat.y@psu.ac.th

ตารางที่ ๗ ระบบทะเบียนและบัณฑิตศึกษา (การศึกษา)

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
๑	SIS	ระบบสารสนเทศนักศึกษา	https://sis-hatyai6.psu.ac.th	นางปวริศา เส้งเสน นางลัดดาวัลย์ วงค์ไชย นางวรรณรี ชาติดำ นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตรีรานุรัตน์ นางสาวพิมพ์สุจี ศรีสุวรรณ นางรณิดา อำภา	pawarisa.s@psu.ac.th laddawan.w@psu.ac.th wannaree.t@psu.ac.th nongyaow.u@psu.ac.th benjawan.t@psu.ac.th pimsujee.s@psu.ac.th ranida.a@psu.ac.th
๒	tqf	ระบบ มคอ.3 และ มคอ.5 ออนไลน์	https://tqf.psu.ac.th	นางปวริศา เส้งเสน นางสาว ธนิษฐา อวิรุตม์ นางสาววรวรรณ พฤษศรี นางสาวเบญจวรรณ ตรีรานุรัตน์ นางสาวพิมพ์สุจี ศรีสุวรรณ นางรณิดา อำภา นางอัจฉรา ทิพย์สุเนตร	pawarisa.s@psu.ac.th thanittha.a@psu.ac.th worrawan.p@psu.ac.th benjawan.t@psu.ac.th pimsujee.s@psu.ac.th ranida.a@psu.ac.th atchara.th@psu.ac.th
๓	PSU-TES	ระบบประเมินอาจารย์ออนไลน์	https://tes.psu.ac.th/login.asp	นางปวริศา เส้งเสน นางลัดดาวัลย์ วงค์ไชย นางสาววรวรรณ พฤษศรี นางสาวเบญจวรรณ ตรีรานุรัตน์ นางสาวพิมพ์สุจี ศรีสุวรรณ นางรณิดา อำภา นางณภัทรชนก มหาเกตุ	pawarisa.s@psu.ac.th laddawan.w@psu.ac.th worrawan.p@psu.ac.th benjawan.t@psu.ac.th pimsujee.s@psu.ac.th ranida.a@psu.ac.th napatchanok.m@psu.ac.th
๔	ระบบสารสนเทศบัณฑิตวิทยาลัย	ระบบสารสนเทศบัณฑิตวิทยาลัย	https://gradmis.psu.ac.th	นางปวริศา เส้งเสน นางสาวเบญจวรรณ ตรีรานุรัตน์	pawarisa.s@psu.ac.th benjawan.t@psu.ac.th
๕	ระบบรับเข้านักศึกษา	ระบบรับเข้านักศึกษา	https://gradmis.psu.ac.th/grad_admission	นางปวริศา เส้งเสน นางสาวเบญจวรรณ ตรีรานุรัตน์ นางรณิดา อำภา นางณภัทรชนก มหาเกตุ	pawarisa.s@psu.ac.th benjawan.t@psu.ac.th ranida.a@psu.ac.th napatchanok.m@psu.ac.th
๖	ระบบการจัดสรรทุนการศึกษา	ระบบการจัดสรรทุนการศึกษา	https://gradmis.psu.ac.th/grad_scholarship	นางปวริศา เส้งเสน นางสุดาวัลย์ จิโรจน์วณิชชากร นางสาวเบญจวรรณ ตรีรานุรัตน์	pawarisa.s@psu.ac.th sudawan.j@psu.ac.th benjawan.t@psu.ac.th

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
	ระดับบัณฑิตศึกษา	ระดับบัณฑิตศึกษา			
๗	ระบบการเบิกจ่ายทุนอุดหนุนการวิจัยเพื่อวิทยานิพนธ์	ระบบการเบิกจ่ายทุนอุดหนุนการวิจัยเพื่อวิทยานิพนธ์	https://gradmis.psu.ac.th/scholar_payment	นางปวริศา เส้งเสน นางสาวเบญจวรรณ ตรีรานุรัตน์	pawarisa.s@psu.ac.th benjawan.t@psu.ac.th
๘	ระบบ GSMIS	ระบบ GSMIS (แต่งตั้งอาจารย์พิเศษ)	https://gsmis.psu.ac.th/gsmis2	นางปวริศา เส้งเสน นางสาวเบญจวรรณ ตรีรานุรัตน์	pawarisa.s@psu.ac.th benjawan.t@psu.ac.th
๙	ระบบการขออนุมัติเดินทางไปต่างประเทศ	Inbound / Outbound for Student	https://io-student.psu.ac.th	นางปวริศา เส้งเสน นางวรรณรี ชาติดำ นางสุดาวัลย์ จิโรจน์วณิชชากร นางสาวเบญจวรรณ ตรีรานุรัตน์	pawarisa.s@psu.ac.th wannaree.t@psu.ac.th sudawan.j@psu.ac.th benjawan.t@psu.ac.th
๑๐	Fiscal management information system: FMIS	ระบบการจัดเก็บค่าธรรมเนียมการศึกษา	https://fmisbudget.psu.ac.th		
๑๑	ทรานสคริปกิจกรรมนักศึกษา	ทรานสคริปกิจกรรมนักศึกษา	https://student.psu.ac.th/TS234	นางวรรณรี ชาติดำ	wannaree.t@psu.ac.th
๑๒	Tell Me More Online		http://tmm.psu.ac.th	นางสุริวัสสา จันทร์เขียว	suriwatsa.j@psu.ac.th

ตารางที่ ๘ ระบบสารสนเทศภายนอกมหาวิทยาลัย

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
๑	NSHO-UC	โปรแกรมตรวจสอบสิทธิ สปสช	https://www.nhso.go.th/frontend/page-information_detail.aspx?ContentID=NjEwMDAwMzI3	นางสาววรวรรณ สมัตถนาค นางเครือสิรี เดชชนินทร์	vorawan.s@psu.ac.th kruasiree.d@psu.ac.th
๒	E-claim	โปรแกรมเบิกจ่ายตรง	https://eclaim.nhso.go.th/webComponent/	นางพิกุล อนันต์	pigul.k@psu.ac.th
๓	HRMS	ระบบสารสนเทศการบริหารจัดการความเสี่ยงของสถานพยาบาล (Healthcare Risk Management System)	http://dpsu.thai-nrls.org/	นางสาวราเวีย ฮูเสน	ravia.h@psu.ac.th
๔	dfct-kpi	ระบบฐานข้อมูลตัวชี้วัด	https://mis.dent.cmu.ac.th/dfct-kpi/web/index.php?r=site/login	นางสาวกนกวรรณ สุวรรณรัตน์ นางลัดดาวัลย์ วงค์ไชย นางสาวสุทิศา จรียานุวัฒน์	kanokwan.s@psu.ac.th laddawan.w@psu.ac.th suthisa.j@psu.ac.th

ภาคผนวก ช

บัญชีผู้ดูแลระบบ/ผู้ใช้งานระบบสารสนเทศ คณะทันตแพทยศาสตร์ (คณะฯ พัฒนาระบบเอง)

ตารางที่ ๙ ระบบสารสนเทศสนับสนุนบริหารบุคคล การเงิน สำนักงาน

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address	หมายเหตุ
๑	e-TOR16	ระบบภาระงานส่วนงานกำหนดสายสนับสนุน	https://sys.dent.psu.ac.th/tor16	นางสุธาสินี ตั้นหุ้ย	sutasinee@psu.ac.th	
		ระบบภาระงานส่วนงานกำหนดวิชาการ	https://sys.dent.psu.ac.th/workload16/			
๒	e-Activity	ระบบลงทะเบียนกิจกรรมหน่วยการเจ้าหน้าที่	https://sys.dent.psu.ac.th/activity/app/	นางสุธาสินี ตั้นหุ้ย นางทิชาภรณ์ รัตนะ นางสาวจรรยากร คงแก้ว	sutasinee@psu.ac.th tichaporn.r@psu.ac.th janyakorn.k@psu.ac.th	
๓	e-Training	ลงทะเบียนโปรแกรมการอบรมคอมพิวเตอร์	https://sys.dent.psu.ac.th/training	นางสาวนิตตยา ตรีสุวรรณ	nittaya.t@psu.ac.th	
๔		ระบบคลังพัสดุออนไลน์	http://10.151.127.68/mis	นางสาวฉัตทริกา หลีเบ็นหมาน	chattarika.l@psu.ac.th	
๕	e-LineNotify	ระบบแจ้งเตือน				
๖	e-Report (Key Report)	ระบบรายงานสำหรับผู้บริหาร	https://sys.dent.psu.ac.th/reportcenter	นางสาวกนกวรรณ สุวรรณรัตน์	kanokwan.s@psu.ac.th	
	Strategic Organization Development System	ระบบติดตามและรายงานผลการดำเนินงานในระดับยุทธศาสตร์และระดับแผนปฏิบัติการ	https://sys.dent.psu.ac.th/keyreport/			

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address	หมายเหตุ
๗		ระบบออกใบเสร็จหน่วยคลัง	https://app.dent.psu.ac.th/app/bill	นางสาวอรวรรณ เจริญวุฒิวงษา	orawan.ch@psu.ac.th	
๘	e-Maintenance	ระบบแจ้งซ่อมครุภัณฑ์-วัสดุ	https://sys.dent.psu.ac.th/repair	- **ส่วนแจ้งซ่อมงานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ** นางสาวนิตตยา ตรีสุวรรณ นายธีรเดช เขมะธีรรัตน์ นายธนาวุฒิ สงสุข - **ส่วนแจ้งซ่อมงานวิศวะ** นางสาวอุษา สวัสดี นายนิพัฒน์ พลด้วง	nittaya.t@psu.ac.th teeradet.k@psu.ac.th tanawut.s@psu.ac.th usa.sa@psu.ac.th niphat.p@psu.ac.th	
๙	e-Zoom			นางสาววาสนา โกมล	wasana.ko@psu.ac.th	
๑๐	e-request		https://sys.dent.psu.ac.th/erequest	- **ส่วนงานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ** นางสาวนิตตยา ตรีสุวรรณ - **ส่วนงานธุรการโรงพยาบาล** นางสาวเพลินพิศ สิทธิจันทร์ นางทิชาภรณ์ รัตนะ	nittaya.t@psu.ac.th phleanphit.s@psu.ac.th tichaporn.r@psu.ac.th	
๑๑	e-Proofing Programs	ระบบจองโปรแกรมขัดเกลาภาษา	http://10.151.127.78/eproofing/	นายเขมรัฐ เขมวงศ์	kemarajt.k@psu.ac.th	
๑๒	e-room	ระบบ e-Room ระบบจองห้องคณะทันตแพทยศาสตร์ (ห้องบรรยาย / ห้องคอม / ห้องประชุม)	https://sys.dent.psu.ac.th/eroom/	- **ห้องบรรยาย** นางสาว ธนิษฐา อวิรุตม์ - **ห้องประชุม** นางสาวสุดารัตน์ สังข์ทอง - **ห้องปฏิบัติคอมพิวเตอร์** นางสาวนิตตยา ตรีสุวรรณ - **ห้องแลปทันตกรรม** นางณัฐธิดา หาญชนะ	thanittha.a@psu.ac.th sudarat.s@psu.ac.th nittaya.t@psu.ac.th natthidar.h@psu.ac.th	
๑๓	complaintcenter		https://sys.dent.psu.ac.th/complaintcenter/	- อาจารย์วรรธนะ พิธพรชัยกุล - นางสาวรัชฎาภรณ์ นะมาเส - นางสาวพรชนก ช่วยวิจิตร	wattana.p@psu.ac.th ratchadaporn.j@psu.ac.th pornchanok.c@psu.ac.th	

ตารางที่ ๑๐ ระบบงานวิจัย

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address	หมายเหตุ
๑	Research Laboratory Risk Management System	ระบบบริหารจัดการความเสี่ยงห้องปฏิบัติการวิจัย	https://sys.dent.psu.ac.th/dentlabrisk	นายเขมรัฐ เขมวงศ์ นางสาวสโรชา ฤทธิเดช	kemarajt.k@psu.ac.th sarocha.ri@psu.ac.th	
๒	EM-EMS	ระบบขอใช้พื้นที่และยืมเครื่องมือวิจัยวิจัย	https://sys.dent.psu.ac.th/emsis/	นายเขมรัฐ เขมวงศ์ นางสาวสโรชา ฤทธิเดช	kemarajt.k@psu.ac.th sarocha.ri@psu.ac.th	

ตารางที่ ๑๑ ระบบสารสนเทศสนับสนุนโรงพยาบาล

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address	หมายเหตุ
๑	e-Consent	ระบบแบบฟอร์มขอความยินยอม	http://his.dent.psu.ac.th/consentform/	นางสาวราเวีย ฮูเส็น	ravia.h@psu.ac.th	
๒		ระบบตรวจเช็คครุภัณฑ์โรงพยาบาลทันตกรรม	https://sys.dent.psu.ac.th/maintain	นางสาวปภัชญา โกศัยกานนท์	maythinee.k@psu.ac.th	
๓	e-Report (Dynamic)	ระบบรายงานสารสนเทศโรงพยาบาลทันตกรรม (HOSxPXE)	https://sys.dent.psu.ac.th/ptreport			
๔	Endodontic Charting		10.0.1.108/special	อาจารย์และนักศึกษา สาขา Endodontic		
๕	Elderly	ระบบคลินิกผู้สูงอายุ	http://10.151.127.208/elderly	นางกานดา ณ พัทลุง (คลินิกศัลย์) นางพิกุล ชโนวรรณะ (คลินิก OM-OPT) นางสาวปทิตญา ทะสะระ (คลินิกบัณฑิต 2)	kanda.su@psu.ac.th pikul.c@psu.ac.th patidthaya.t@psu.ac.th	

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address	หมายเหตุ
				นางสาวศิริวดี บัวดวง (คลินิกสูงอายุ) อ.สุพิชชา ตลึงจิตร (ดูแลภาพรวม)	siriwadee.b@psu.ac.th supitcha.t@psu.ac.th	
๖		ระบบบออกใบเสร็จ หน่วยเงินรายได้	10.0.1.108/bill_income	นางวิภาดา อัครภา นางสาวสุภาวดี นุ่นสง นางจินดา หนูหมื่น	wipada.a@psu.ac.th supawadee.d@psu.ac.th jinda.n@psu.ac.th	
๗		ระบบงานค่าตอบแทนคลินิกนอกเวลา	10.0.1.108/overtime	นางจินดา หนูหมื่น	supawadee.d@psu.ac.th	
๘		ระบบจัดการใบนำฝาก - ถอนเงินธนาคาร	10.0.1.108/payin	นางสาวสุภาวดี นุ่นสง	supawadee.d@psu.ac.th	
๙	recall	ระบบคิวผู้ป่วยเด็ก (ลงคิว recall ผู้ป่วยเด็ก ที่ผ่านการผ่าตัด full mouth rehab)	10.0.1.108/recall_ga	นางยินดี ไชยจิตร	yindee.c@psu.ac.th	
๑๐	recall	ระบบคิวผู้ป่วยเด็ก (ลงคิว recall ผู้ป่วย เด็ก)	10.0.1.107/recall	นางยินดี ไชยจิตร	yindee.c@psu.ac.th	
๑๑		ระบบเปลี่ยนรหัสผ่าน HOSxPXE	10.0.1.108/resetpw			

ตารางที่ ๑๒ ระบบทะเบียนและบัณฑิตศึกษา (การศึกษา)

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address	หมายเหตุ
๑		ระบบประเมินรายวิชาบัณฑิตศึกษา คณะทันตแพทยศาสตร์	https://app.dent.psu.ac.th/eval	นางปวริศา เส้งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางลัดดาวัลย์ วงค์ไชย นางกัลยา โลหะประเสริฐ นางสาววรวรรณ พฤษศรี นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตรีรานุรัตน์ นางสาวพิมพ์สุจี ศรีสุวรรณ นางรณิดา อำภา	pawarisa.s@psu.ac.th paweenrat.n@psu.ac.th laddawan.w@psu.ac.th kanlaya.l@psu.ac.th worrawan.p@psu.ac.th nongyaow.u@psu.ac.th benjawan.t@psu.ac.th pimsujee.s@psu.ac.th ranida.a@psu.ac.th	
๒	e-Clinical Case Report		https://sys.dent.psu.ac.th/epatient	นางลัดดาวัลย์ วงค์ไชย นางสาวนวลนภา แซ่ลี้ นางสาวธนิษฐา อวิรุตม์	laddawan.w@psu.ac.th nuannapa.s@psu.ac.th thanittha.a@psu.ac.th	
		ระบบคลังรายงานผู้ป่วย	https://app.dent.psu.ac.th/patients/			
๓	Dentlab	ระบบประเมินการปฏิบัติงานห้อง Lab นักศึกษาชั้นปีที่ 3	http://10.151.127.78/lab_new	สาขาวิชา OPER ยังไม่ระบุ ADMIN		
๔	e-Unit	ระบบจอง Unit	http://ed.dent.psu.ac.th/dent_unit	นางราเจล วิทยวีรศักดิ์ หัวหน้าคลิกสาขา Pedo	rajel.n@psu.ac.th	
	e-Dent-Lab	ระบบประเมินการปฏิบัติงาน Lab ของสาขาวิชาทันตกรรมหัตถการ	http://10.151.127.78/lab_new/	นางสาววรวรรณ พฤษศรี	worrawan.p@psu.ac.th	
	e-Practical la	ระบบจองโต๊ะปฏิบัติการ ในห้อง Practical lab	http://10.151.127.78/ePracticallab/	นางณัฐธิดา หาญชนะ	natthidar.h@psu.ac.th	

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address	หมายเหตุ
๕		ระบบยื่นคำร้องเพื่อปรับปรุงข้อมูลการประเมิน	http://10.151.112.11/edit_clinic	นางลัดดาวัลย์ วงค์ไชย นางสาวนวลนภา แซ่ลี้ นางสาวธนิษฐา อวิรุตม์	laddawan.w@psu.ac.th nuannapa.s@psu.ac.th thanittha.a@psu.ac.th	
๖	Fingerscan	ระบบรายงานการลงปฏิบัติงานในคลินิกของนักศึกษา (ระบบดึงข้อมูล Fingerscan น.ศ.)	http://10.151.112.14:8080/timestamp	นางสาวธนิษฐา อวิรุตม์	thanittha.a@psu.ac.th	
๗	e-student	ระบบฐานข้อมูลนักศึกษาทันตแพทยศาสตร์ (ปริญญาตรี)	https://sys.dent.psu.ac.th/estudent/	นางวรรณรี ชาติดำ	wannaree.t@psu.ac.th	
๘	e-Clinic	ระบบคลินิกรวมนักศึกษา	http://10.151.127.78/clinic/	นางลัดดาวัลย์ วงค์ไชย นางสาวนวลนภา แซ่ลี้ นางสาวธนิษฐา อวิรุตม์ หัวหน้าคลินิก	laddawan.w@psu.ac.th nuannapa.s@psu.ac.th thanittha.a@psu.ac.th	กำลังพัฒนา

ภาคผนวก ซ

รายงานการวิเคราะห์และการประเมินความเสี่ยง ประจำปีงบประมาณ ๒๕๖๘

ภารกิจด้าน/งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ

รายงานการวิเคราะห์และการประเมินความเสี่ยง ประจำปีงบประมาณ ...2568.....

ประเภทเหตุการณ์ความเสี่ยง(10): **ด้านการดำเนินงาน(O)**

เหตุการณ์ความเสี่ยง --2	สาเหตุ --3	ตัวชี้วัดความเสี่ยง	กิจกรรมควบคุมที่มีอยู่ --5	ผลประเมินกิจกรรมการควบคุมที่มีอยู่	ระดับโอกาสเกิด	ระดับผลกระทบ	ด้านของผลกระทบ	ระดับความเสี่ยง	แผนบริหารจัดการความเสี่ยง --2	ผู้รับผิดชอบ	ช่วงเวลาดำเนินการและกำหนดเสร็จ
(11)	(12)	(13)	(14)	(15)	(16)	(17)		(18)	(19)	(20)	(21)
1. ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก	1.มาตรการป้องกันข้อมูลไม่รัดกุม	จำนวนครั้งของการถูกบุกรุกข้อมูล	ตรวจสอบเมื่อพบสิ่งผิดปกติบนเครื่องแม่ข่าย	สามารถพบและดำเนินการแก้ไขได้	2	5	ด้านประสิทธิภาพ/ประสิทธิผล	สูง	1.มีการอัพเดทแพทช์ระบบปฏิบัติการของเครื่องแม่ข่าย	งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ	ต.ค. 62 - ก.ย. 68
	2.มี Firewall	จำนวนครั้งที่โดนโจมตี	Service โดนโจมตี หรือ เจาะ หรือ ติด Malware						2. มีการติดตาม (monitor) log file ของเครื่องแม่ข่าย อย่างน้อยสัปดาห์ละ ๑ ครั้ง		
	3.ยังไม่มี WAF										
2. การดูแลอุปกรณ์ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	1.มีการเคลื่อนย้ายตำแหน่งคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	จำนวนครั้งของการย้ายตำแหน่ง	มีการตั้งค่าปิดกั้นเพื่อควบคุมไม่ให้มีการเชื่อมต่ออุปกรณ์ต่อพ่วง	สามารถพบและดำเนินการแก้ไขได้	4	4		สูงมาก	1. ควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม	งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ	ต.ค. 62 - ก.ย. 68
	2.การติดตั้งอุปกรณ์เครือข่ายโดยไม่ได้รับอนุญาต	จำนวนครั้งของการติดตั้ง		สามารถพบและดำเนินการแก้ไขได้	3	4		สูง	2. เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการและกำหนดค่าหมายเลขไอพีแอดเดรสบน DHCP Server		
	3.การดูแลเครื่องสำรองไฟสำหรับอุปกรณ์เครือข่ายหลัก	จำนวนครั้งของเครื่องสำรองไฟไม่ทำงาน		สามารถพบและดำเนินการแก้ไขได้	3	5		สูง	1.มีการทดสอบความพร้อมอุปกรณ์ ทุก 6 เดือน	งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ	ต.ค. 62 - ก.ย. 68
3.ข้อมูลเสียหาย	1. เกิดจากอุปกรณ์ชำรุด	จำนวนครั้งที่อุปกรณ์ที่เกี่ยวข้องชำรุด	จัดหาอุปกรณ์สำรอง	สามารถพบและดำเนินการแก้ไขได้	3	5		สูง	จัดหาอุปกรณ์สำรอง	งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ	ต.ค. 62 - ก.ย. 68
	2.เกิดจากการจัดการข้อมูลผิดพลาด	จำนวนครั้งที่บริหารจัดการผิดพลาด	1.จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศสำคัญและจำเป็นต้องมีระบบสำรอง		3	4			1. กำหนดความถี่การสำรองข้อมูล โดยมีการสำรองฐานข้อมูลระบบสารสนเทศตามประเภทการไหลเวียนของข้อมูลในระบบ		
			2. ข้อมูลสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก					สูง	2. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ		
			3. สำรองข้อมูลอัตโนมัติ ควบคู่ไปกับการสำรองข้อมูลโดยเจ้าหน้าที่ในบางระบบ						3. ทดสอบการกู้คืนข้อมูล		
4. ความปลอดภัยของห้องควบคุมระบบเครือข่ายสารเทศ	1. อัคคีภัย	จำนวนครั้งของการเกิดอัคคีภัย	1. มีกล้องวงจรปิดในห้องเครือข่ายหลัก 2. มีถังดับเพลิงหน้าห้องเครือข่ายหลัก		1	5		ปานกลาง	1. ติดตั้งกล้องวงจรปิดครอบคลุมทุกห้องควบคุมเครือข่าย	งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ	ก.พ. 64 - ก.ย. 68
									2. ติดตั้งถังดับเพลิงและสัญญาณแจ้งเตือนครอบคลุมทุกห้องระบบเครือข่าย	งานอาคารฯ	ก.พ. 64 - ก.ย. 68
	2.การเข้าห้องระบบเครือข่ายโดยไม่ได้รับอนุญาติ	จำนวนครั้งที่ไม่ได้รับอนุญาต	1. มีกล้องวงจรปิดในห้องเครือข่ายหลัก 2.มีการล็อกประตูห้องควบคุมระบบเครือข่าย	สามารถพบและดำเนินการแก้ไขได้	2	5		สูง	1.มีการล็อกห้องควบคุมระบบเครือข่าย 2.ติดตั้งอุปกรณ์เข้าถึง (Access Control)	งานนวัตกรรมดิจิทัลและศูนย์ข้อมูลสารสนเทศ	ก.พ. 64 - ก.ย. 68

ภารกิจด้าน/ความปลอดภัยของข้อมูล

แผนปฏิบัติงานและรายงานผลการบริหารความเสี่ยง ประจำปีงบประมาณ ...2568.....

ประเภทเหตุการณ์ความเสี่ยง(10): **ด้านการดำเนินงาน(O)**

เหตุการณ์ความเสี่ยง (11)	ตัวชี้วัดความเสี่ยง (12)	แผนบริหารจัดการความเสี่ยง (13)	แผน/ผล	ระยะเวลาดำเนินการตามแผนบริหารจัดการความเสี่ยง (14)												ระดับความเสี่ยงก่อนการบริหารจัดการความเสี่ยง (15)				ส่งผลกระทบต่อวัตถุประสงค์ (16)	ระดับความเสี่ยงหลังการบริหารจัดการความเสี่ยง (17)			ผลลัพธ์ที่ได้ (18)
				พ.ศ 2567			พ.ศ 2568									ระดับโอกาสเกิด	ระดับผลกระทบ	ด้านของผลกระทบ	ระดับความเสี่ยง		ระดับโอกาสเกิด	ระดับผลกระทบ	ระดับความเสี่ยง	
				ต.ค	พ.ย	ธ.ค	ม.ค	ก.พ	มี.ค	เม.ษ	พ.ค	มิ.ย	ก.ค	ส.ค	ก.ย									
1. ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก	จำนวนครั้งของการถูกบุกรุกข้อมูล	1.มีการอัพเดทแพทช์ระบบปฏิบัติการของเครื่องแม่ข่าย	แผน	↔						↔						2	5	ด้านประสิทธิภาพ/ประสิทธิผล	สูง	ระบบเครือข่ายและระบบสารสนเทศในคณะทันตแพทยศาสตร์	2	4	ปานกลาง	เครื่องแม่ข่ายมีความปลอดภัย
			ผล	↔																				
		2. มีการติดตาม (monitor) log file ของเครื่องแม่ข่าย อย่างน้อยสัปดาห์ละ ๑ ครั้ง	แผน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔									
			ผล	↔	↔	↔	↔	↔	↔	↔														
2. การดูแลอุปกรณ์ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	จำนวนครั้งของการย้ายตำแหน่ง	1. ควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม	แผน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	4	4		สูงมาก		3	4	สูง	สามารถควบคุมอุปกรณ์เครือข่ายได้
			ผล	↔	↔	↔	↔	↔	↔	↔														
		2. เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการ และกำหนดค่าหมายเลขไอพีแอดเดรสบน DHCP Server	แผน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔									
			ผล	↔	↔	↔	↔	↔	↔	↔														
	จำนวนครั้งของการติดตั้ง	1. ควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม	แผน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	3	4		สูง		2	4	ปานกลาง	
			ผล	↔	↔	↔	↔	↔	↔	↔														
		2. เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการ และกำหนดค่าหมายเลขไอพีแอดเดรสบน DHCP Server	แผน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔									
			ผล	↔	↔	↔	↔	↔	↔	↔														
	จำนวนครั้งของเครื่องสำรองไฟไม่ทำงาน	1.มีการทดสอบความพร้อมอุปกรณ์ ทุก 6 เดือน	แผน		↔						↔					3	5		สูง		2	4	ปานกลาง	
			ผล		↔																			
3.ข้อมูลเสียหาย	จำนวนครั้งที่อุปกรณ์ที่เกี่ยวข้องชำรุด	จัดหาอุปกรณ์สำรอง	แผน		↔	↔				↔	↔					3	5		สูง		2	4	ปานกลาง	มี Disk เสียหายในทั้ง 2 Server เก่า และ Server ใหม่อยู่ระหว่างจัดซื้อทดแทน โดยระหว่างรอ มีการย้ายไปทำงานบน NAS แบบ Raid 5
			ผล		↔	↔																		

ภารกิจด้าน/ความปลอดภัยของข้อมูล

แผนปฏิบัติงานและรายงานผลการบริหารความเสี่ยง ประจำปีงบประมาณ ...2568.....

ประเภทเหตุการณ์ความเสี่ยง(10): **ด้านการดำเนินงาน(O)**

เหตุการณ์ความเสี่ยง (11)	ตัวชี้วัดความเสี่ยง (12)	แผนบริหารจัดการความเสี่ยง (13)	แผน/ผล	ระยะเวลาดำเนินการตามแผนบริหารจัดการความเสี่ยง (14)												ระดับความเสี่ยงก่อนการบริหารจัดการความเสี่ยง (15)				ส่งผลกระทบต่อวัตถุประสงค์ (16)	ระดับความเสี่ยงหลังการบริหารจัดการความเสี่ยง (17)			ผลลัพธ์ที่ได้ (18)
				พ.ศ 2567			พ.ศ 2568									ระดับโอกาสเกิด	ระดับผลกระทบ	ด้านของผลกระทบ	ระดับความเสี่ยง		ระดับโอกาสเกิด	ระดับผลกระทบ	ระดับความเสี่ยง	
				ต.ค	พ.ย	ธ.ค	ม.ค	ก.พ	มี.ค	เม.ษ	พ.ค	มิ.ย	ก.ค	ส.ค	ก.ย									
	จำนวนครั้งที่บริหารจัดการผิดพลาด	1. กำหนดความถี่การสำรองข้อมูล โดยมีการสำรองฐานข้อมูลระบบสารสนเทศตามประเภทการไหลเวียนของข้อมูลในระบบ (ตามภาคผนวก ง) ในแนวปฏิบัติการจัดการด้านความปลอดภัยความเสี่ยงของระบบฐานข้อมูลและเครือข่ายเทคโนโลยีสารสนเทศ	แผน													3	4		สูง		2	4	ปานกลาง	มีข้อมูลสำรอง
			ผล																					
		2. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ	แผน																					
			ผล																					
		3. ทดสอบการกู้คืนข้อมูล	แผน																					
			ผล																					
4. ความปลอดภัยของห้องควบคุมระบบเครือข่ายสารเทศ	จำนวนครั้งของการเกิดอัคคีภัย	1. ติดตั้งกล้องวงจรปิดครอบคลุมทุกห้องควบคุมเครือข่าย	แผน													1	5		ปานกลาง		1	5	ปานกลาง	
			ผล																					
		2. ติดตั้งถังดับเพลิงและสัญญาณแจ้งเตือนครอบคลุมทุกห้องระบบเครือข่าย	แผน																					
			ผล																					
	จำนวนครั้งที่ไม่ได้รับอนุญาต	1. ติดตั้งอุปกรณ์เข้าถึง (Access Control)	แผน													2	5		สูง		1	5	ปานกลาง	
			ผล																					
		2.มีการล็อกประตูห้องควบคุมระบบเครือข่าย	แผน													2	5		สูง		1	4	ต่ำ	
			ผล																					

ประเมินความเสี่ยง

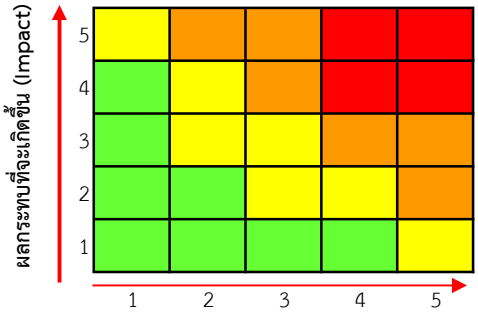
ระดับผลกระทบเหตุการณ์ที่เป็นความเสี่ยง

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	> 10 ล้านบาท หรือ เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูล	5
สูง	> 5 แสนบาท – 10 ล้านบาท หรือ เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน	4
ปานกลาง	> 2.5 แสนบาท – 5 แสนบาท หรือ ระบบมีปัญหาและมีความสูญเสียไม่มาก	3
น้อย	> 1 แสนบาท – 2.5 แสนบาท หรือ เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้	2
น้อยมาก	ไม่เกิน 100,000 บาท หรือ เกิดเหตุร้ายที่ไม่มีความสำคัญ	1

ระดับโอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง

โอกาสที่จะเกิดความเสี่ยง	ความถี่ที่เกิดขึ้น (เฉลี่ย)	ระดับคะแนน
สูงมาก	1 เดือนต่อครั้งหรือมากกว่า	5
สูง	1-6 เดือนต่อครั้งแต่ไม่เกิน 5 ครั้งต่อปี	4
ปานกลาง	6-12 เดือนต่อครั้ง	3
น้อย	2-3 ปี ต่อครั้ง	2
น้อยมาก	5 ปีต่อครั้ง	1

ระดับความเสี่ยง



ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ * ความรุนแรงของเหตุการณ์ต่างๆ แบ่งเป็น 4 ระดับดังนี้

- ระดับความเสี่ยงสูงมาก (Extreme) คะแนนระดับความเสี่ยง 16-25 คะแนน
- ระดับความเสี่ยงสูง (High) คะแนนระดับความเสี่ยง 10-15 คะแนน
- ระดับความเสี่ยงปานกลาง (Medium) คะแนนระดับความเสี่ยง 5-9 คะแนน
- ระดับความเสี่ยงต่ำ (Low) คะแนนระดับความเสี่ยง 1-4 คะแนน