

รายละเอียดของรายวิชา

ชื่อสถาบันอุดมศึกษา
วิทยาเขต/คณะ/ภาควิชา

มหาวิทยาลัยราชภัฏสวนดุสิต
คณะวิทยาศาสตร์และเทคโนโลยี สาขาวิชาเทคโนโลยีสารสนเทศ

หมวดที่ 1 ข้อมูลทั่วไป

- รหัสและชื่อรายวิชา
4124106 ความมั่นคงของระบบเครือข่าย
Network Security
- จำนวนหน่วยกิต
3 หน่วยกิต 3 (2-2-6)
- หลักสูตรและประเภทของรายวิชา
วิทยาศาสตรบัณฑิต สาขาเทคโนโลยีสารสนเทศ / รายวิชาเลือก
- อาจารย์ผู้รับผิดชอบรายวิชาและอาจารย์ผู้สอน
อาจารย์จิระ จิตสุภา
- ภาคการศึกษา/ชั้นปีที่เรียน
ภาคการศึกษาที่ 2/2555 ชั้นปีที่ 3
- รายวิชาที่ต้องเรียนมาก่อน (Pre-requisite) (ถ้ามี)
การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์
- รายวิชาที่ต้องเรียนพร้อมกัน (Co-requisites) (ถ้ามี)
-
- สถานที่เรียน
ห้อง 11408 อาคาร 11 มหาวิทยาลัยราชภัฏสวนดุสิต
- วันที่จัดทำหรือปรับปรุงรายละเอียดของรายวิชาครั้งล่าสุด
30 ตุลาคม 2555

หมวดที่ 2 จุดมุ่งหมายและวัตถุประสงค์

1. จุดมุ่งหมายของรายวิชา

1. เพื่อให้ผู้เรียนมีความรู้ ความเข้าใจเทคโนโลยีเกี่ยวกับระบบความปลอดภัยและการสร้างความมั่นคงให้ระบบเครือข่าย
2. เพื่อให้ผู้เรียนมีความรู้ ความเข้าใจภัยคุกคามที่สามารถเกิดขึ้นกับเครือข่าย
3. เพื่อให้ผู้เรียนมีความรู้ ความเข้าใจความล้มเหลวด้านความปลอดภัยที่สามารถเกิดขึ้นในส่วนของ การเข้ารหัสลับและโปรโตคอลของเครือข่าย
4. เพื่อให้ผู้เรียนมีความรู้ ความเข้าใจโครงสร้างพื้นฐานของระบบกุญแจสาธารณะ
5. เพื่อให้ผู้เรียนมีความรู้ ความเข้าใจการตรวจสอบความปลอดภัยและความมั่นคงของโปรโตคอล และมาตรฐานการสื่อสาร
6. เพื่อให้ผู้เรียนมีความรู้ ความเข้าใจระบบความปลอดภัยของจดหมายอิเล็กทรอนิกส์ ระบบไฟร์วอลล์ และระบบตรวจจับผู้บุกรุกระบบเครือข่าย

2. วัตถุประสงค์ในการพัฒนา/ปรับปรุงรายวิชา

-

หมวดที่ 3 ลักษณะและการดำเนินการ

1. คำอธิบายรายวิชา

ศึกษาเทคโนโลยีเกี่ยวกับระบบความปลอดภัยและการสร้างความมั่นคงให้ระบบเครือข่าย ภัยคุกคามที่สามารถเกิดขึ้นกับเครือข่าย ความล้มเหลวด้านความปลอดภัยที่สามารถเกิดขึ้นในส่วนของ การเข้ารหัสลับและโปรโตคอลของเครือข่าย เครื่องแม่ข่ายที่ใช้ในกระบวนการพิสูจน์ตัวตนจริง โครงสร้างพื้นฐานของระบบกุญแจสาธารณะ การตรวจสอบความปลอดภัยและความมั่นคงของโปรโตคอลและมาตรฐานการสื่อสาร ระบบความปลอดภัยของจดหมายอิเล็กทรอนิกส์ ระบบไฟร์วอลล์ และระบบตรวจจับผู้บุกรุกระบบเครือข่าย

2. จำนวนชั่วโมงที่ใช้ต่อภาคการศึกษา

บรรยาย	สอนเสริม	ปฏิบัติ/งานภาคสนาม/การฝึกงาน	การศึกษาด้วยตนเอง
30 ชั่วโมง ต่อภาคการศึกษา	สอนเสริมตามความต้องการของนักศึกษาแต่ละคน	30 ชั่วโมง ต่อภาคการศึกษา	การศึกษาด้วยตนเอง 6 ชั่วโมงต่อสัปดาห์

3. จำนวนชั่วโมงต่อสัปดาห์ที่อาจารย์ให้คำปรึกษาและแนะนำทางวิชาการแก่นักศึกษาเป็นรายบุคคล
อาจารย์จัดเวลาให้คำปรึกษาเป็นรายบุคคล หรือรายกลุ่มตามความต้องการผ่านการสื่อสารช่องทางต่างๆ

หมวดที่ 4 การพัฒนาการเรียนรู้ของนักศึกษา

1. คุณธรรม จริยธรรม

1.1 คุณธรรม จริยธรรมที่ต้องพัฒนา

1. มีความรับผิดชอบ ละเอียดรอบคอบ ซื่อสัตย์ และมีวินัยในตนเอง
2. ตระหนักในคุณธรรม จริยธรรม เสียสละ รับผิดชอบต่อผู้อื่น
3. ซื่อสัตย์ มีวินัย ตรงต่อเวลา รู้กาลเทศะ และมีความรับผิดชอบต่อหน้าที่ของตนเอง และสังคม

1.2 วิธีการสอน

1. สอดแทรกประสบการณ์และกรณีตัวอย่าง ระหว่างการเรียนการสอน
2. อภิปรายและแสดงความคิดเห็นร่วมกัน
3. ให้นักศึกษาทำงานกลุ่ม รวบรวมข้อมูลจากเอกสารและภาคสนาม

1.3 วิธีการประเมินผล

1. ประเมินจากการอภิปราย แลกเปลี่ยนความคิดเห็นในชั้นเรียน
2. ประเมินจากการเข้าเรียนและพฤติกรรมในชั้นเรียนของนักศึกษา
3. ประเมินจากการตรงต่อเวลาในการส่งงานและประสิทธิภาพของงานที่ได้รับมอบหมาย
4. ประเมินจากการสังเกตพฤติกรรมการแสดงออก
5. ประเมินจากแบบทดสอบ

2. ความรู้

2.1 ความรู้ที่ต้องได้รับ

1. ความรู้ ความเข้าใจเทคโนโลยีเกี่ยวกับระบบความปลอดภัยและการสร้างความมั่นคงให้ระบบเครือข่าย
2. ความรู้ ความเข้าใจภัยคุกคามที่สามารถเกิดขึ้นกับเครือข่าย
3. ความรู้ ความเข้าใจความล้มเหลวด้านความปลอดภัยที่สามารถเกิดขึ้นในส่วนของการเข้ารหัสลับ และโปรโตคอลของเครือข่าย
4. ความรู้ ความเข้าใจโครงสร้างพื้นฐานของระบบกัญญาสารสนเทศ
5. ความรู้ ความเข้าใจการตรวจสอบความปลอดภัยและความมั่นคงของโปรโตคอลและมาตรฐานการสื่อสาร
6. ความรู้ ความเข้าใจระบบความปลอดภัยของจดหมายอิเล็กทรอนิกส์ ระบบไฟร์วอลล์ และระบบตรวจจับผู้บุกรุกระบบเครือข่าย

2.2 วิธีการสอน

1. บรรยายและให้แสดงความคิดเห็นเชิงวิเคราะห์เป็นรายบุคคล
2. ให้นักศึกษาจัดทำรายงานกลุ่มโดยรวบรวมข้อมูลจากเอกสารและภาคสนาม
3. ให้นักศึกษาค้นคว้าเพิ่มเติมด้วยตนเอง จากประเด็นสอนในชั้นเรียน

4. ฝึกปฏิบัติด้านความมั่นคงของระบบเครือข่าย
5. ร่วมกิจกรรมหรือจัดสัมมนาทางวิชาการ

2.3 วิธีการประเมินผล

1. ประเมินจากการนำเสนอรายงานการศึกษาค้นคว้าของนักศึกษา
2. ประเมินจากการมีส่วนร่วม แลกเปลี่ยนความคิดเห็นจากความรู้และประสบการณ์
3. ประเมินจากผลการปฏิบัติด้านความมั่นคงของระบบเครือข่าย
4. ประเมินจากแบบทดสอบปลายภาคเรียน

3. ทักษะทางปัญญา

3.1 ทักษะทางปัญญาที่ต้องพัฒนา

1. สามารถบูรณาการความรู้ในศาสตร์ต่างๆ ให้เกิดประโยชน์แก่ตนเองและส่วนรวม
2. สามารถสืบค้นและประเมินข้อมูลจากแหล่งเรียนรู้ที่หลากหลาย
3. สามารถคิดวิเคราะห์ รู้เท่าทันสถานการณ์และแก้ปัญหาอย่างสร้างสรรค์
4. สามารถนำความรู้ไปทำความเข้าใจและสร้างสรรค์สังคม

3.2 วิธีการสอน

1. บรรยาย และอภิปราย การทำกรณีศึกษาร่วมกันในชั้นเรียน
2. ให้นักศึกษาแสดงความคิดเห็นแลกเปลี่ยนประสบการณ์และมีข้อคิดเห็นร่วมกัน
3. มองสาระของแนวคิดทฤษฎีเชื่อมโยงไปสู่ปัญหาในพื้นที่

3.3 วิธีการประเมินผล

1. ประเมินผลจากการอภิปรายในชั้นเรียน
2. ประเมินผลจากประสิทธิผลของการนำเสนอรายงาน ผลงาน
3. แบบฝึกปฏิบัติ แบบทดสอบ

4. ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ

4.1 ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบที่ต้องพัฒนา

1. สามารถปฏิบัติและรับผิดชอบต่องานที่ได้รับมอบหมายตามหน้าที่และบทบาทของตนเองในกลุ่มได้อย่างเหมาะสม รวมทั้งมีส่วนร่วมในการช่วยเหลือผู้ร่วมงานและแก้ไขปัญหากลุ่ม
2. สามารถปรับตัว รับฟัง ยอมรับความคิดเห็น และทำงานร่วมกับผู้อื่นได้ ทั้งในฐานะผู้นำและสมาชิกของกลุ่ม
3. มีมนุษยสัมพันธ์ที่ดีกับผู้ร่วมงานในองค์กรและกับบุคคลทั่วไป
4. สามารถพัฒนาทักษะมนุษยสัมพันธ์ บุคลิกภาพและจริยธรรมได้อย่างเหมาะสม

4.2 วิธีการสอน

1. จัดกิจกรรมการเรียนการสอนที่เน้นการทำงานเป็นกลุ่มและงานที่ต้องมีปฏิสัมพันธ์ระหว่างบุคคล ด้วยการฝึกปฏิบัติ
2. ฝึกปฏิบัติ อภิปราย รายงานผลร่วมกัน
3. สอดแทรกประสบการณ์และสถานการณ์ปัจจุบันในด้าน คุณธรรม จริยธรรม ความรับผิดชอบต่อ การเคารพสิทธิมนุษยชน ผลกระทบจากการละเมิดลิขสิทธิ์ การมีมนุษยสัมพันธ์และการทำงานเป็นทีม ระหว่างการเรียนการสอน

4.3 วิธีการประเมินผล

1. ประเมินจากการอภิปรายร่วมกันในชั้นเรียน
2. ประเมินจากพฤติกรรมการทำกิจกรรมกลุ่ม
3. ประเมินจากประสิทธิผลของงานที่ได้รับมอบหมาย

5. ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ

5.1 ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศที่ต้องพัฒนา

1. สามารถใช้ภาษาในการฟัง พูด อ่าน เขียน ได้อย่างเหมาะสมและสื่อสารกับบุคคลอื่นได้อย่างมีประสิทธิภาพ
2. สามารถใช้เทคโนโลยีสารสนเทศในการสืบค้น ศึกษา ค้นคว้าด้วยตนเอง ติดต่อสื่อสารและนำเสนอข้อมูลในการอภิปรายหรือรายงาน และในชีวิตประจำวันได้ ได้อย่างมีประสิทธิภาพ
3. มีทักษะการวิเคราะห์เชิงตัวเลขที่เหมาะสม

5.2 วิธีการสอน

1. ให้นักศึกษาแลกเปลี่ยนความคิดเห็นและประสบการณ์ในชั้นเรียน นอกชั้นเรียน ระหว่างผู้เรียน ผู้สอน และผู้เกี่ยวข้องอื่นๆ
2. ให้นักศึกษาจัดทำรายงานกลุ่ม โดยรวบรวมข้อมูลจากเอกสารตามแหล่งข้อมูลเทคโนโลยีสารสนเทศและการสื่อสารที่หลากหลายและเหมาะสม
3. นำเสนอรายงานและอภิปรายสถานการณ์ โดยส่งเสริมให้นักศึกษาใช้เทคโนโลยีสารสนเทศ และนวัตกรรมที่หลากหลายและเหมาะสมร่วมกันในชั้นเรียน
4. จัดประสบการณ์ให้ผู้เรียนนำเสนอผลงานโดยใช้เทคโนโลยีสารสนเทศทางคณิตศาสตร์และสถิติ
5. ให้นักศึกษาเข้าร่วมหรือจัดสัมมนาทางวิชาการหรือฝึกอบรมด้านความมั่นคงของระบบเครือข่าย

5.3 วิธีการประเมินผล

1. ประเมินจากการอภิปรายร่วมกันในชั้นเรียน
2. ประเมินจากประสิทธิผลของการแลกเปลี่ยนข้อคิดเห็น ประสบการณ์และรายงานกลุ่ม
3. ความสามารถในการใช้เทคโนโลยีสารสนเทศ
4. ความสามารถในการใช้ทักษะทางคณิตศาสตร์และสถิติเพื่ออธิบาย อภิปราย และนำเสนอผลงานได้อย่างเหมาะสม
5. ประเมินจากคำตอบข้อสอบเชิงวิเคราะห์

หมวดที่ 5 แผนการสอนและการประเมินผล

1. แผนการสอน

ลำดับที่	หัวข้อ/รายละเอียด	จำนวน ชั่วโมง	กิจกรรมการเรียนการสอน/สื่อที่ใช้
1	แนะนำรายวิชา <ul style="list-style-type: none"> • ทดสอบก่อนเรียน • อธิบาย มคอ.3 • อธิบายเนื้อหาและระบบการเรียนรู้ • การวัดและการประเมินผลการเรียน การประเมินทักษะด้านความมั่นคงของระบบเครือข่าย	4	<ul style="list-style-type: none"> - ทดสอบก่อนเรียนด้วยข้อสอบปรนัย จำนวน 60 ข้อ - มคอ.3 - อธิบายเนื้อหาของบทเรียน - บรรยายและอภิปรายกลุ่ม กิจกรรมเพื่อประเมินทักษะด้านความมั่นคงของระบบเครือข่ายของผู้เรียน
2	ความมั่นคงปลอดภัยของระบบเครือข่าย	4	<ul style="list-style-type: none"> - บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย
3	การรักษาความมั่นคงปลอดภัยของระบบเครือข่าย	4	<ul style="list-style-type: none"> - บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย
4	ภัยคุกคามความมั่นคงปลอดภัยของระบบเครือข่าย	4	<ul style="list-style-type: none"> - บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - มอบหมายหัวข้อให้ศึกษาค้นคว้าและนำเสนอหน้าชั้นเรียน
5	วิทยาการรหัสลับ	4	<ul style="list-style-type: none"> - บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - ฝึกปฏิบัติการเข้ารหัสลับข้อมูล
6	ความมั่นคงปลอดภัยของเว็บ (Web)	4	<ul style="list-style-type: none"> - บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - ปฏิบัติการใช้ซอฟต์แวร์ด้านความมั่นคงปลอดภัยของระบบเครือข่าย
7	ความมั่นคงปลอดภัยของระบบเครือข่ายท้องถิ่น (LAN)	4	<ul style="list-style-type: none"> - บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - ปฏิบัติการใช้ซอฟต์แวร์ด้านความมั่นคงปลอดภัยของระบบเครือข่าย
8	สอบกลางภาค	2	
9	ความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย (Wireless LAN)	4	<ul style="list-style-type: none"> - บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - ปฏิบัติการใช้ซอฟต์แวร์ด้านความมั่นคง

			ปลอดภัยของระบบเครือข่าย
10	ไฟร์วอลล์ (Firewall)	4	- บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - ปฏิบัติการใช้ซอฟต์แวร์ด้านความมั่นคงปลอดภัยของระบบเครือข่าย
11	การเจาะระบบเครือข่ายและการป้องกัน	4	- บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - ปฏิบัติการใช้ซอฟต์แวร์ด้านความมั่นคงปลอดภัยของระบบเครือข่าย
12	ระบบตรวจจับผู้บุกรุก	4	- บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - ปฏิบัติการใช้ซอฟต์แวร์ด้านความมั่นคงปลอดภัยของระบบเครือข่าย
13	ความปลอดภัยของวินโดวส์ (Windows)	4	- บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - ปฏิบัติการใช้ซอฟต์แวร์ด้านความมั่นคงปลอดภัยของระบบเครือข่าย
14	ความมั่นคงปลอดภัยทางกายภาพและการจัดเก็บข้อมูลการจราจรของระบบเครือข่าย	4	- บรรยายและอภิปรายกลุ่ม - ศึกษาค้นคว้าด้วยตนเองผ่านระบบเครือข่ายคอมพิวเตอร์ และสื่อการเรียนที่หลากหลาย - ฝึกอบรมและบรรยายความมั่นคงปลอดภัยทางกายภาพ โดยวิทยากร
15	นำเสนอรายงาน	4	นำเสนอรายงานกลุ่มจากการศึกษาดูงานด้านความมั่นคงปลอดภัยของระบบเครือข่าย
16	สอบปลายภาค	2	ทดสอบหลังเรียน

2. แผนการประเมินผลการเรียนรู้

กิจกรรมที่	ผลการเรียนรู้	วิธีการประเมิน	สัปดาห์ที่ประเมิน	สัดส่วนของการประเมินผล
1	1.1, 2.1, 3.1, 4.1	<p>พฤติกรรมการเรียนรู้</p> <ul style="list-style-type: none"> - การเข้าชั้นเรียน - การมีส่วนร่วมอภิปราย และเสนอความคิดเห็นในชั้นเรียน - การตรงต่อเวลา - ความมีวินัย - บุคลิกภาพ <p>การทำงานที่ได้รับมอบหมาย</p> <ul style="list-style-type: none"> - รายงานการศึกษาค้นคว้า, งานที่ได้รับมอบหมาย และการนำเสนอ - การฝึกปฏิบัติ และการทดสอบปฏิบัติ 	ตลอดภาคการศึกษา	<p>10 %</p> <p>(50%) (20%)</p> <p>(30%)</p>
3	1.1, 2.1, 3.1, 4.1, 5.1	สอบปลายภาค	16	40 %

หมวดที่ 6 ทรัพยากรประกอบการเรียนการสอน

1. เอกสารและตำราหลัก

จิระ จิตสุภา. (2555). ความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ เอกสารประกอบการสอน.

มหาวิทยาลัยราชภัฏสวนดุสิต.

จตุชัย แพงจันทร์. (2553). Master in Security (2nd ed.). นนทบุรี: ไอทีซี พรีเมียร์.

ธวัชชัย ชมศิริ. (2553). ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์. กรุงเทพฯ: โปริวิชั่น.

พนิดา พานิชกุล. (2553). ความมั่นคงปลอดภัยของสารสนเทศและการจัดการ. กรุงเทพฯ: เคทีพี แอนด์คอนซัลท์.

2. เอกสารและข้อมูลสำคัญ

นฤมล สอาดโฉม. (2548). การบริหารความเสี่ยง Risk Management. กรุงเทพฯ. ก.พลพิมพ์ 1996.

ปริญญ์ เสรีพงศ์. (2551). ISO 27001 Introduction to Information Security Management System. กรุงเทพฯ: อมรินทร์พริ้นติ้งแอนด์พับลิชชิ่ง.

วรเศรษฐ์ สุวรรณิก. (2553). วิทยาการรหัสลับ Cryptography. กรุงเทพฯ: วรณิก.

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. (2552). ร่างแนวทางปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ. กรุงเทพฯ: ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ ประเทศไทย.

สุเมธ จิตภักดิ์ดินทร์. (2554). Hacking & Security ฉบับ ก้าวสู่ผู้ทดสอบและป้องกันการเจาะระบบ. กรุงเทพฯ: อีซีไอที บุ๊คส์.

สานนท์ ฉิมมณี และ ภส จันทศิริ. (2553). เอกสารประกอบการฝึกอบรมโครงการเสริมสร้างศักยภาพบุคลากร ICT ไทย ระยะที่ 1 หลักสูตรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบเครือข่ายและคอมพิวเตอร์ระดับที่ 3. กรุงเทพฯ: สำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.

สำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศ. (2553). เอกสารประกอบการฝึกอบรมโครงการเสริมสร้างศักยภาพบุคลากร ICT ไทย ระยะที่ 2 หลักสูตรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบเครือข่ายและคอมพิวเตอร์ระดับที่ 3. ปทุมธานี: สำนักพิมพ์มหาวิทยาลัย

3. เอกสารและข้อมูลแนะนำ

- เว็บไซต์ที่เกี่ยวกับหัวข้อในคำอธิบายรายวิชา

หมวดที่ 7 การประเมินและปรับปรุงการดำเนินการของรายวิชา

1. กลยุทธ์การประเมินประสิทธิผลของรายวิชาโดยนักศึกษา

การประเมินประสิทธิผลในรายวิชานี้ ที่จัดทำโดยนักศึกษาได้จัดกิจกรรมในการนำแนวคิดและความเห็นจากนักศึกษา ดังนี้ การสนทนากลุ่มระหว่างผู้สอนและผู้เรียน การสังเกตการณ์จากพฤติกรรมของผู้เรียน แบบประเมินผู้สอนที่จัดทำโดยมหาวิทยาลัยราชภัฏสวนดุสิต โดยให้นักศึกษาเข้าประเมินผลการเรียนการสอนทางเว็บไซต์ของระบบบริหารการศึกษ สำนักส่งเสริมวิชาการและงานทะเบียน และการจัดประเมินผู้สอนโดยใช้แบบประเมินของคณะวิทยาการจัดการ และผ่านทางเว็บบอร์ดที่อาจารย์ผู้สอนได้จัดทำเป็นช่องทางการสื่อสารกับนักศึกษา

2. กลยุทธ์การประเมินการสอน

- แลกเปลี่ยนข้อมูลการสอนกับผู้สอนรายวิชาเดียวกัน
- ผลการสอบ
- การทวนสอบผลประเมินการเรียนรู้

3. การปรับปรุงการสอน

หลังจากได้ผลการประเมินการสอนในข้อ 2 จึงมีการปรับปรุงการสอน โดยการจัดกิจกรรมในการระดมสมอง และหาข้อมูลเพิ่มเติมในการปรับปรุงการสอน และการวิจัยในชั้นเรียน

4. การทวนสอบมาตรฐานผลสัมฤทธิ์ของนักศึกษาในรายวิชา

ในระหว่างกระบวนการสอนรายวิชา มีการทวนสอบผลสัมฤทธิ์ในรายหัวข้อ ตามที่คาดหวังจากการเรียนรู้ในรายวิชา ได้จากการสอบถามนักศึกษา หรือการสุ่มตรวจผลงานของนักศึกษา รวมถึงพิจารณาจากผลการทดสอบย่อย และหลังการออกผลการเรียนรายวิชา มีการทวนสอบผลสัมฤทธิ์โดยรวมในวิชาได้ ดังนี้ การทวนสอบการให้คะแนนจากการสุ่มตรวจผลงานของนักศึกษาโดยอาจารย์ท่านอื่น หรือผู้ทรงคุณวุฒิที่ไม่ใช่อาจารย์ประจำวิชา

5. การดำเนินการทบทวนและการวางแผนปรับปรุงประสิทธิผลของรายวิชา

จากผลการประเมิน และทวนสอบผลสัมฤทธิ์ประสิทธิผลรายวิชา จะมีการวางแผนการปรับปรุงการสอนและรายละเอียดวิชา เพื่อให้เกิดคุณภาพมากขึ้น ดังนี้ ปรับปรุงรายวิชาทุกปี หรือตามข้อเสนอแนะปรับปรุงการสอนในข้อ 3 และผลการทวนสอบมาตรฐานผลสัมฤทธิ์ตามข้อ 4