

แนวปฏิบัติการจัดการด้านความปลอดภัย ความเสี่ยงของระบบฐานข้อมูล
และเครือข่ายเทคโนโลยีสารสนเทศ
คณะทันตแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์
ปี ๒๕๖๖

สารบัญ

ความเป็นมา.....	๑
๑. หลักการและเหตุผล.....	๑
๒. วัตถุประสงค์.....	๑
๓. เป้าหมาย.....	๑
๔. องค์ประกอบของแนวปฏิบัติ.....	๒
ส่วนที่ ๑ แนวปฏิบัติควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ.....	๓
วัตถุประสงค์.....	๓
ผู้รับผิดชอบ.....	๓
อ้างอิงมาตรฐาน.....	๓
แนวปฏิบัติ.....	๓
๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของคณะทันตแพทยศาสตร์.....	๓
๒. การบริหารจัดการบัญชีผู้ใช้และการเข้าถึงของผู้ใช้งาน.....	๖
๓. การควบคุมการเข้าถึงระบบเครือข่าย.....	๑๑
๔. การใช้งานอินเทอร์เน็ต.....	๑๓
๕. การบริหารจัดการคอมพิวเตอร์แม่ข่าย.....	๑๓
๖. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย.....	๑๔
๗. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ.....	๑๔
๘. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ.....	๑๕
๙. การตรวจสอบความถูกต้องของข้อมูล.....	๑๖
ส่วนที่ ๒ แนวปฏิบัติการบำรุงรักษาคอมพิวเตอร์และอุปกรณ์.....	๑๘
วัตถุประสงค์.....	๑๘
ผู้รับผิดชอบ.....	๑๘
อ้างอิงมาตรฐาน.....	๑๘
แนวปฏิบัติ.....	๑๘
ส่วนที่ ๓ แนวปฏิบัติการปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์.....	๒๐

วัตถุประสงค์	๒๐
ผู้รับผิดชอบ	๒๐
อ้างอิงมาตรฐาน	๒๐
แนวปฏิบัติ	๒๐
ส่วนที่ ๔ แนวปฏิบัติการจัดทำระบบสำรองสารสนเทศ	๒๑
วัตถุประสงค์	๒๑
ผู้รับผิดชอบ	๒๑
อ้างอิงมาตรฐาน	๒๑
แนวปฏิบัติ	๒๑
ส่วนที่ ๕ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงสารสนเทศ	๒๓
วัตถุประสงค์	๒๓
ผู้รับผิดชอบ	๒๓
อ้างอิงมาตรฐาน	๒๓
แนวปฏิบัติ	๒๓
ส่วนที่ ๖ แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	๒๔
วัตถุประสงค์	๒๔
ผู้รับผิดชอบ	๒๔
อ้างอิงมาตรฐาน	๒๔
แนวปฏิบัติ	๒๔
ส่วนที่ ๗ แนวปฏิบัติการแก้ไขปัญหาาระบบสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน	๒๕
วัตถุประสงค์	๒๕
ผู้รับผิดชอบ	๒๕
อ้างอิงมาตรฐาน	๒๕
แนวปฏิบัติ	๒๕
ส่วนที่ ๘ แนวปฏิบัติการจัดการข้อมูลในเครื่องคอมพิวเตอร์	๒๗
วัตถุประสงค์	๒๗

ผู้รับผิดชอบ	๒๗
อ้างอิงมาตรฐาน	๒๗
แนวปฏิบัติ	๒๗
ภาคผนวก	๒๙
ภาคผนวก ก ตารางรายละเอียดช่องทางการติดต่อหน่วยงานผู้ดูแลข้อมูลแต่ละประเภท	๓๐
ภาคผนวก ข แบบฟอร์มขอใช้งาน E-Request	๓๒
ภาคผนวก ค ตารางสมรรถนะพื้นฐานทางด้านคอมพิวเตอร์ให้เหมาะสมกับลักษณะการปฏิบัติงาน	๓๕
ภาคผนวก ง ตารางการสำรองข้อมูลและแผนปฏิบัติงานและตารางการบริหารความเสี่ยงระบบเครือข่าย เครื่องแม่ข่าย ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	๓๘
ภาคผนวก จ แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม ..	๔๒
ภาคผนวก ฉ บัญชีผู้ดูแลระบบ/ผู้ใช้งานระบบส่วนกลางมหาวิทยาลัย	๔๓
ภาคผนวก ช บัญชีผู้ดูแลระบบ/ผู้ใช้งานระบบสารสนเทศ คณะทันตแพทยศาสตร์ (คณะฯ พัฒนาระบบเอง) ..	๕๒
ภาคผนวก ซ รายงานการวิเคราะห์และการประเมินความเสี่ยง ประจำปีงบประมาณ ๒๕๖๕	๕๙

ความเป็นมา

๑. หลักการและเหตุผล

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

๒. วัตถุประสงค์

งานเทคโนโลยีสารสนเทศ คณะทันตแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ กำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยมีวัตถุประสงค์ ดังต่อไปนี้

- ๒.๑. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ
- ๒.๒. เพื่อให้เกิดความเชื่อมั่นด้านความปลอดภัย การใช้งานระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพและประสิทธิผล
- ๒.๓. เพื่อเผยแพร่แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ทุกระดับ นักศึกษา - และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร มีความรู้ ความเข้าใจและถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด
- ๒.๔. เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของงานเทคโนโลยีสารสนเทศมีรายละเอียดดังต่อไปนี้

- ๓.๑. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของคณะทันตแพทยศาสตร์
- ๓.๒. เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ
- ๓.๓. เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับที่เกี่ยวข้อง
- ๓.๔. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๔. องค์ประกอบของแนวปฏิบัติ

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ งานเทคโนโลยีสารสนเทศ 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 แนวปฏิบัติการบำรุงการรักษาคอมพิวเตอร์และอุปกรณ์

ส่วนที่ ๓ แนวปฏิบัติการปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์

ส่วนที่ ๔ แนวปฏิบัติการจัดทำระบบสำรองสารสนเทศ

ส่วนที่ ๕ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

ส่วนที่ ๖ แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๗ แนวปฏิบัติการแก้ไขปัญหาหาระบบสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน

ส่วนที่ ๑

แนวปฏิบัติควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศ

วัตถุประสงค์

- เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศของคณะ
- เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจและปฏิบัติตามขั้นตอนโดยเคร่งครัด

ผู้รับผิดชอบ

- งานเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบที่ได้รับมอบหมาย
- เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕
- สำนักงานนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

- การควบคุมการเข้าถึงข้อมูลและสารสนเทศของคณะทันตแพทยศาสตร์
 - จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน
 - จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน
 - กำหนดสิทธิ์การเข้าถึงข้อมูลและสารสนเทศของคณะ ดังนี้
 - ไม่มีสิทธิ์
 - อ่านได้อย่างเดียว
 - สร้างข้อมูล
 - ป้อนข้อมูล
 - แก้ไขข้อมูล
 - ลบข้อมูล
 - อนุมัติการใช้ข้อมูล
 - กำหนดประเภทข้อมูลของคณะ
 - ข้อมูลนักศึกษา
 - ข้อมูลบุคลากร
 - ข้อมูลการเงินและบัญชี
 - ข้อมูลการศึกษา
 - ข้อมูลการบริหาร
 - ข้อมูลผู้ป่วย

๑.๔. เกณฑ์ในการกำหนดระดับชั้นความลับของข้อมูลและสารสนเทศของคณะ

- ๑.๔.๑. ลับ รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง
- ๑.๔.๒. ใช้ภายในเท่านั้น เป็นข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างภายในหน่วยงาน หรือ ข้อมูลเผยแพร่เฉพาะภายในเท่านั้น
- ๑.๔.๓. ส่วนบุคคล ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลนั้น
- ๑.๔.๔. เปิดเผยได้ เป็นข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกคณะ

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 หน่วยทะเบียนและประเมินผลการศึกษา และหน่วยกิจการนักศึกษา
- ๑.๗.๒. ข้อมูลบุคลากร หน่วยงานหลักคือ หน่วยบริหารทรัพยากรบุคคล
- ๑.๗.๓. ข้อมูลการเงินและบัญชี หน่วยงานหลักคือ งานคลังและพัสดุ และหน่วยเงินรายได้ดูแลในส่วนการเงินรายได้ที่เกิดจากโรงพยาบาลทันตกรรม
- ๑.๗.๔. ข้อมูลการศึกษา หน่วยงานหลักคือ ระดับปริญญาตรี หน่วยทะเบียนและประเมินผลการศึกษา และสาขาวิชา ระดับหลังปริญญา หน่วยบัณฑิตศึกษา
- ๑.๗.๕. ข้อมูลทางการบริหาร หน่วยงานหลัก คือ
 - (๑) งานบริหารทรัพยากรบุคคล นโยบายและแผน ดูแลข้อมูลการบริหารจัดการนโยบาย งบประมาณ และอัตรากำลัง
 - (๒) หน่วยส่งเสริมและพัฒนางานวิจัย ดูแลฐานข้อมูลวิจัย

- (๓) สำนักงานจริยธรรมดูแลโครงการวิจัยที่ดำเนินการเกี่ยวข้องกับมนุษย์
- (๔) งานคลังและพัสดุ ดูแลในส่วนของการจัดการงบประมาณทั้งหมดภายในคณะ
- (๕) งานอาคาร วิศวกรรมและซ่อมบำรุง ดูแลในส่วนระบบกล้องวงจรปิด รักษาความปลอดภัยในส่วนภาพรวมของคณะ

๑.๗.๖. 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. จัดเก็บซอร์สโค้ดและไลบรารีของระบบสารสนเทศทั้งเวอร์ชันปัจจุบันและ เวอร์ชันเก่าไว้ในสถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็น

๑.๙. การกำหนดการใช้งานตามภารกิจ

๑.๙.๑. การควบคุมการเข้าถึงระบบสารสนเทศ

- (๑) นักศึกษา จะให้สิทธิ์เมื่อหน่วยทะเบียนและประเมินผลการศึกษา และหน่วยบัณฑิตศึกษาได้ทำหนังสือแจ้งมาทางงานเทคโนโลยีสารสนเทศ 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 โดยผู้ดูแลระบบร้องขอรายชื่อที่ลาออกหรือมีการเปลี่ยนแปลงไปยังหน่วยงานที่เกี่ยวข้อง
- 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 รวมทั้งกรณีการส่งมอบระบบที่งานเทคโนโลยีสารสนเทศได้พัฒนาขึ้น
- (๒) ระบบสารสนเทศและข้อมูลสารสนเทศทางการเรียนการสอน การประเมินผล การศึกษา และระบบฐานข้อมูลผู้ป่วย โดยหลังจากอบรมจะมีการวัดผลประเมินผลการเข้าร่วมอบรม ด้วยข้อสอบที่งานเทคโนโลยีสารสนเทศจัดทำขึ้น มีการรายงานผลการสอบไปยังหน่วยงานต้นสังกัด ในกรณีนักศึกษา จะรายงานผลไปยังหน่วยทะเบียนและประเมินผลการศึกษา หรือหน่วยบัณฑิตศึกษา และมีการทวนอบรมซ้ำทุกปี เพื่อผู้ใช้งานทราบถึงนโยบายและขั้นตอนการบันทึกข้อมูลทางสารสนเทศที่เป็นปัจจุบัน

๒.๑.๒. การจัดทำคู่มือการใช้งานระบบ เพื่อให้ผู้ใช้งานสามารถทวนศีกษาวิธีการใช้งานระบบได้ด้วยตนเอง

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 และผู้ใช้งานจะต้องลงชื่อเข้าใช้ระบบใหม่ หากเปิดระบบค้างไว้เกิน ๑๘๐ นาที โดยมีขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยดังนี้

(๑) รูปแบบของรหัสผ่านจะต้องมีอย่างน้อย ๔ หลัก ประกอบด้วย

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

(๒) ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราว โดยการกำหนดรหัสผ่านให้มีความยากต่อการคาดเดาและกำหนดให้แตกต่างกัน ซึ่งรูปแบบของรหัสผ่านชั่วคราวประกอบด้วย รหัสตัวอักษรที่ตั้งขึ้นโดยแบ่งตามกลุ่มผู้ใช้งาน และรหัสบัตรประชาชน ๔ หลักสุดท้ายของผู้ใช้งาน

(๓) ผู้ดูแลระบบจัดส่งรหัสผ่านให้ผู้ใช้งานโดยตรง โดยกำหนดให้ผู้ใช้งานกรอกแบบฟอร์มขอรหัสผู้ใช้งาน พร้อมรายละเอียดข้อมูลส่วนบุคคล และจัดส่งให้ผู้ใช้งานโดยตรงทางอีเมลที่ระบุมาในแบบฟอร์ม

(๔) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากได้รับรหัสผ่านชั่วคราว ซึ่งผู้ดูแลระบบจัดทำแบบฟอร์มแจ้งรหัสผู้ใช้ และวิธีการเปลี่ยนรหัสผ่านให้แก่ผู้ใช้งานผ่านทางอีเมล (ระบบไม่มีให้ตั้งค่าเปลี่ยนรหัสทันที จึงทำเป็นข้อบังคับผ่านแบบฟอร์มแจ้งรหัสผู้ใช้แทน)

(๕) กรณีผู้ใช้ลืมรหัสผ่าน ต้องดำเนินการกรอกฟอร์ม E-request เพื่อให้งานเทคโนโลยีสารสนเทศตั้งรหัสผ่านให้ใหม่

๒.๔. การบริหารจัดการการเข้าถึงข้อมูลผู้ป่วย

๒.๔.๑. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลผู้ป่วยภายในระบบตามบทบาทหน้าที่ของผู้ใช้งาน

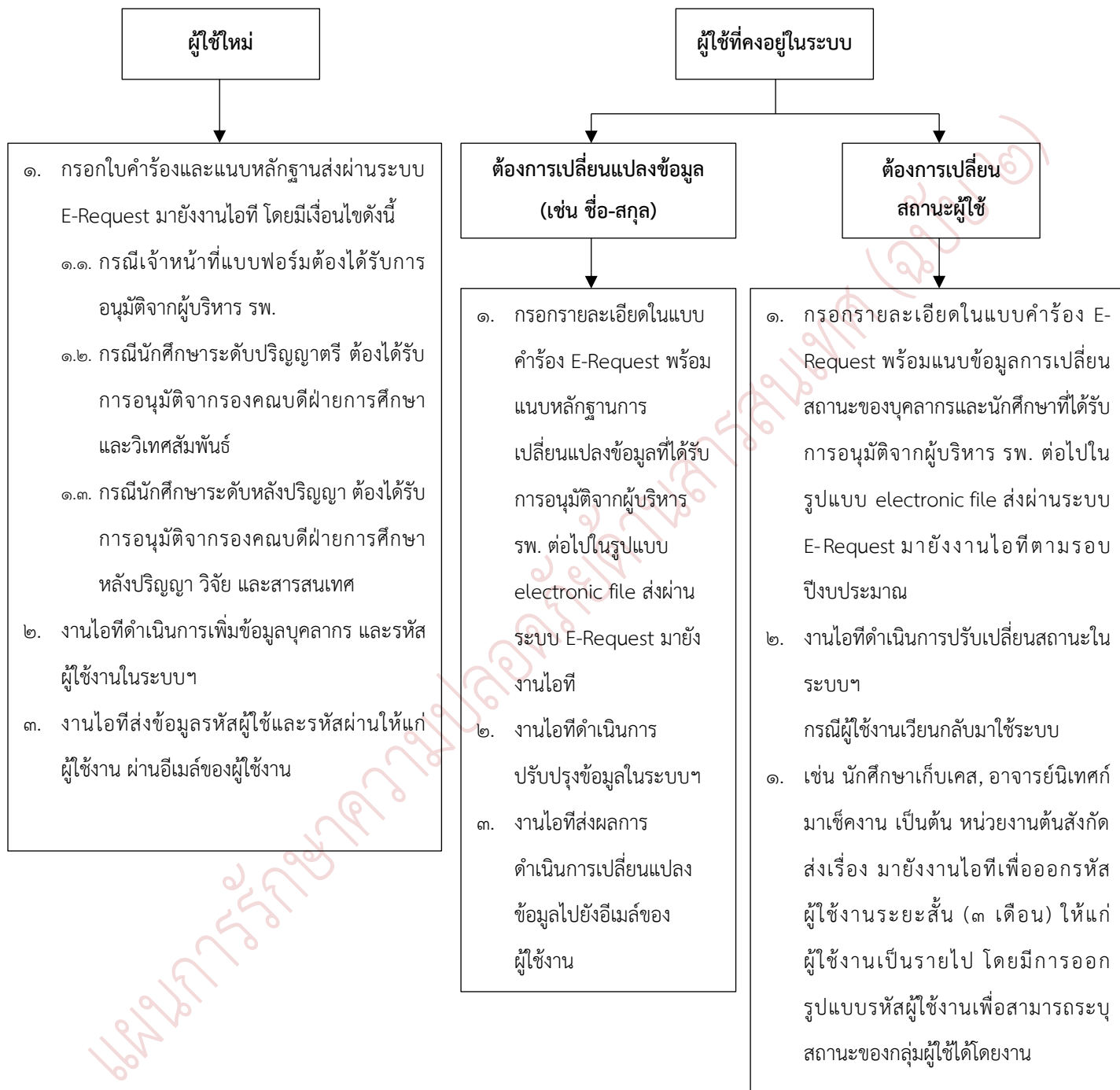
๒.๔.๒. ผู้ดูแลระบบต้องกำหนดแนวทางการส่งออก ข้อมูลผู้ป่วยภายในระบบตามบทบาทหน้าที่ของผู้ใช้งาน

การส่งออกข้อมูลมีหลายวัตถุประสงค์ ดังนี้

- (๑) การขอข้อมูลเพื่อรายงานและ/หรือ ช่วยในการตัดสินใจของผู้บริหาร ผู้ขอข้อมูลกรอกฟอร์มผ่านระบบ E-Request
 - (๒) การขอข้อมูลเพื่อการวิจัย
 - (๓) การขอข้อมูลเพื่อประกอบการเรียนการสอน
- ทั้งนี้ ได้มีการกำหนดแนวปฏิบัติในข้อ (๒) และ (๓) ดังแผนภาพด้านล่างนี้

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

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. บันทึกรายชื่อขอขออนุญาตดำเนินการวิจัย ซึ่งได้รับการเห็นชอบจากรองคมนตรีฝ่ายโรงพยาบาล / รองคณบดีฝ่ายการศึกษาและวิเทศสัมพันธ์
๖. แบบบันทึกข้อมูลสำหรับการวิจัย หรือแบบฟอร์มข้อมูลสถิติทางการแพทย์ (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 : รายละเอียดค่าบริการของสำนักนวัตกรรมการดิจิทัลและระบบอัจฉริยะ (ศูนย์คอมฯ) แนบท้ายประกาศสำนักนวัตกรรมการดิจิทัลและระบบอัจฉริยะ (ศูนย์คอมฯ) ฉบับลงวันที่ ๓๓ 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

ข้อมูลที่จัดเตรียมจะสามารถเข้าถึงได้โดยผ่านระบบอินเทอร์เน็ต 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
- ๓.๒.๒. ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้
 - (๑) ลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นำมาใช้ในระบบเครือข่ายไร้สาย
 - (๒) ควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณเพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
 - (๓) ทำการเปลี่ยนค่า SSID เป็นตามมหาวิทยาลัย
 - (๔) เปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตี ไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้ง่าย
 - (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. ในจุดที่มีหำมนำอุปกรณ์อื่นมาต่อพ่วงเพิ่ม 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 ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่าย ภายในและอุปกรณ์ต่าง 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 ซึ่งสอดคล้องกับแนวปฏิบัติควบคุมการเข้าถึงและการทำงานของบริการเครือข่ายของหน่วยงาน

๓.๖. การควบคุมการเชื่อมต่อทางเครือข่าย

- ๓.๖.๑. อนุญาตการเชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น
- ๓.๖.๒. ในกรณีที่ผู้ดูแลระบบตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติต่อระบบเครือข่ายหลัก จะทำการหยุดให้บริการโดยการตัดการเชื่อมต่อกับระบบเครือข่าย โดยไม่มีการแจ้งให้ทราบล่วงหน้า จนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

๓.๗. การควบคุมการจัดเส้นทางบนเครือข่าย

- ๓.๗.๑. อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด
- ๓.๗.๒. ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการทำงานของบริการเครือข่าย

- ๓.๗.๓. ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการ ติดตั้ง เครือข่ายแบบไร้สายด้วย (Wireless Network) การติดตั้งและการเชื่อมต่ออุปกรณ์ เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่คอมพิวเตอร์ หรือผู้ที่ได้รับมอบหมายจากผู้ดูแล ระบบ เท่านั้น

๔. การใช้งานอินเทอร์เน็ต

- ๔.๑. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้ตามสิทธิ์ที่ได้รับ
- ๔.๒. ห้ามใช้อินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล
- ๔.๓. ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัย ต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย เป็นต้น
- ๔.๔. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลด การปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
- ๔.๕. ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน และ ระบบของมหาวิทยาลัยมีการจัดสรร Bandwidth Management ให้จำกัด เพื่อไม่ให้กระทบกับการ ใช้งานของผู้อื่น
- ๔.๖. ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ
- ๔.๗. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต
- ๔.๘. หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ที่ใช้งาน และออกจากการ เครือข่ายอินเทอร์เน็ตด้วยการ Logout จากการ Authentication เพื่อป้องกันการเข้าใช้งานโดย บุคคลอื่น ๆ
- ๔.๙. มีการเก็บ Traffic Log โดยมหาวิทยาลัย

๕. การบริหารจัดการคอมพิวเตอร์แม่ข่าย

- ๕.๑. กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง
- ๕.๒. มีขั้นตอน/กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย
- ๕.๓. ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ ตรงกับเวลาอ้างอิงมาตรฐาน (time.psu.ac.th) ที่มหาวิทยาลัยใช้อ้างอิง
- ๕.๔. เปิดให้บริการเท่าที่จำเป็นเท่านั้น โดยต้องมีมาตรการป้องกันเพิ่มเติมสำหรับบริการที่มีความเสี่ยงต่อ ระบบรักษาความปลอดภัยด้วย
- ๕.๕. ปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่ออุดช่องโหว่ต่าง ๆ

- ๕.๖. ทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา
- 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 หักถถการ การออกไปเสร็จ การยกเลิกใบเสร็จ เป็นต้น
 - ๗.๓.๕. แสดงการใช้สิทธิ์ เช่น สิทธิ์ของผู้ดูแลระบบ
 - ๗.๓.๖. หมายเลขไอพีแอดเดรสที่เข้าถึง
- ๗.๔. การควบคุมผู้รับเหมาช่วง (outsourcer) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และ พัฒนาระบบสารสนเทศ
 - ๗.๔.๑. มีกระบวนการคัดเลือกผู้รับเหมาช่วงโดยเฉพาะ และต้องกำหนดคุณสมบัติของผู้รับเหมาช่วงที่ชัดเจน เช่น ต้องมีประสบการณ์ มีลูกค้าอ้างอิงน่าเชื่อถือ หรือมีใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยี ของการรับเหมาช่วงทั้งในส่วนของ ฮาร์ดแวร์และซอฟต์แวร์รวมถึงระบบสนับสนุน 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. ผู้ดูแลระบบเครือข่าย 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

๘.๔. ผู้ดูแลระบบสารสนเทศ และผู้ดูแลเว็บไซต์มีหน้าที่และความรับผิดชอบในแต่ละระบบดังนี้

- ๘.๔.๑. ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

- ๘.๔.๒. ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศ
นั้นให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ
- ๘.๔.๓. การดึงรายงานเพื่อพัฒนางานหรือเพื่อประกอบการตัดสินใจการบริหารองค์กร สามารถ
ดึงผ่านระบบสารสนเทศ โดยหน่วยงานที่รับผิดชอบข้อมูล หากรายงานที่ต้องการไม่อยู่
ในรายการที่ระบุไว้ ให้เขียนคำร้องมายังงานเทคโนโลยีสารสนเทศโดยผ่านความคิดเห็น
ของผู้บังคับบัญชาต้นสังกัด แสดงในภาคผนวก ข
- ๘.๔.๔. ผู้ดูแลเว็บไซต์ดูแลเนื้อหา ปรับปรุงเนื้อหาให้ถูกต้องและปัจจุบันเสมอ

๘.๕. หลักธรรมาภิบาลของผู้ดูแลระบบ

- ๘.๕.๑. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานโดยไม่มีเหตุผลอันสมควร
- ๘.๕.๒. ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือ
มีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร
- ๘.๕.๓. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้
บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๙. การตรวจสอบความถูกต้องของข้อมูล

มีแนวทางในการตรวจสอบความถูกต้องของระบบสารสนเทศ ดังนี้

- ๙.๑. ระบบสารสนเทศสนับสนุนงานสำนักงานเลขานุการ
 - ๙.๑.๑ ข้อมูลพื้นฐานของบุคลากร และนักศึกษา มีการเชื่อมโยงกับระบบฐานข้อมูลสารสนเทศ
ด้านบุคลากรและระบบฐานข้อมูลนักศึกษาซึ่งมีความถูกต้องตามมหาวิทยาลัย
 - ๙.๑.๒ มอบหมายให้หน่วยงานที่รับผิดชอบข้อมูลสารสนเทศ เป็นผู้ดูแลข้อมูลในการบันทึก
แก้ไขข้อมูลให้มีความถูกต้อง ครบถ้วน ทันสมัย และแม่นยำ หากพบว่าข้อมูล
คลาดเคลื่อน ไม่ถูกต้อง และไม่ทันสมัย สามารถแจ้งเจ้าหน้าที่ที่เป็นเจ้าของข้อมูลเพื่อ
ปรับปรุงแก้ไข
- ๙.๒. ระบบสารสนเทศงานโรงพยาบาล
 - ๙.๒.๑ กำหนดข้อมูลพื้นฐาน เป็นตัวเลือกให้แก่ผู้ใช้ เพื่อลดข้อผิดพลาดจากการกรอกข้อมูลของ
ผู้ใช้งาน
 - ๙.๒.๒ ใช้เมนูสำหรับผู้ดูแลระบบ เพื่อกำหนดให้ระบบตรวจสอบและแสดงข้อความแจ้งเตือน
ก่อนผู้ใช้จะทำการบันทึกข้อมูลเข้าสู่ระบบ ในกรณีที่ผู้ใช้กรอกข้อมูลไม่ครบถ้วน หรือ
กรอกข้อมูลที่ผิดปกติ
 - ๙.๒.๓ ผู้ดูแลระบบจัดทำรายงานทางสถิติ เพื่อให้ตัวแทนเจ้าหน้าที่ประจำหน่วยงาน ตรวจสอบ
ความถูกต้องของข้อมูล โดยแบ่งเป็น รายงานรายคาบ รายวัน รายเดือน รายไตรมาส
รายปี และรายปีงบประมาณ
- ๙.๓. สารสนเทศงานการเรียนการสอน
 - ๙.๓.๑ มีระบบสารสนเทศตรวจสอบคะแนนสำหรับนักศึกษาทันตแพทย์ เพื่อตรวจสอบความ
ถูกต้องของคะแนนกับอาจารย์แต่ละสาขา

- 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

แนวปฏิบัติการบำรุงรักษาคอมพิวเตอร์และอุปกรณ์

วัตถุประสงค์

- เพื่อควบคุมดูแล และบำรุงรักษาให้ทรัพยากรสารสนเทศของคณะทันตแพทยศาสตร์มีสภาพพร้อมใช้งานอยู่เสมอ รวมถึงการแก้ไข ปรับปรุง เพื่อให้การใช้งานทรัพยากรสารสนเทศเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล
- ลดการติดขัดในการทำงาน สามารถทำงานได้อย่างต่อเนื่อง
- เพื่อบันทึก รวบรวมข้อมูลเกี่ยวกับอุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง
- เพื่อเป็นการป้องกันภัยคุกคามทางคอมพิวเตอร์และทางอินเทอร์เน็ต

ผู้รับผิดชอบ

- งานเทคโนโลยีสารสนเทศ
- ผู้ดูแลทรัพยากรสารสนเทศ
- เจ้าหน้าที่ของหน่วยงานที่ใช้งานทรัพยากรสารสนเทศ

อ้างอิงมาตรฐาน

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

แนวปฏิบัติ

๑. ถ่ายทอดความรู้และแนะนำการใช้งาน

- ๑.๑. สมรรถนะพื้นฐานทางด้านคอมพิวเตอร์ให้เหมาะสมกับลักษณะการปฏิบัติงานแสดงในภาคผนวก ค
- ๑.๒. การแก้ไขปัญหาเบื้องต้นในใช้งานทรัพยากรสารสนเทศของแต่ละหน่วยงาน
- ๑.๓. การใช้งานคอมพิวเตอร์และอุปกรณ์ Mobile
- ๑.๔. การติดตั้ง Software และการใช้งานระบบ
- ๑.๕. การเชื่อมต่อใช้งานอินเทอร์เน็ต

๒. ดำเนินการตรวจสอบ

- ๒.๑. อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงที่อยู่ในระยะเวลารับประกัน หากเกิดปัญหา เสียหายหรือชำรุด ทางเจ้าหน้าที่ผู้ดูแลทรัพยากรสารสนเทศจะทำการตรวจเช็คพร้อมทั้งดำเนินการส่งเคลมและติดตามงานกับทางบริษัท
- ๒.๒. อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงที่หมดประกันหากเกิดปัญหา เสียหายหรือชำรุด ทางเจ้าหน้าที่ผู้ดูแลทรัพยากรสารสนเทศจะทำการตรวจเช็คแก้ไขปัญหาก่อนส่งซ่อม และมีอุปกรณ์สำรองให้ใช้งานในขณะดำเนินการส่งซ่อม
- ๒.๓. ในการตรวจสอบคอมพิวเตอร์ในทุกกรณี ทางเจ้าหน้าที่ผู้ดำเนินการตรวจสอบจะไม่เข้าถึง แก้ไข เปลี่ยนแปลง หรือคัดลอกข้อมูลส่วนบุคคลของผู้ใช้งาน และไม่เข้าถึงระบบต่างๆ ที่ผู้ใช้งานมีสิทธิ์

ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน เว้นแต่ผู้ใช้งานมีความประสงค์และยินยอม ในกรณีที่ต้องย้ายข้อมูลในกรณีที่อุปกรณ์จัดเก็บข้อมูลเกิดการชำรุดเสียหาย โดยทางเจ้าหน้าที่ผู้ตรวจซ่อมจะปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ อย่างเคร่งครัด

๓. การบำรุงรักษา

- ๓.๑. ตรวจสอบเช็คอุปกรณ์คอมพิวเตอร์ เครื่องสำรองไฟ (UPS) ของแต่ละหน่วยงานให้มีสภาพใช้งานได้ปีละ ๒ ครั้ง (เดือนพฤษภาคม และเดือนพฤศจิกายนของทุกปี)
- ๓.๒. Update Software Web Browser และ Antivirus ให้เป็นปัจจุบัน เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางอินเทอร์เน็ต
- ๓.๓. ปรับเปลี่ยนระบบปฏิบัติการให้มีความเหมาะสม (Upgrade Version) และปรับปรุงช่องโหว่ของระบบปฏิบัติการ (Patch Windows) กรณีที่ผู้ใช้งานมีความต้องการปรับเปลี่ยน ผู้ใช้ต้องทำการ Backup ข้อมูลในเครื่องคอมพิวเตอร์ไว้
- ๓.๔. การเข้าถึงคอมพิวเตอร์ของผู้ใช้งานจะมีทำการแจ้งผู้ใช้งานก่อนดำเนินการเพื่อทราบทางเจ้าหน้าที่ผู้ดำเนินการจะไม่เข้าถึง แก้ไข เปลี่ยนแปลง หรือคัดลอกข้อมูลส่วนบุคคลของผู้ใช้งาน และไม่เข้าถึงระบบต่างๆ ที่ผู้ใช้งานมีสิทธิ์ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน จะดำเนินการในส่วนขั้นตอนการบำรุงรักษาอุปกรณ์คอมพิวเตอร์เท่านั้น โดยทางเจ้าหน้าที่ผู้ตรวจซ่อมจะปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ อย่างเคร่งครัด

ส่วนที่ ๓

แนวปฏิบัติการปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์

วัตถุประสงค์

1. เพื่อให้การปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์เป็นไปด้วยความเรียบร้อย
2. เพื่อให้มีความเข้าใจตรงกันในกระบวนการการปรับปรุงสิ่งก่อสร้าง
3. เพื่อลดความเสียหายจากการปรับปรุงสิ่งก่อสร้าง

ผู้รับผิดชอบ

1. งานเทคโนโลยีสารสนเทศ
2. ผู้ดูแลระบบที่ได้รับมอบหมาย
3. เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

1. มาตรฐานระบบเครือข่าย ที่กำหนดโดย IEEE

แนวปฏิบัติ

1. กรอกฟอร์มขอใช้บริการจากระบบ E-request
2. นัดหรือพูดคุยเกี่ยวกับการปรับปรุงสิ่งก่อสร้างที่เกี่ยวข้องกับระบบเครือข่าย เช่น สาย LAN, อุปกรณ์กระจายสัญญาณไร้สาย, เครื่องคอมพิวเตอร์ และเครื่องพิมพ์
3. เจ้าหน้าที่เทคโนโลยีสารสนเทศเข้าไปสำรวจจุดเครือข่าย (Outlet) เดิม และอุปกรณ์ระบบเครือข่าย
4. จุดเครือข่ายเดิม (Outlet) ให้ย้ายเก็บไว้ สำหรับนำมาใช้ได้อีก เพื่อประหยัดงบประมาณในการติดตั้งใหม่
5. แนวทางการติดตั้งและการเพิ่มเติมอุปกรณ์เครือข่ายต้องเป็นไปตาม TOR ที่เจ้าหน้าที่เทคโนโลยีสารสนเทศกำหนด

ส่วนที่ ๔

แนวปฏิบัติการจัดทำระบบสำรองสารสนเทศ

วัตถุประสงค์

- เพื่อให้ระบบสารสนเทศของคณะมีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง
- เพื่อกำหนดแนวปฏิบัติการทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบสารสนเทศระบบงานสำนักงานเลขานุการระบบงานโรงพยาบาล และระบบสารสนเทศงานการเรียนการสอนถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีข้อมูลที่สำรองและสามารถกู้คืนข้อมูลได้ในเวลาที่กำหนด

ผู้รับผิดชอบ

- งานเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบที่ได้รับมอบหมาย
- เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕
- สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

๑. ระบบสำรอง

- ๑.๑. จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศสำคัญและจำเป็นต้องมีระบบสำรอง แสดงดังภาคผนวก ก
- ๑.๒. ข้อมูลสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม
- ๑.๓. มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๒. การสำรองข้อมูล

- ๒.๑. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของระบบสารสนเทศ
- ๒.๒. กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ โดยวิธีการเขียนสคริปต์การสำรองข้อมูลอัตโนมัติ ควบคุมไปกับการสำรองข้อมูลโดยเจ้าหน้าที่ในบางระบบ
- 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 ติ๊กถล่ม สามารถนำข้อมูลที่เก็บไว้อีกที่มาใช้ได้ โดยได้สำรองไว้ย้อนหลัง ๑ - ๓ เดือน โดยเก็บแยกออกจากเครื่องคอมพิวเตอร์แม่ข่ายระบบใช้งานจริง

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

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

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

ส่วนที่ ๕

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายได้รับทราบถึงหน้าที่ ความรับผิดชอบ และความจำเป็นในการประเมินความเสี่ยงสารสนเทศ เพื่อหาแนวทางป้องกันภัยคุกคามและการโจมตีต่าง ๆ

ผู้รับผิดชอบ

- งานเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบที่ได้รับมอบหมาย
- เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕
- สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

- ต้องมีการตรวจสอบและป้องกันความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ
- ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อประเมินความเสี่ยงนั้น
 - ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต
 - มีการอัปเดตแพทช์ระบบปฏิบัติการของเครื่องแม่ข่าย
 - มีการเปลี่ยนพาสเวิร์ดของเครื่องแม่ข่ายอย่างน้อยปีละ ๒ ครั้ง
 - มีการติดตาม (monitor) log file ของเครื่องแม่ข่าย อย่างน้อยสัปดาห์ละ ๑ ครั้ง
 - ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สาย
 - มีการใช้งาน PSU Passport เพื่อป้องกันบุคคลภายนอก
 - มีการตั้งค่าอุปกรณ์เครือข่ายที่ปลอดภัยตามมาตรฐานความปลอดภัยของเครือข่าย WPA2
 - ความเสี่ยงที่เกิดจากการลงบันทึกเข้าสารสนเทศที่สำคัญผ่านระบบเครือข่าย
 - ตั้งค่าไม่ให้บันทึกที่รหัสผ่านบนเบราว์เซอร์เพื่อป้องกันไม่ให้บุคคลอื่นเข้าถึงสิทธิ์การใช้งานของผู้ใช้เฉพาะคอมพิวเตอร์บริการส่วนกลาง (เครื่องคอมพิวเตอร์ประจำศูนย์นิทรรศการ ห้องปฏิบัติการคอมพิวเตอร์ และหน่วยส่งเสริมและพัฒนาการศึกษาด้วยตนเอง)
- ทำรายงานการวิเคราะห์และประเมินความเสี่ยงประจำปีตามภาคผนวก ข

ส่วนที่ ๖

แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อเผยแพร่แนวปฏิบัติให้กับผู้บริหาร บุคลากรและผู้เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

- งานเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบที่ได้รับมอบหมาย
- เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕
- สำนักงานนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

- อบรมผู้ใช้งานและเจ้าหน้าที่ผู้เกี่ยวข้อง ให้มีความรู้ความเข้าใจ เกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานสารสนเทศโดยไม่ระมัดระวัง
- อบรมการใช้งานสารสนเทศให้กับหน่วยงานอย่างสม่ำเสมอ
- จัดทำคู่มือการใช้งานระบบสารสนเทศ

ส่วนที่ ๗

แนวปฏิบัติการแก้ไขปัญหาาระบบสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน

วัตถุประสงค์

- เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของคณะทันตแพทยศาสตร์
- เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและปฏิบัติในการดูแลรักษาระบบความปลอดภัยของระบบสารสนเทศของคณะทันตแพทยศาสตร์
- เพื่อให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และสามารถตอบสนองสถานการณ์ได้อย่างทันท่วงที

ผู้รับผิดชอบ

- งานเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบสารสนเทศ เจ้าหน้าที่ระบบเครือข่ายที่ได้รับมอบหมาย
- เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕
- สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ

แนวปฏิบัติ

- ติดต่อหน่วยบริหารและประสานงาน โทร. ๗๕๔๐
- ระบบเครือข่ายขัดข้อง ติดต่อหน่วยพัฒนาระบบเครือข่ายสารสนเทศ โทร. ๗๗๕๘
- ระบบสารสนเทศขัดข้องติดต่อหน่วยพัฒนาระบบสารสนเทศและฐานข้อมูล

ระบบงาน	ติดต่อ
สนับสนุนสำนักงานและวิจัยนวัตกรรม (Smart Administration/ Smart research and innovation)	๗๖๘๔
	๗๕๔๑
	๗๕๐๕
ระบบสารสนเทศโรงพยาบาล (Smart dental hospital)	๗๕๔๑
ระบบสารสนเทศสนับสนุนการเรียนการสอน (Smart dental education)	๗๕๐๕

- เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงขัดข้อง ติดต่อ ส่วนบริการซ่อมบำรุงทรัพยากรสารสนเทศ โทร. ๗๗๕๘

ทั้งนี้ช่องทางการติดต่อแต่ละหน่วยข้างต้น สามารถติดต่อผ่านทางระบบตอบข้อความอัตโนมัติของเว็บเพจ เฟสบุ๊ก งานเทคโนโลยีสารสนเทศ : <https://www.facebook.com/dentitpsu/> ซึ่งระบบจะแนะนำการแก้ไขปัญหาเบื้องต้น ส่วนปัญหาอื่น ๆ จะดำเนินการแก้ไขปัญหาภายในวันทำการถัดไป

การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน จัดเตรียมทีมงาน และมอบหน้าที่ความรับผิดชอบ ทีมงานแผนดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan Team)

แผนกู้คืนกลับสู่สภาพปกติ

1. แผนการกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery)
2. แผนกู้คืนเครื่องสำรองไฟสำหรับ Data Center ชัดช่อง
3. แผนกู้คืนระบบสารสนเทศ
 - แผนการกู้คืนระบบสารสนเทศโรงพยาบาล (HOSxPXE)
 - แผนการกู้คืนเว็บไซต์
 - แผนการกู้คืน Dent Web Application
 - แผนการกู้คืนระบบสารสนเทศการศึกษา

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์ฉุกเฉิน ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเป็นประจำทุกเดือน และรายงานการเกิดปัญหาและผลการแก้ไขให้ทราบทันที พร้อมทั้งปรับปรุงแนวปฏิบัติการจัดการด้านความปลอดภัย ปลอดภัย ความเสี่ยงของระบบฐานข้อมูลและเครือข่ายเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ เพื่อให้สามารถนำไปมาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติต่อไป

ส่วนที่ ๘

แนวปฏิบัติการจัดการข้อมูลในเครื่องคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อให้การจัดการข้อมูลในคอมพิวเตอร์เป็นไปด้วยความเรียบร้อย
๒. ควบคุมข้อมูลคอมพิวเตอร์ไม่ให้รั่วไหลหรือนำไปใช้ต่อในทางไม่พึงประสงค์
๓. ลดปัญหาเรื่องข้อมูลสูญหาย
๔. ลดการติดขัดในการทำงาน หน่วยงานสามารถทำงานได้อย่างต่อเนื่อง

ผู้รับผิดชอบ

๑. งานเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลทรัพยากรสารสนเทศ
๓. หน่วยงานที่ใช้ทรัพยากรสารสนเทศ
๔. เจ้าหน้าที่ของหน่วยงานที่ใช้งานทรัพยากรสารสนเทศ

อ้างอิงมาตรฐาน

๑. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

แนวปฏิบัติ

๑. กรณีอุปกรณ์ Harddisk เสียหาย
 - ๑.๒. บุคลากรเจ้าของข้อมูลต้องทำการ Backup ข้อมูลไว้อุปกรณ์เก็บข้อมูลอื่น เช่น Handy Drive , External Harddisk หรือ บน Cloud Google Drive อยู่สม่ำเสมอเพื่อป้องกันข้อมูลเสียหายหรือสูญหาย
 - ๑.๒. หากเป็น Harddisk ที่อยู่ในประกัน ทางเจ้าหน้าที่สารสนเทศ จะทำการส่งเคลม เพื่อนำ Harddisk ตัวใหม่มาเปลี่ยน หาก Harddisk หมดประกัน จะดำเนินการจัดหา Hard disk ใหม่ทดแทน
๒. กรณีบุคลากรลาออก หรือไม่ได้ทำงานอยู่ในคณะ
 - ๒.๑. บุคลากรเจ้าของข้อมูลต้องดำเนินการจัดการข้อมูลส่วนตัวที่อยู่ในเครื่องคอมพิวเตอร์และลบข้อมูลส่วนตัวออก
 - ๒.๒. บุคลากรเจ้าของข้อมูลต้องส่งมอบข้อมูลเกี่ยวกับงานในองค์กรให้กับหน่วยงานที่สังกัดเพื่อนำไปใช้ต่อ
 - ๒.๓. หน่วยงานแจ้งเรื่องไปทางงานเทคโนโลยีสารสนเทศ ทางเจ้าหน้าที่เทคโนโลยีสารสนเทศ จะมาดำเนินการ ลบข้อมูลทั้งหมดที่อยู่ในเครื่องคอมพิวเตอร์ และติดตั้ง Software ใหม่ให้เพื่อหน่วยงานนำเครื่องคอมพิวเตอร์ไปใช้งานต่อ
๓. กรณีบุคลากรเสียชีวิต

- ๓.๑. หน่วยงานที่บุคลากรสังกัดนำข้อมูลออกจากเครื่องคอมพิวเตอร์เพื่อนำไปใช้ต่อในองค์กร หากติดปัญหาให้แจ้งมายังเจ้าหน้าที่เทคโนโลยีสารสนเทศ
- ๓.๒. หน่วยงานแจ้งเรื่องไปทางงานเทคโนโลยีสารสนเทศ ทางเจ้าหน้าที่เทคโนโลยีสารสนเทศ จะมาดำเนินการลบข้อมูลทั้งหมดที่อยู่ในเครื่องคอมพิวเตอร์ และติดตั้ง Software ใหม่ให้เพื่อหน่วยงานนำเครื่องคอมพิวเตอร์ไปใช้งานต่อ

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

ภาคผนวก

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

ภาคผนวก ก

ตารางรายละเอียดช่องทางการติดต่อหน่วยงานผู้ดูแลข้อมูลแต่ละประเภท

ตารางที่ ๑ รายละเอียดช่องทางการติดต่อหน่วยงานผู้ดูแลข้อมูลแต่ละประเภท

ประเภทข้อมูล	หน่วยงาน	เบอร์โทรติดต่อ	อีเมล
๑. ข้อมูลนักศึกษา	หน่วยทะเบียนและประเมินผลการศึกษา	๐๗๔-๒๘๗๕๒๙	dentpsu_registrar@hotmail.com
	หน่วยกิจการนักศึกษา	๐๗๔-๒๘๗๕๓๒	dentpsu.studentaffairs@gmail.com
	หน่วยบัณฑิตศึกษา - ระดับหลังปริญญา	๐๗๔-๒๘๗๕๒๙	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

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

ภาคผนวก ข
แบบฟอร์มขอใช้งาน E-Request



แบบฟอร์มขอพัฒนาระบบสารสนเทศ โทร. 7540
งานเทคโนโลยีสารสนเทศ คณะทันตแพทยศาสตร์ ม.อ.

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

วันที่ขอ..... โทรศัพท์..... อีเมล.....

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 (.....)/...../.....	<input type="checkbox"/> เห็นชอบ โดยมอบหมาย..... <input type="checkbox"/> ไม่เห็นชอบ..... ลงชื่อ..... (นางสาวสุทิดา จรรย์วัฒน์) หัวหน้างานเทคโนโลยีสารสนเทศ/...../.....	<input type="checkbox"/> รับทราบ.....
ลงชื่อ..... ผู้บังคับบัญชา (.....)/...../.....	<input type="checkbox"/> อนุมัติ <input type="checkbox"/> ไม่อนุมัติ ลงชื่อ..... (ผศ.ดร.ทพญ. สุภาวดี เนาว์รุ่งโรจน์) ผู้ช่วยคณบดีฝ่ายสารสนเทศ/...../.....	ลงชื่อ..... (.....)/...../.....



แบบฟอร์ม แจ้งปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ โทร. 7758
งานเทคโนโลยีสารสนเทศ คณะทันตแพทยศาสตร์ ม.อ.

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

วันที่ขอ..... โทรศัพท์..... อีเมล.....

มีความประสงค์ ปรับปรุงพื้นที่ ขอยืมอุปกรณ์เครือข่าย

พื้นที่ปรับปรุง.....

วัตถุประสงค์ ความต้องการ/.....

ผู้เกี่ยวข้องกับพื้นที่ปรับปรุง หน่วยงาน /.....

เอกสารสนับสนุนการปรับปรุงพื้นที่

ผังปรับปรุงพื้นที่เดิม

ผังปรับปรุงพื้นที่ใหม่

แบบฟอร์ม แจ้งปรับปรุงพื้นที่ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์

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

สำหรับผู้ขอใช้บริการ	เห็นควรอนุมัติ/คำสั่ง	สำหรับเจ้าหน้าที่ผู้ได้รับมอบหมาย
ลงชื่อ.....ผู้ขอใช้บริการ (.....)/...../.....	<input type="checkbox"/> เห็นชอบ โดยมอบหมาย..... <input type="checkbox"/> ไม่เห็นชอบ..... ลงชื่อ..... (นางสาวสุทิดา จรรย์นุวัฒน์) หัวหน้างานเทคโนโลยีสารสนเทศ/...../.....	<input type="checkbox"/> รับทราบ.....
ลงชื่อ..... ผู้บังคับบัญชา (.....)/...../.....	<input type="checkbox"/> อนุมัติ <input type="checkbox"/> ไม่อนุมัติ ลงชื่อ..... (ผศ.ดร.ทพญ. สุภาวดี เนาว์รุ่งโรจน์) ผู้ช่วยคณบดีฝ่ายสารสนเทศ/...../.....	ลงชื่อ..... (.....)/...../.....

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

ภาคผนวก ค

ตารางสมรรถนะพื้นฐานทางด้านคอมพิวเตอร์ให้เหมาะสมกับลักษณะการปฏิบัติงาน

ตารางที่ ๒ สมรรถนะพื้นฐานทางด้านคอมพิวเตอร์ที่เหมาะสมกับลักษณะการปฏิบัติงาน ให้ครอบคลุม Digital Literacy ๙ ด้าน

ตำแหน่ง	ทักษะทางด้านคอมพิวเตอร์
๑. อาจารย์/ทันตแพทย์	๑.๑ โปรแกรมพื้นฐานที่ต้องใช้ภายในสำนักงาน MS Office เช่น Word, Excel, Power Point ๑.๒ โปรแกรมสำหรับโต้ตอบ รับ-ส่งอีเมลล์ 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 ระบบคลินิกกรรมนักศึกษา 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-ส่งอีเมลล์ 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 แจ้งซ่อมครุภัณฑ์ 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-ส่งอีเมลล์ 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 แจ้งซ่อมครุภัณฑ์ จองห้องประชุม เบิกวัสดุออนไลน์

ตำแหน่ง	ทักษะทางด้านคอมพิวเตอร์
	๓.๗ สามารถแก้ไขปัญหาคอมพิวเตอร์เบื้องต้น เช่น การเปลี่ยนหมึกพิมพ์ แก้ไขปัญหากระดาษติด ปรับช่วงเครื่องพิมพ์แคร่กระดาษต่อเนื่อง ๓.๘ สามารถสร้างข้อมูลประชาสัมพันธ์หน่วยงานและ/หรือผลงานของตนเองได้ ผ่านช่องทางต่าง ๆ เช่น เว็บไซต์หน่วยงาน เพชบุ๊ก เป็นต้น
๔. นักศึกษาทันตแพทย์ และทันตแพทย์หลังปริญญา และนักศึกษาผู้ช่วยทันตแพทย์	๔.๑ โปรแกรมพื้นฐานที่ต้องใช้ภายในสำนักงาน MS Office เช่น Word, Excel, Power Point ๔.๒ โปรแกรมสำหรับโต้ตอบ รับ-ส่งอีเมล 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 ระบบคลินิกกรรมนักศึกษา ๔.๗ สามารถแก้ไขปัญหาคอมพิวเตอร์เบื้องต้น เช่น การเปลี่ยนหมึกพิมพ์ แก้ไขปัญหากระดาษติด ปรับช่วงเครื่องพิมพ์แคร่กระดาษต่อเนื่อง

ภาคผนวก ง
ตารางการสำรองข้อมูลและแผนปฏิบัติงานและตารางการบริหารความเสี่ยงระบบเครือข่าย เครื่องแม่ข่าย ระบบ
คอมพิวเตอร์และอุปกรณ์ต่อพ่วง

ตารางที่ ๓ การสำรองข้อมูล

ระบบสารสนเทศ	ความถี่	ผู้รับผิดชอบ
ระบบสนับสนุนงานบริหารและเว็บไซต์		
<ul style="list-style-type: none"> - 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	สุทิตา จรรย์านูวัฒน์
Database Server (Mysql)	ทุกวัน	สุทิตา จรรย์านูวัฒน์
Database Server (Oracle Link จากสำนักนวัตกรรมการดิจิทัลและระบบอัจฉริยะ)	ในวันศุกร์ ของทุกสัปดาห์	สุทิตา จรรย์านูวัฒน์

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 Backup) เวลา ๐๐.๐๐ น.	นพสิทธิ์ ไชยนนท์ อูมา เพ็ชรคง รัชดา โรจน์หัตถิน
- ระบบคัดกรองก่อนการรักษาทางทันตกรรม	ทุกวัน	
ระบบบัญชีเครือข่าย		
- DHCP-Server สำหรับ สนล. + รพ. + Wi-Fi และการอบรม	ทุกวัน เวลา ๒๒.๐๐ น.	รัชดา โรจน์หัตถิน
- Core-Switch	ทุกสิ้นเดือน	

ตารางที่ ๕ ตารางแผนปฏิบัติงานและการบริหารความเสี่ยงระบบเครือข่าย เครื่องแม่ข่าย ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

แผนบริหารความเสี่ยง	ความถี่	ผู้รับผิดชอบ
ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก		
1. อัปเดตแพทช์ระบบปฏิบัติการของเครื่องแม่ข่าย		
1.1 www.dent.psu.ac.th	1 ครั้ง / เดือน	สุทิตา จรรย์านุวัฒน์
1.2 sys.dent.psu.ac.th	1 ครั้ง / เดือน	สุทิตา จรรย์านุวัฒน์
1.3 app.dent.psu.ac.th	1 ครั้ง / เดือน	สุทิตา จรรย์านุวัฒน์
1.4 his.dent.psu.ac.th	1 ครั้ง / เดือน	รัชดา โรจนหัสติน
1.5 vcenter-dent.psu.ac.th(Hospital)	1 ครั้ง/ปี	รัชดา โรจนหัสติน
1.6 vcenter2-dent.psu.ac.th(Office)	1 ครั้ง/ปี	รัชดา โรจนหัสติน
1.7 vcenter3-dent.psu.ac.th(PACs)	1 ครั้ง/ปี	รัชดา โรจนหัสติน
1.8 DHCP-Server(Office)	1 ครั้ง/ปี	รัชดา โรจนหัสติน
1.9 DHCP-Server(Wi-Fi)	1 ครั้ง/ปี	รัชดา โรจนหัสติน
1.10 DHCP-Server(LAB3515)	1 ครั้ง/ปี	รัชดา โรจนหัสติน
1.11 DHCP-Server(Hospital)	1 ครั้ง/ปี	รัชดา โรจนหัสติน
2. เปลี่ยนพาสเวิร์ดของเครื่องแม่ข่าย และอุปกรณ์กระจายสัญญาณ	2 ครั้ง/ปี	รัชดา โรจนหัสติน
3. การติดตาม (monitor) log file ของเครื่องแม่ข่าย	1 ครั้ง / สัปดาห์	รัชดา โรจนหัสติน
4. อัปเดตเวอร์ชันของ wordpress ของเว็บไซต์คณะฯ และหน่วยงานภายในคณะฯ	ทุกวันสุดท้ายของเดือน	สุทิตา จรรย์านุวัฒน์
5. อัปเดตปลั๊กอินเว็บไซต์คณะฯ และหน่วยงานภายในคณะฯ	ทุกวันที่ 15 และวันสุดท้ายของเดือน	สุทิตา จรรย์านุวัฒน์
6. อัปเดต Certificate Web Server (psu.ac.th)	1 ครั้ง / ปี	สุทิตา จรรย์านุวัฒน์
7. อัปเดตเวอร์ชันระบบโรงพยาบาล (HOSxPXE)	2 ครั้ง / ปี	นพลสิทธิ์ ไชยนนท์ อูมา เพ็ชรคง
การดูแลอุปกรณ์ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง		
1. การทดสอบความพร้อมอุปกรณ์ของ UPS เครื่องแม่ข่าย	2 ครั้ง / ปี	ธีรเดช เขมะธีรรัตน์ ธนาวุฒ สงสุข มานิช จันทรวัดน์
2. ตรวจสอบเช็คคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	2 ครั้ง / ปี	ธีรเดช เขมะธีรรัตน์ ธนาวุฒ สงสุข มานิช จันทรวัดน์

ภาคผนวก จ

แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)



แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม

กลุ่มผู้ใช้งาน	หน่วยงานรับผิดชอบ	ขั้นตอนการส่งเอกสารปรับสถานะผู้ใช้งาน	ขั้นตอนการทวนสอบข้อมูล	ช่วงเวลาดำเนินการทวนสอบข้อมูล	รูปแบบรหัสผู้ใช้งาน	
					ปฏิบัติงานในเวลา	ปฏิบัติงาน ค. นอกเวลา
1. ทันตแพทย์						
1.1 อ. ทพ./ทพ. *มีสัญญาจ้างกับคณะฯ	ภาควิชา/ธุรการ รพ. (ขึ้นอยู่กับหน่วยงานที่สังกัด)	หน่วยงานที่รับผิดชอบ ธุรการ รพ. หน่วยงาน IT *แจ้ง Update ข้อมูลทันทีเมื่อได้รับอนุมัติให้ลาออก/ลาศึกษาต่อ	หน่วยงานเจ้าหน้าที่ หน่วยงาน IT	หน่วยงานเจ้าหน้าที่ส่งข้อมูลรายชื่อทันตแพทย์ ที่ได้รับการอัปเดตจากหน่วยงานต้นสังกัด มาตลอดปี มายังงาน IT ในสัปดาห์ที่ 3 ของเดือนธันวาคมของทุกปี	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				X	11ชื่อ.อักษรสกุลตัวแรก ตัวอย่าง 11nittayo.t

HOSxP Username request for DENTISTS





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	หน่วยทะเบียนและประเมินผลการศึกษา ☺ ธุรการ รพ. ☺ งาน IT	หน่วยงานที่รับผิดชอบส่งข้อมูลภายในสัปดาห์แรกของภาคการศึกษา	รหัสนักศึกษา	X
2.2 ระดับปริญญาตรี เกือบเคส		*แจ้ง Update ข้อมูลทันทีเมื่อได้รับการอนุมัติสำเร็จ การศึกษา/เหตุแห่งการพ้นสภาพ	*ทวนสอบข้อมูลตามช่วงเวลาที่กำหนด	งาน IT ดำเนินการสัปดาห์ที่ 2 ของภาคการศึกษา	33.รหัสนักศึกษา ตัวอย่าง 33.0123456789	
<p>หมายเหตุ ขั้นตอนการปรับสถานะผู้ใช้งาน</p> <ol style="list-style-type: none"> กรณีรับนักศึกษาใหม่ หน่วยทะเบียนฯ ส่งไฟล์ข้อมูลรายชื่อ รหัสบัตรประชาชน พร้อมรหัสนักศึกษาในรูปแบบไฟล์ .xlsx ☺ ธุรการ รพ. ☺ งาน IT (ดำเนินการช่วงเดือนสิงหาคมของทุกปี) กรณีจบการศึกษา หน่วยทะเบียนฯ ส่งไฟล์ข้อมูลรายชื่อพร้อมรหัสนักศึกษาในรูปแบบไฟล์ .xlsx ☺ ธุรการ รพ. ☺ งาน IT (ดำเนินการทันที Update เป็นปัจจุบัน) กรณีนักศึกษาเกือบเคส ส่งไฟล์ข้อมูลรายชื่อ รหัสบัตรประชาชน พร้อมรหัสนักศึกษาในรูปแบบไฟล์ .xlsx พร้อมระบุช่วงเวลาที่ต้องคงอยู่ในระบบฯ 						

HOSxP Username request for Undergrad students

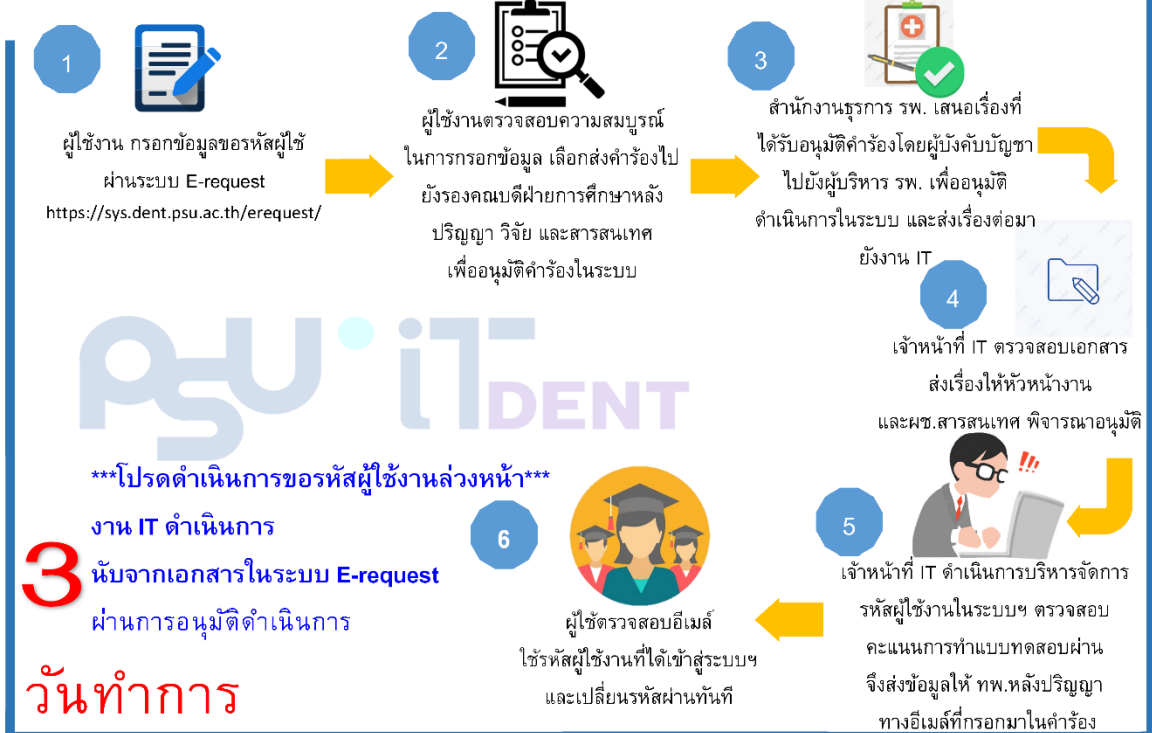




แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม

กลุ่มผู้ใช้งาน	หน่วยงานรับผิดชอบ	ขั้นตอนการส่งเอกสาร ปรับสถานะผู้ใช้งาน	ขั้นตอนการทวนสอบข้อมูล	ช่วงเวลาดำเนินการทวนสอบข้อมูล	รูปแบบรหัสผู้ใช้งาน	
					ปฏิบัติงานในเวลา	ปฏิบัติงาน ค. นอเวลา
3. ทันตแพทย์หลังปริญญา						
3.1 ทันตแพทย์หลังปริญญา	ภาควิชา และ หน่วยบัณฑิตศึกษา	หน่วยงานในสังกัด ▼ หน่วยบัณฑิตศึกษา ▼ ธุรการ รพ. ▼ งาน IT	หน่วยงานในสังกัด ▼ หน่วยบัณฑิตศึกษา ▼ หน่วยการเจ้าหน้าที่ ▼ ธุรการ รพ. ▼ งาน IT	หน่วยงานที่รับผิดชอบส่งข้อมูล ภายในสัปดาห์แรก ของภาคการศึกษา งาน IT ดำเนินการสัปดาห์ที่ 2 ของภาคการศึกษา หน่วยงานต้นสังกัดรับผิดชอบส่ง ข้อมูล พร้อมระบุช่วงเวลาที่ต้องคง อยู่ในระบบ งาน IT ดำเนินการ 3 วันทำการ นับ จากได้รับแจ้งเอกสารผ่านทางระบบ E-doc	รหัสนักศึกษา	11ชื่อ.อักษรสกุลตัวแรก ตัวอย่าง 11nittaya.t (ดำเนินการทวนสอบ เหมือน ชื่อ 1.3 ทพ. *ไม่มีสัญญาจ้างกับ คณะฯ)
3.2 ทันตแพทย์หลังปริญญา เก็บเคส		*แจ้ง Update ข้อมูลทันทีเมื่อได้รับ อนุมัติสำเร็จ การศึกษา/เหตุแห่ง การพ้นสภาพ	*ทวนสอบข้อมูล ตามช่วงเวลา ที่กำหนด	66.รหัสนักศึกษา ตัวอย่าง 66.0123456789		
หมายเหตุ ขั้นตอนการปรับสถานะผู้ใช้งาน 1. กรณีรับนักศึกษาใหม่ หน่วยบัณฑิตรวบรวมข้อมูลจากภาควิชา นำส่งไฟล์ข้อมูลส่วนบุคคล รายละเอียดข้อมูลตามแบบฟอร์มขอ user HOSxP ส่งข้อมูลมาในรูปแบบไฟล์ .xlsx พร้อมบันทึกข้อความปะหน้า ➡ ธุรการ รพ. ➡ งาน IT (ดำเนินการช่วงเดือนสิงหาคมของทุกปี) 2. กรณีจบการศึกษา หน่วยบัณฑิตรวบรวมข้อมูลจากภาควิชา นำส่งไฟล์ข้อมูลส่วนบุคคล รายละเอียดข้อมูลตามแบบฟอร์มขอ user HOSxP ส่งข้อมูลมาในรูปแบบไฟล์ .xlsx พร้อมบันทึกข้อความปะหน้า ➡ ธุรการ รพ. ➡ งาน IT (ดำเนินการทันที Update เป็นปัจจุบัน) 3. กรณีนักศึกษาเก็บเคส ภาควิชา ส่งไฟล์ข้อมูลรายชื่อ รหัสนักศึกษาในรูปแบบไฟล์ .xlsx พร้อมระบุช่วงเวลาที่ต้องคงอยู่ในระบบ ➡ หน่วยบัณฑิต ➡ ธุรการ รพ. ➡ งาน IT (หมายเหตุ หน่วยบัณฑิตส่งข้อมูลส่ง ➡ หน่วยการเจ้าหน้าที่ เพื่อ Update ข้อมูลเป็นปัจจุบัน)						

HOSxP Username request for Postgrad students





แนวปฏิบัติการขอรหัสเข้าใช้งานระบบสารสนเทศ ภายในคณะฯ และ โรงพยาบาลทันตกรรม

กลุ่มผู้ใช้งาน	หน่วยงาน รับผิดชอบ	ขั้นตอนการ ส่งเอกสาร ปรับสถานะผู้ใช้งาน	ขั้นตอนการ ทวนสอบข้อมูล	ช่วงเวลาดำเนินการ ทวนสอบข้อมูล	รูปแบบรหัสผู้ใช้งาน	
					ปฏิบัติงานในเวลา	ปฏิบัติงาน ค. นอกเวลา
4. บุคลากร						
4.1 สังกัด รพ. ทันตกรรม *มีสัญญาจ้างกับ คณะฯ	ธุรการ รพ./ คลินิกต่าง ๆ/ หน่วยการเจ้าหน้าที่ (ขึ้นอยู่กับ หน่วยงาน ที่สังกัด)	หน่วยงานที่รับผิดชอบ ☺ ธุรการ รพ. ☺ หน่วยการเจ้าหน้าที่ ☺ งาน IT *แจ้ง Update ข้อมูลทันทีเมื่อ ได้รับอนุมัติ เข้าปฏิบัติงาน/ ลาออก	หน่วยการเจ้าหน้าที่ ☺ งาน IT *ทวนสอบข้อมูล ตามช่วงเวลา ที่กำหนด	หน่วยการเจ้าหน้าที่ส่งข้อมูลรายชื่อ บุคลากร ที่ได้รับการอภัยโทษจาก หน่วยงานต้นสังกัด มาตลอดปี มายังงาน IT ใน สัปดาห์ที่ 3 ของเดือน ธันวาคม ของทุกปี งาน IT ดำเนินการสัปดาห์สุดท้าย ของเดือน ธันวาคม ของทุกปี	ชื่อ.อักษรสกุลตัวแรก	ชื่อ.อักษรสกุลตัวแรก
4.1.1 เจ้าหน้าที่ รพ. ทั้งหมด						
4.1.2 เจ้าหน้าที่ รายคาบ						
4.2 สังกัดสำนักงาน เลขานุการ**	หน่วยการเจ้าหน้าที่					
4.3 เจ้าหน้าที่ ค. นอกเวลา *มีคำสั่งแต่งตั้งจาก คณะฯ รวมถึง จนท. คณะฯ ที่ทำงานเสริม ณ ค. นอกเวลา	คลินิกบริการ ทันตกรรม นอกเวลา				X	22 ชื่อ.อักษรสกุลตัวแรก ตัวอย่าง 22nittaya.t
4.5 เจ้าหน้าที่งาน IT	งาน IT	ดำเนินการเหมือน 1.1 ทพ. สัญญาจ้าง Admin ระบบ HIS ของงาน IT บริหารจัดการข้อมูลตามบทบาทหน้าที่ ของเจ้าหน้าที่ในงาน		สัปดาห์ที่ 3 ของเดือน เมษายน ของทุกปี งาน IT ดำเนินการสัปดาห์สุดท้าย ของเดือน เมษายน ของทุกปี	ชื่อ.อักษรสกุลตัวแรก	X

**หมายเหตุ ข้อ 4.2 ขั้นตอนการปรับสถานะผู้ใช้งานดำเนินการดังนี้ หน่วยงานที่รับผิดชอบ ☺ หน่วยการเจ้าหน้าที่ ☺ ธุรการ รพ. ☺ งาน IT

คล้าย

HOSxP Username request for Staffs



หมายเหตุ :

๑. กำหนดให้ไฟล์ข้อมูล การทวนสอบข้อมูลผู้ใช้ที่จะส่งมายังงานไอที เป็นไฟล์ Excel เท่านั้น
๒. การทวนสอบข้อมูลผู้ใช้ของทุกหน่วยงานจะต้องมีทั้งข้อมูลผู้ใช้งานที่ยังคงปฏิบัติงานอยู่ และข้อมูล ผู้ใช้งานที่พ้นสภาพ/ลาออกไปแล้ว 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 จึงจะเข้าใช้งานระบบฯ ได้
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

แผนการรักษาความปลอดภัย (ฉบับ ๒)

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	นางสุชาลีณี ต้นห้วย นางเสาวณี แซ่หลี นางสุทิตา จรรย์านวัฒน์ 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		นางสุชาลีณี ต้นห้วย นางเสาวณี แซ่หลี นางสาวธัญพิชชา ชูไสต 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	นางสุชาลีณี ต้นห้วย นางเสาวณี แซ่หลี	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th
๓	Fund	ระบบกองทุนสวัสดิการพนักงานมหาวิทยาลัย	https://fund.psu.ac.th	นายสุภัทร์ พงศาธิรัตน์ นางกวิณทิพย์ ชูศรี	supat.p@psu.ac.th kavinthip.l@psu.ac.th
๔	PVD	ระบบกองทุนสำรองเลี้ยงชีพ	https://pvd.psu.ac.th	นายสุภัทร์ พงศาธิรัตน์ นางสุชาลีณี ต้นห้วย	supat.p@psu.ac.th sutasinee.n@psu.ac.th
๕	work.psu.ac.th	ระบบดูรายงานการลงเวลาปฏิบัติราชการบนเว็บของบุคลากรในหน่วยงาน	https://work.psu.ac.th	นางสุชาลีณี ต้นห้วย นางเสาวณี แซ่หลี	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th
๖	PSU Passport	ระบบจัดการบัญชีผู้ใช้งาน	https://adsadmin.psu.ac.th	นางสุชาลีณี ต้นห้วย	sutasinee.n@psu.ac.th

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
		ระบบสารสนเทศ			
๗	TOR Online	ระบบประเมินผล การปฏิบัติงาน	https://tor.psu.ac.th	นางสุธาสินี ต้นห้วย นางเสาวณี แซ่หลี่ นางสาวนิตตยา ตริสุวรรณ	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th nittaya.t@psu.ac.th
๘	Competency	ระบบประเมินสมรรถนะ	https://competency.psu.ac.th	นางสุธาสินี ต้นห้วย นางเสาวณี แซ่หลี่ นางสุทิสสา จรรย์านูวัฒน์	sutasinee.n@psu.ac.th saowanee.sa@psu.ac.th suthisa.j@psu.ac.th
๙	hrmis	ระบบผลงานวิชาการและภาระงาน	https://hrmis.psu.ac.th	นางสุธาสินี ต้นห้วย นางสาวกนกวรรณ สุวรรณรัตน์ นายเขมรัฐ เขมวงศ์ นางสุทิสสา จรรย์านูวัฒน์	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	ระบบตะกร้าขาว	https://epr.psu.ac.th	นางอัญชลี สุวรรณโร	aunchalee.su@psu.ac.th
๑๓	edoc	ระบบเอกสาร	https://edoc.psu.ac.th	นางนารี จันทร์ตัน	naree.t@psu.ac.th
๑๔	emeeting	ระบบประชุม	http://meeting.dent.psu.ac.th/dentmeeting	นางสาวจรรยากร คงแก้ว นางทิชาภรณ์ รัตน์ะ	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 ตริรัฐเพ็ชร นายสุภัทร์ พงศาธิรัตน์ นางสาวอรวรรณ เจริญวุฒิมวงษา นางกวิณฑิพย์ ชูศรี นางสาวชื่นพจี แสนหา นางกาญจนา กัลยาศิริ นางปิ่นประภา ทันหะवास นางเสาวณี แซ่หลี่ นางสาวผกาพฤษ สีคำอ่อน นางสาวเครือวัลย์ พวงสอน นางสาวฉัตริกา หลีเป็นหมาน นางสาวปวีริศา 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	ระบบผลงานวิชาการและภาระงาน	https://hrmis.psu.ac.th	นายเขมรัฐ เขมวงศ์ นางสาวปรียาภัทร์ ยอดทอง	kemarajt.k@psu.ac.th peeyapat.y@psu.ac.th
๓	NRIS	ระบบข้อมูลสารสนเทศวิจัยและนวัตกรรมแห่งชาติ	http://nriss.nrc.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	ระบบรางวัล บทความ ตีพิมพ์ของ มหาวิทยาลัย สงขลา นครินทร์	https://aro.psu.ac.th/aro-test	นางสาวปรียาภัทร์ ยอดทอง	peeyapat.y@psu.ac.th

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

ตารางที่ ๗ ระบบทะเบียนและบัณฑิตศึกษา (การศึกษา)

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
๑	SIS	ระบบสารสนเทศนักศึกษา	https://sis-hatyai6.psu.ac.th	นางปวีริศา เล็งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางลัดดาวัลย์ วงศ์ไชย นางวรรณรี ซาติดำ นางสาวรัชกร ธนกุลเลิศ นางกัลยา โลหะประเสริฐ นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตีรารานูรัตน์ นางสาวพิมพ์สุจี ศรีสุวรรณ นางรณิดา อ่ำภา	pawarisa.s@psu.ac.th paweenrat.n@psu.ac.th laddawan.w@psu.ac.th wannaree.t@psu.ac.th ratchakorn.m@psu.ac.th kanlaya.l@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	นางปวีริศา เล็งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางสาว ธนิษฐา อวีรุตม์ นางกัลยา โลหะประเสริฐ นางสาววรรณ พฤษศรี นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตีรารานูรัตน์ นางสาวพิมพ์สุจี ศรีสุวรรณ นางรณิดา อ่ำภา นางอัจฉรา ทิพย์สุนทร	pawarisa.s@psu.ac.th paweenrat.n@psu.ac.th thanittha.a@psu.ac.th kanlaya.l@psu.ac.th worawan.p@psu.ac.th nongyaow.u@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	นางปวีริศา เล็งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางลัดดาวัลย์ วงศ์ไชย นางกัลยา โลหะประเสริฐ นางสาววรรณ พฤษศรี นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตีรารานูรัตน์ นางสาวพิมพ์สุจี ศรีสุวรรณ นางรณิดา อ่ำภา นางณภัทรชนก มหาเกตุ	pawarisa.s@psu.ac.th paweenrat.n@psu.ac.th laddawan.w@psu.ac.th kanlaya.l@psu.ac.th worawan.p@psu.ac.th nongyaow.u@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	นางปวีริศา เล็งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางกัลยา โลหะประเสริฐ นางสาวนงเยาว์ อุไรรัตน์	pawarisa.s@psu.ac.th paweenrat.n@psu.ac.th kanlaya.l@psu.ac.th nongyaow.u@psu.ac.th

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
				นางสาวเบญจวรรณ ตรีรานูรัตน์	benjawan.t@psu.ac.th
๕	ระบบรับเข้า นักศึกษา	ระบบรับเข้า นักศึกษา	https://gradmis.psu.ac.th/grad_admission	นางปวีริศา เล็งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางกัลยา โลหะประเสริฐ นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตรีรานูรัตน์ นางรณิดา อ่ำภา นางณภัทรชนก มหาเกตุ	pawarisa.s@psu.ac.th paweenrat.n@psu.ac.th kanlaya.l@psu.ac.th nongyaow.u@psu.ac.th benjawan.t@psu.ac.th ranida.a@psu.ac.th napatchanok.m@psu.ac.th
๖	ระบบการจัดสรร ทุนการศึกษา ระดับ บัณฑิตศึกษา	ระบบการจัดสรร ทุนการศึกษา ระดับ บัณฑิตศึกษา	https://gradmis.psu.ac.th/grad_scholarship	นางปวีริศา เล็งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางสุดาวลัย จิโรจน์วณิชชากร นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตรีรานูรัตน์	pawarisa.s@psu.ac.th paweenrat.n@psu.ac.th sudawan.j@psu.ac.th nongyaow.u@psu.ac.th benjawan.t@psu.ac.th
๗	ระบบการเบิกจ่าย ทุนอุดหนุน การวิจัยเพื่อ วิทยานิพนธ์	ระบบการเบิกจ่าย ทุนอุดหนุน การวิจัยเพื่อ วิทยานิพนธ์	https://gradmis.psu.ac.th/scholar_payment	นางปวีริศา เล็งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตรีรานูรัตน์	pawarisa.s@psu.ac.th paweenrat.n@psu.ac.th nongyaow.u@psu.ac.th benjawan.t@psu.ac.th
๘	ระบบ GSMIS	ระบบ GSMIS (แต่งตั้ง อาจารย์ พิเศษ)	https://gsmis.psu.ac.th/gsmis2	นางปวีริศา เล็งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางกัลยา โลหะประเสริฐ นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตรีรานูรัตน์	pawarisa.s@psu.ac.th paweenrat.n@psu.ac.th kanlaya.l@psu.ac.th nongyaow.u@psu.ac.th benjawan.t@psu.ac.th
๙	ระบบการขอ อนุมัติ เดินทางไป ต่างประเทศ	Inbound / Outbound for Student	https://io-student.psu.ac.th	นางสาวปวีณรัตน์ ณ พัทลุง นางปวีริศา เล็งเสน นางวรรณวี ชาติดำ นางสุดาวลัย จิโรจน์วณิชชากร นางกัลยา โลหะประเสริฐ นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตรีรานูรัตน์	paweenrat.n@psu.ac.th pawarisa.s@psu.ac.th wannaree.t@psu.ac.th sudawan.j@psu.ac.th kanlaya.l@psu.ac.th nongyaow.u@psu.ac.th benjawan.t@psu.ac.th
๑๐	Fiscal management information	ระบบการ จัดเก็บ ค่าธรรมเนียม การศึกษา	https://fmisbudget.psu.ac.th	นางสาวรัชกร ชนกุลเลิศ	ratchakorn.m@psu.ac.th

ลำดับ	ชื่อระบบ (EN)	ชื่อระบบ (TH)	URL	ผู้ดูแลระบบ/ผู้ใช้งาน	Email Address
	n system: FMIS				
๑๑	ทรานสคริป กิจกรรม นักศึกษา	ทรานสคริป กิจกรรม นักศึกษา	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

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

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	นางสาววรรณ สมัตตนาคนางเครือสิรี เดชชินินทร์	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.thainrsls.org/	นางสาวราเวีย สุเสน	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 วงศ์ไชย นางสาวสุทิสสา จรรย์านูวัฒน์	kanokwan.s@psu.ac.th laddawan.w@psu.ac.th suthisa.j@psu.ac.th

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ ๒)

ภาคผนวก ข

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 ตันห้วย	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 ตันห้วย นางทิจาภรณ์ รัตน์ชะ 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	นางสาวฉัตรทริกา หลีเป็นหมาน	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	
		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 เจริญวุฒิมวงษา	orawan.ch@psu.ac.th	
๘	e-Maintenance	ระบบแจ้งซ่อมครุภัณฑ์-วัสดุ	https://sys.dent.psu.ac.th/repair	- ส่วนแจ้งซ่อมงานเทคโนโลยีสารสนเทศ นางสาวนิตตยา ตริสุวรรณ นายธีรเดช เขมะธีรรัตน์ นายธนาวุฒิ สงสุข - ส่วนแจ้งซ่อมงานวิศวะ นางสาวอุษา สวัสดิ์ นายนิพนธ์ 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	- ส่วนงานเทคโนโลยีสารสนเทศ นางสาวนิตตยา ตริสุวรรณ - ส่วนงานธุรการโรงพยาบาล นางสาวเพลินพิศ สิทธิจันทร์ นางทิชาภรณ์ รัตน์ะ	nittaya.t@psu.ac.th phleanphit.s@psu.ac.th tichaporn.r@psu.ac.th	
๑๑	e-Proofing Programs	ระบบจองโปรแกรมชุดแปลภาษา	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 อวีรุตม์ - ห้องประชุม นางสาวสุภารัตน์ สังข์ทอง - ห้องปฏิบัติคอมพิวเตอร์ นางสาวนิตตยา ตริสุวรรณ - 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/	- อาจารย์วรัณษา พิธพรชัยกุล - นางสาวรัชฎาภรณ์ นมะเส - นางสาวพรชนก ช่วยวิจิตร	wattana.p@psu.ac.th ratchadapom.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	ระบบบริหารจัดการความเสี่ยง ห้องปฏิบัติการวิจัย	https://sys.dent.psu.ac.th/dentlabrisk	นายเขมรัฐ เขมวงศ์ นางสาวสโรชา ฤทธิเดช	kemarajt.k@psu.ac.th sarocha.ri@psu.ac.th	
๒	EM-EMS	ระบบขอใช้พื้นที่และยืมเครื่องมือวิจัย	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 ฮูเสิน	ravia.h@psu.ac.th	
๒		ระบบตรวจเช็คครุภัณฑ์โรงพยาบาลทันตกรรม	https://sys.dent.psu.ac.th/maintain	นางสาวปัทมา 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) นางสาวปัทมา 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 ตลิ่งจิตร (ดูแลภาพรวม)	siriwadee.b@psu.ac.th supitcha.t@psu.ac.th	
๖		ระบบออกใบเสร็จ 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/over_time	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	นางปวีริศา ส่งเสน นางสาวปวีณรัตน์ ณ พัทลุง นางลัดดาวัลย์ วงศ์ไชย นางกัลยา โลหะประเสริฐ นางสาววรรรณ พฤษศรี นางสาวนงเยาว์ อุไรรัตน์ นางสาวเบญจวรรณ ตีรารานูรัตน์ นางสาวพิมพ์สุจี ศรีสุวรรณ นางรณิดา อ่ำภา	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 วงศ์ไชย นางสาวนวลนภา แซ่ลี นางสาวรณิษฐา อวีรุตม์	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 วิทยวีร์ศักดิ์ หัวหน้าคลินิกสาขา Pedo	rajel.n@psu.ac.th	
	e-Dent-Lab	ระบบประเมินการปฏิบัติงาน Lab ของสาขาวิชาทันตกรรมหัตถการ	http://10.151.127.78/lab_new/	นางสาววรรรณ พฤษศรี	worrawan.p@psu.ac.th	
	e-Practical la	ระบบจองโต๊ะปฏิบัติการในห้อง 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 วงศ์ไชย นางสาวนวนลภา แซ่ลี นางสาวธนัชฐา อวีรุตม์	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	นางสาวธนัชฐา อวีรุตม์	thanittha.a@psu.ac.th	
๗	e-student	ระบบฐานข้อมูลนักศึกษาทันตแพทยศาสตร์ (ปริญญาตรี)	https://sys.dent.psu.ac.th/estudent/	นางวรรณรีชาติคำ	wannaree.t@psu.ac.th	
๘	e-Clinic	ระบบคลินิกรวมนักศึกษา	http://10.151.127.78/clinic/	นางลัดดาวัลย์ วงศ์ไชย นางสาวนวนลภา แซ่ลี นางสาวธนัชฐา อวีรุตม์ หัวหน้าคลินิก	laddawan.w@psu.ac.th nuannapa.s@psu.ac.th thanittha.a@psu.ac.th	กำลังพัฒนา

แผนการรักษาความปลอดภัยสารสนเทศ (ฉบับ ๒)

ภาคผนวก ซ

รายงานการวิเคราะห์และการประเมินความเสี่ยง ประจำปีงบประมาณ ๒๕๖๕

ภารกิจด้านความปลอดภัยของข้อมูล

แผนปฏิบัติงานและรายงานผลการบริหารความเสี่ยง ประจำปีงบประมาณ ...2566....

ประเภทเหตุการณ์ความเสี่ยง(10):

ด้านกาหนดินทาง(๐)

เหตุการณ์ความเสี่ยง (11)	ตัวชี้วัดความเสี่ยง (12)	แผนบริหารจัดการความเสี่ยง (13)	แผนผล	ระยะเวลาดำเนินการตามแผนบริหารจัดการความเสี่ยง (14)												ระดับความเสี่ยงก่อนการบริหารจัดการความเสี่ยง (15)			สัมผลกระทบต่อวัตถุประสงค์ (16)	ระดับความเสี่ยงหลังการบริหารจัดการความเสี่ยง (17)			ผลลัพธ์ที่ได้ (18)	
				พ.ศ 2565						พ.ศ 2566						ระดับโอกาสเกิด	ระดับผลกระทบ	ด้านของผลกระทบ		ระดับความเสี่ยง	ระดับโอกาสเกิด	ระดับผลกระทบ		ระดับความเสี่ยง
				ค.ค	ค.ธ	ก.ค	ก.พ	ก.ค	ก.ย	ค.ค	ค.ธ	ก.ค	ก.พ	ก.ค	ก.ย									
3. ข้อมูลเสียหาย (๐๖)	จำนวนครั้งที่บริหารจัดการผิดพลาด	1. กำหนดความถี่การสำรองข้อมูลโดยมีการสำรองข้อมูลระบบสารสนเทศตามประกาศใช้โดยในของข้อมูลในระบบ (ตามภาคผนวก ๖) ในแผนปฏิบัติการจัดการความเสี่ยง ปลอดภัย ความถี่ของระบบฐานข้อมูลและเครือข่ายเทคโนโลยีสารสนเทศ	แผน	←												สูง	สูง	ปานกลาง	2	4	ปานกลาง	ข้อมูลสูญหาย		
			สบ	←																				
			แผน	←																				
		2. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ	แผน	←												3	4	สูง	2	4	ปานกลาง			
			สบ	←																				
			แผน	←																				
		3. ทดสอบการกู้คืนข้อมูล	แผน	←												สูง	สูง	ปานกลาง	2	4	ปานกลาง			
			สบ	←																				
			แผน	←																				
4. ความปลอดภัยของข้อมูลระบบเครือข่ายสารสนเทศ	จำนวนครั้งของการเกิดอุบัติเหตุ	1. ติดตั้งโปรแกรมหรือแพตช์ความปลอดภัยบนระบบเครือข่าย	แผน	←												สูง	สูง	ปานกลาง	1	5	ปานกลาง			
			สบ	←																				
			แผน	←																				
		2. ติดตั้งโปรแกรมหรือแพตช์ความปลอดภัยบนระบบเครือข่าย	แผน	←												1	5	ปานกลาง						
			สบ	←																				
			แผน	←																				
	จำนวนครั้งที่ไม่ได้ยินข้อมูล	1. ติดตั้งโปรแกรมจำตั้ง (Access Control)	แผน	←												สูง	สูง	ปานกลาง	1	5	ปานกลาง			
			สบ	←																				
			แผน	←																				
		2. มีการล็อกประตูคอมพิวเตอร์ระบบเครือข่าย	แผน	←												สูง	สูง	ปานกลาง	2	5	สูง			
			สบ	←																				
			แผน	←																				

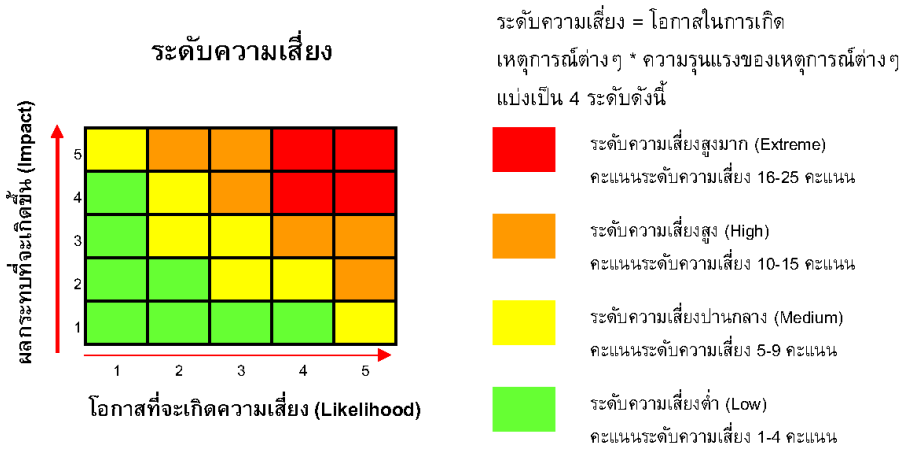
ประเมินความเสี่ยง

ระดับผลกระทบเหตุการณ์ที่เป็นความเสี่ยง

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	> 10 ล้านบาท หรือ เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูล	5
สูง	> 5 แสนบาท – 10 ล้านบาท หรือ เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลกระทบต่อความถูกต้องของข้อมูลบางส่วน	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

โอกาสที่จะเกิดความเสียหาย	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



อ่าน = > [แผนปฏิบัติงานและรายงานผลการบริหารความเสี่ยงงานเทคโนโลยีสารสนเทศ](#)

แผนการรักษาความปลอดภัยด้านสารสนเทศ (ฉบับ -