แนวปฏิบัติการพัฒนาเว็บไซต์หน่วยงาน
ภายในมหาวิทยาลัยราชภัฏกำแพงเพชร
ให้สอดคล้องกับมาตรฐานเว็บไซต์ภาครัฐ

คณะผู้จัดทำ

ผศ.ดร.ฆัมภิชา ตันติสันติสม
อ.จินดาพร อ่อนเกตุ
อ.กนกวรรณ เขียววัน
น.ส.อรปรียา คำแพ่ง
นายวันเฉลิม พูนใจสม

มีนาคม 2562

คำนำ

การออกแบบเว็บไซต์สำหรับหน่วยงานภาครัฐ มีลักษณะเฉพาะที่แตกต่างจากการออกแบบเว็บไซต์ทั่วไป โดยเว็บไซต์หน่วยงานภาครัฐควรประกอบไปด้วยข้อมูล ข่าวสาร และรายละเอียดต่างๆ มากมายที่สมควรนำเสนอผ่านทางเว็บไซต์ การเพิ่มข้อมูลข่าวสารที่ไม่จำเป็นหรือไม่เหมาะสมจะส่งผลให้เกิดภาพลักษณ์ในแง่ลบต่อเว็บไซต์ของหน่วยงานได้ อีกทั้งการมุ่งเน้นความสวยงามและการดึงดูดผู้ใช้งานโดยละเลยการนำเสนอข้อมูลข่าวสารที่จำเป็น อาจส่งผลต่อการสื่อสารจากหน่วยงานไปยังผู้ใช้งานอื่นๆได้ เพื่อให้การออกแบบเว็บไซต์ของหน่วยงานมีความเหมาะสมและสอดคล้องกับมาตรฐานเว็บไซต์ภาครัฐ พ.ศ.2555 การศึกษาแนวปฏิบัตินี้จะช่วยให้ผู้ดูแลเว็บไซต์สามารถออกแบบและจัดการเว็บไซต์ของตนเองได้สะดวกยิ่งขึ้น

ผู้จัดทำ

มีนาคม 2562

สารบัญ

สารบัญภาพ

แนวปฏิบัติการพัฒนาเว็บไซต์หน่วยงานให้สอดคล้องกับมาตรฐานเว็บไซต์ภาครัฐ
มหาวิทยาลัยราชภัฏกำแพงเพชร

ในการออกแบบเว็บไซต์ของหน่วยงาน ใน**เว็บเพจหลัก (main web page**) ควรแบ่งออกเป็นอย่างน้อย 3 ส่วน ดังนี้

1. ส่วนบนของหน้า (header) ควรประกอบไปด้วย

1.1 สัญลักษณ์ที่ใช้ในการเลือกภาษาแสดงผล เช่น ภาษาไทย (TH) ภาษาอังกฤษ (ENG) หรือ 

1.2 สัญลักษณ์ที่ใช้ในการปรับขนาดตัวอักษร เช่น 

1.3 เว็บลิงค์ไปยังหน่วยงานย่อยที่สังกัดภายใต้หน่วยงานนั้นๆ

1.4 เว็บลิงค์ไปยังเว็บเพจเกี่ยวกับเรา (about us)

1.5 เว็บลิงค์ไปยังหน้าข้อมูลผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

1.6 ระบบสืบค้นข้อมูล (search engine) ให้สามารถสืบค้นข้อมูลที่อยู่ภายในหน่วยงานได้ (รายละเอียด หน้า 7)

1.7 เว็บลิงค์ไปยังหน้าแบบฟอร์มที่ดาวน์โหลดได้

1.8 เว็บลิงค์ไปยังหน้าคลังความรู้ (ถ้ามี)

1.9 กรณีที่เป็นหน่วยงานให้บริการแก่บุคคลอื่น เช่น สำนักส่งเสริมวิชาการและงานทะเบียน สำนักบริการวิชาการและจัดหารายได้ และศูนย์ส่งเสริมและตรวจสอบการผลิต ควรมีเว็บลิงค์ เชื่อมโยงไปยังหน้ารายละเอียดข้อมูลการให้บริการ

1.10 เว็บลิงค์ไปยังหน้าคำถามที่พบบ่อย (FAQ)

2. ส่วนเนื้อหา (body) หน้าหลักควรประกอบไปด้วยเนื้อหาดังนี้

2.1 ข่าวประชาสัมพันธ์ทั่วไป เรียงลำดับจากใหม่สุด ย้อนหลังไปยังเก่าสุด โดยให้ระบุวันที่ที่นำเสนอข่าวนั้นๆ ไว้ด้วย

2.2 ประกาศของหน่วยงาน เช่น ประกาศรับสมัครงาน การจัดซื้อจัดจ้าง การจัดฝึกอบรม เป็นต้น

2.3 ปฏิทินกิจกรรมของหน่วยงาน

นอกจากนี้ ในส่วนเนื้อหา ควรปรับรูปแบบการนำเสนอเนื้อหาซึ่งประกอบไปด้วย

1) การใช้งาน Really Simple Syndication (RSS) เพื่อการนำเสนอข่าวสารของหน่วยงาน

2) การนำเสนอในรูปแบบของเสียงและวิดีโอ เช่น Youtube นำเสนอหน่วยงาน เป็นต้น แต่ไม่ควรมีเสียงเพลงบรรเลงเป็นเบื้องหลังของเว็บเพจ เพื่อลดภาระการใช้งานแบนด์วิธ

3. ส่วนล่างของหน้า (footer) ควรประกอบไปด้วย

3.1 เมนูหลักในรูปแบบข้อความ

3.2 ลิงค์เชื่อมไปยังเว็บไซต์ภายนอกที่เกี่ยวข้องโดยตรง

3.3 ลิงค์เชื่อมไปยังเว็บไซต์อื่นๆ ที่น่าสนใจ

3.4 ข้อมูลติดต่อหน่วยงาน ได้แก่ ชื่อและที่อยู่ หมายเลขโทรศัพท์ หมายเลขโทรสาร และ email address

3.5 เว็บลิงค์เชื่อมไปยังหน้าประกาศคำสงวนลิขสิทธิ์ (copyright) (ตัวอย่างในภาคผนวก ก) ซึ่งทุกหน่วยงานสามารถเชื่อมโยงมายังหน้าดังกล่าวของมหาวิทยาลัยได้ที่

3.6 เว็บลิงค์เชื่อมไปยังหน้าประกาศการปฏิเสธความรับผิด (disclaimer) (ตัวอย่างในภาคผนวก ข) ซึ่งทุกหน่วยงานสามารถเชื่อมโยงมายังหน้าดังกล่าวของมหาวิทยาลัยได้ที่

3.7 เว็บลิงค์เชื่อมไปยังหน้าประกาศนโยบายเว็บไซต์ (website policy) (ตัวอย่างในภาคผนวก ค) ซึ่งทุกหน่วยงานสามารถเชื่อมโยงมายังหน้าดังกล่าวของมหาวิทยาลัยได้ที่

3.8 เว็บลิงค์เชื่อมไปยังหน้าประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) (ตัวอย่างในภาคผนวก ง) ซึ่งทุกหน่วยงานสามารถเชื่อมโยงมายังหน้าดังกล่าวของมหาวิทยาลัยได้ที่

3.9 เว็บลิงค์เชื่อมไปยังหน้าประกาศนโยบายการรักษาความมั่นคงปลอดภัยของเว็บไซต์ (website security policy) (ตัวอย่างในภาคผนวก จ) ซึ่งทุกหน่วยงานสามารถเชื่อมโยงมายังหน้าดังกล่าวของมหาวิทยาลัยได้ที่ http://www.kpru.ac.th/files/banner-network-security-kpru-2017.pdf

3.10 เว็บลิงค์เชื่อมไปยังหน้ากฎ ระเบียบ ข้อบังคับที่เกี่ยวข้องกับหน่วยงาน

3.11 ผังเว็บไซต์ ที่สร้างในรูปแบบของ sitemap.xml

3.12 เว็บลิงค์ถาม/ตอบ เพื่อให้ผู้ใช้บริการสามารถสอบถามข้อมูล หรือข้อสงสัยได้ เช่น email หรือ web board เป็นต้น อย่างไรก็ตาม กรณีที่ใช้ web board ในการถาม/ตอบ ควรกำหนดให้ผู้ดูแลเว็บไซต์เป็นผู้อนุญาตให้แสดงผลคำถาม/คำตอบเท่านั้น ไม่ควรอนุญาตให้ผู้รับบริการสามารถแสดงข้อความใน web board ได้โดยทันที

3.13 ช่องทางการติดต่อสื่อสารอื่นๆ ระหว่างผู้ใช้และหน่วยงาน เช่น Facebook Twitter email SMS web board เป็นต้น

3.14 ช่องทางรับเรื่องร้องเรียน และติดตามสถานะเรื่องร้องเรียน เช่น สายตรงอธิการบดี เป็นต้น

3.15 แบบสำรวจออนไลน์ เพื่อใช้ในการส ารวจความพึงพอใจของการใช้บริการเว็บไซต์ หรือการสำรวจความคิดเห็นของผู้ใช้งาน (online poll) หรือ การออกเสียงลงคะแนนต่างๆ (online voting) โดยให้พิจารณาจากความจำเป็นและความเหมาะสมในแต่ละแบบสำรวจ

นอกจากนี้ ในส่วน**หน้าอื่นๆ ของเว็บไซต์** ควรใช้รูปแบบที่ใกล้เคียงกับหน้าหลัก โดยเพิ่มเติมส่วนของ

1. ส่วนบนของหน้า (header) ควรสร้างส่วน navigation ที่ระบุต าแหน่งของเว็บเพจในเว็บไซต์หน่วยงานนั้นๆ เช่น

หน้าหลัก > สำหรับบุคลากร > e-university เป็นต้น

2. ส่วนลิงค์เชื่อมโยงกลับไปยังหน้าหลักของเว็บไซต์ ซึ่งอาจอยู่ในรูปของลิงค์ข้อความหรือลิงค์รูปภาพก็ได้

เนื้อหาเกี่ยวกับหน่วยงาน (About Us) ควรประกอบไปด้วยเนื้อหาดังนี้

1. ประวัติความเป็นมา วิสัยทัศน์ และพันธกิจ
2. โครงสร้างหน่วยงาน ผู้บริหาร อำนาจหน้าที่
3. ภารกิจ และหน้าที่รับผิดชอบของหน่วยงาน
4. ยุทธศาสตร์ และแผนปฏิบัติราชการ
5. แผนงาน โครงการและงบประมาณรายจ่ายประจำปี
6. รายงานผลการปฏิบัติราชการ

ซึ่งอาจแยกหน้าเพจตามตัวอย่าง หรือจัดรูปแบบใหม่ แต่ให้มีเนื้อหาครบถ้วน

หน้าข้อมูลผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ควรประกอบไปด้วยเนื้อหาดังต่อไปนี้

1. ชื่อ-ตำแหน่ง ข้อมูลการติดต่อ (ที่อยู่ เบอร์โทรศัพท์ โทรสาร email) วิสัยทัศน์ และยุทธศาสตร์ ICT
2. นโยบายด้าน ICT เช่น นโยบายการบริหารจัดการด้าน ICT และนโยบายรวมทั้งมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน ICT
3. แผนแม่บท ICT และแผนปฏิบัติการ
4. ข่าวสารจาก CIO
5. ปฏิทินกิจกรรม CIO

ซึ่งอาจแยกหน้าเพจตามตัวอย่าง หรือจัดรูปแบบใหม่ แต่ให้มีเนื้อหาครบถ้วน

หน้ากฎ ระเบียบ ข้อบังคับที่เกี่ยวข้องกับหน่วยงาน ควรประกอบไปด้วยเนื้อหาดังต่อไปนี้ กรณีที่เป็นข้อมูลภายนอก ให้ระบุที่มาของข้อมูลที่นำมาเผยแพร่

1. กฎหมาย พระราชบัญญัติ พระราชกฤษฎีกา กฎกระทรวง และมติคณะรัฐมนตรีที่เกี่ยวข้อง
2. ประกาศ ระเบียบ มาตรฐาน
3. คู่มือ แนวปฏิบัติ

ซึ่งอาจแยกหน้าเพจตามตัวอย่าง หรือจัดรูปแบบใหม่ แต่ให้มีเนื้อหาครบถ้วน

หน้ารายละเอียดข้อมูลการบริการ ควรประกอบไปด้วยเนื้อหาดังต่อไปนี้

1. การบริการตามภารกิจของหน่วยงาน
2. ขั้นตอนการบริการ พร้อมทั้งคำอธิบาย ที่ระบุระยะเวลาในแต่ละขั้นตอน

หน้าแบบฟอร์มที่ดาวน์โหลดได้ ควรประกอบไปด้วยเนื้อหาดังต่อไปนี้

1. กลุ่มของรายการแบบฟอร์ม แบ่งตามประเภทที่เหมาะสม
2. รายการของแบบฟอร์มที่สามารถดาวน์โหลดได้ ทั้งในแบบไฟล์ Word และ PDF
3. เครื่องมือสำหรับค้นหาแบบฟอร์มที่ต้องการ

หน้าคลังความรู้ ควรประกอบไปด้วยเนื้อหาดังต่อไปนี้

1. ผลงานวิจัย บทความ กรณีศึกษา
2. E-book
3. คู่มือปฏิบัติงาน
4. ข้อมูลสถิติต่างๆ

ซึ่งข้อมูลทั้งหมดควรเป็นข้อมูลที่ผลิตเองภายใต้หน่วยงานนั้นๆ พร้อมทั้งระบุวัน เวลาที่สร้างผลงานเหล่านี้ เพื่อประโยชน์ในการนำข้อมูลไปใช้ต่อ

ใน**การพัฒนาเว็บไซต์โดยรวม** ควรพิจารณาประเด็นเพิ่มเติมดังต่อไปนี้

1. การพัฒนาเว็บไซต์ควรใช้ HTML อย่างน้อย 4.01 ซึ่งแนะนำว่าควรปรับให้เป็น HTML5 ในอนาคต
2. เครื่องมือสำหรับเก็บข้อมูลการเยี่ยมชมเว็บไซต์ โดยเก็บข้อมูลต่างๆ เช่น จำนวนครั้ง จำนวนหน้าความสนใจ และระยะเวลาที่ใช้งาน เป็นต้น ซึ่งผู้ดูแลเว็บไซต์อาจใช้เครื่องมือของ Google Analytics ในการรวบรวมข้อมูลดังกล่าว

3. การตั้งชื่อ directory และ file ควรใช้ชื่อที่สื่อความหมาย เป็นภาษาอังกฤษที่สั้น กระชับ ไม่ก่อให้เกิดความสับสน และไม่ใช้ภาษาคาราโอเกะ กรณีที่ตั้งชื่อไฟล์โดยใช้ภาษาอังกฤษมากกว่า 1 คำ ให้ใช้เครื่องหมาย – (hyphen) คั่นระหว่างคำ และไม่ควรใช้เครื่องหมาย _ (underscore) ในการตั้งชื่อไฟล์ นอกจากนี้ควรพิจารณาการเลือกใช้ keyword ของหน้าเพจนั้นๆ มาตั้งเป็นชื่อไฟล์เพื่อให้สอดคล้องกับการค้นหาของ search engine

4. ทุกลิงค์ต้องสามารถใช้งานได้ตลอดเวลา และสามารถเชื่อมโยงไปยังเอกสารที่ระบุได้เสมอ ซึ่งอาจตรวจสอบความพร้อมใช้งานได้ โดยใช้เครื่องมือในเว็บไซต์ เช่น http://www.deadlinkchecker.com เป็นต้น

5. กรณีที่ใช้ Cascade Style Sheets (CSS) ควรตรวจสอบว่าผ่านมาตรฐาน W3C ระดับ 1 ซึ่งอาจตรวจสอบความสอดคล้องกับมาตรฐาน โดยใช้เครื่องมือในเว็บไซต์ เช่น www.css-validator.org/ เป็นต้น

6. เว็บไซต์ควรมีความสอดคล้องข้อกำหนดการทำให้เนื้อหาเว็บสามารถเข้าถึงและใช้ประโยชน์ได้ รุ่น 2.0 (Thai Web Content Accessibility Guidelines 2.0: TWCAG 2.0) อย่างน้อยระดับ A ซึ่งอาจตรวจสอบความสอดคล้องโดยใช้เครื่องมือในเว็บไซต์ เช่น http://www.thaiwebaccessibility.com/validator เป็นต้น

การให้บริการในรูปแบบอิเล็กทรอนิกส์ (e-Service)

การให้บริการตามภารกิจหน่วยงานนั้น จะมีเฉพาะบางหน่วยงานที่ให้บริการแก่ผู้ใช้โดยตรงเท่านั้น เช่น สำนักส่งเสริมวิชาการและงานทะเบียน สถาบันวิจัยและพัฒนา (ในส่วนของการจัดการประชุมวิชาการระดับชาติ) และคณะวิทยาศาสตร์และเทคโนโลยี (ในส่วนของการลงทะเบียนการแข่งขันงานสัปดาห์วิทยาศาสตร์แห่งชาติ) ศูนย์คอมพิวเตอร์ (ในส่วนของการสอบมาตรฐานคอมพิวเตอร์) เป็นต้น

การให้บริการอาจพิจารณาในรูปแบบต่างๆ ดังนี้

1. การลงทะเบียนออนไลน์ (online registration) ควรมีความสามารถดังต่อไปนี้

1.1 กำหนดหน้าเว็บในการใช้งานผ่านชื่อผู้ใช้บริการและรหัสผ่าน (username and password)

1.2 ระบบมีการตรวจสอบและยืนยันตัวตนในการใช้งาน พร้อมทั้งให้แจ้งเตือนกรณีที่ชื่อผู้ใช้หรือรหัสผ่านไม่ถูกต้อง

1.3 ระบบสามารถจัดการกรณีผู้ใช้งานลืมรหัสผ่าน โดยส่งรหัสผ่านให้ใหม่ตามช่องทางที่กำหนดไว้เพื่อความปลอดภัยของข้อมูลได้

2. E-Forms/ Online Forms ควรมีความสามารถดังต่อไปนี้

2.1 ส่วนให้บริการควรบันทึกข้อมูลในแบบฟอร์มออนไลน์ได้ โดยไม่ต้องดาวน์โหลดเอกสารมาพิมพ์ แล้วกรอกส่งในรูปแบบกระดาษได้

2.2 การให้บริการในส่วนนี้ อาจพัฒนาต่อไปยังหน่วยงานอื่นๆ ที่ให้บริการแก่หน่วยงานภายในด้วยกัน เช่น งานกองกลาง งานการเงิน งานการเจ้าหน้าที่ งานจัดหารายได้ งานไฟฟ้า งานพัสดุ และงานธุรการ เป็นต้น

3. ระบบให้บริการในรูปแบบอิเล็กทรอนิกส์ (e-Service) โดยพิจารณาตามความเหมาะสมของภารกิจหน่วยงาน ซึ่งอาจพิจารณาตัวอย่างดังนี้

3.1 ระบบการจองห้องประชุม ระบบการสั่งซื้อสินค้าและของที่ระลึก ระบบการสั่งจองชุดครุย ระบบการจองเวลานวดแผนไทย ระบบการสมัครเรียนหลักสูตรระยะสั้นของสำนักบริการวิชาการและจัดหารายได้

3.2 ระบบ e-Student ของสำนักส่งเสริมวิชาการและงานทะเบียน ทั้งในส่วนของนักศึกษาและอาจารย์ผู้สอน

3.3 ระบบการส่งและจัดการบทความในงานประชุมวิชาการระดับชาติ ของสถาบันวิจัยและพัฒนา

3.4 ระบบการจัดการแข่งขันกิจกรรมต่างๆ ในงานสัปดาห์วิทยาศาสตร์แห่งชาติ ของคณะวิทยาศาสตร์และเทคโนโลยี ซึ่งอาจรวมไปถึงการลงทะเบียนแข่งขัน การกรอกคะแนนผลการแข่งขันโดยคณะกรรมการ การประกาศผลการแข่งขัน และการพิมพ์เกียรติบัตร เป็นต้น

4. **การให้บริการในรูปแบบเฉพาะบุคคล (personalized e-Service)** อาจพิจารณาตามความเหมาะสมของภารกิจหน่วยงาน ซึ่งอาจพิจารณาการดำเนินงานดังนี้

4.1 การส่งข้อมูลเป็นรายบุคคลให้กับผู้ลงทะเบียน

4.2 ผู้ใช้บริการสามารถกำหนดรูปแบบข้อมูลที่ต้องการ และจัดอันดับเนื้อหาที่สนใจได้

4.3 การปรับปรุงแฟ้มข้อมูลของผู้ลงทะเบียนแบบอัตโนมัติ ตามพฤติกรรมของผู้ใช้บริการ

4.4 การนำเสนอข่าว/ข้อมูล/บริการที่ผู้ใช้บริการเข้ามาใช้งานครั้งล่าสุดได้ (last visit)

4.5 การปรับปรุงการให้บริการของหน่วยงานผ่านทางเว็บไซต์ จากการวิเคราะห์พฤติกรรมของผู้ใช้บริการ

4.6 ระบบรายงานที่สามารถเปลี่ยนแปลงไปตามข้อมูลที่ได้รับจากพฤติกรรมของผู้ใช้บริการและสามารถปรับเปลี่ยนรูปแบบรายงานได้ตามความต้องการ (dynamic report)

นอกจากนี้ ผู้ดูแลเว็บไซต์ควรพิจารณาประเด็นเพิ่มเติม กรณีที่พัฒนาแอพพลิเคชันขึ้นมาด้วยดังต่อไปนี้

1. แอพพลิเคชันให้บริการกับแอพพลิเคชันภายในหน่วยงาน

2. แอพพลิเคชันให้บริการกับแอพพลิเคชันของหน่วยงานอื่น

3. การตรวจสอบความถูกต้อง ครบถ้วนของข้อมูล รวมทั้งเงื่อนไขที่จำเป็นต่างๆ ก่อนการส่งข้อมูลบันทึกในระบบผ่านแบบฟอร์ม

4. การเข้ารหัสข้อมูล (encryption) เพื่อเพิ่มความปลอดภัยในการสื่อสาร เช่น Secure Socket Layer (SSL) หรือ https เป็นต้น

5. การระบุและยืนยันตัวตนโดยเลือกใช้เทคโนโลยีที่เหมาะสม เช่น การเข้าสู่ระบบต่างๆ ด้วยการล็อกอินเพียงครั้งเดียว (single sign-on)

6. เครื่องมือแนะนำการใช้งาน (Help) หรือคำอธิบาย content ต่างๆ เพื่ออำนวยความสะดวกในการใช้งาน ซึ่งอาจอยู่ในรูปของ tool tips, pop-up หรือหน้าเว็บคู่มือการใช้งาน เป็นต้น

ระบบสืบค้นข้อมูล (search engine)

สามารถสร้างโดยใช้ code ดังต่อไปนี้ เพื่อเชื่อมโยงกับ Google ในการค้นหาข้อมูลภายใน เว็บไซต์ที่ต้องการ

```
<form method="get" action="http://www.google.co.th/custom" target="_blank">
<table>
   <tr>
      <td>
                  <input type="hidden" name="kpru-domains" value="www.kpru.ac.th"/>
                  <input name="q" class="form-control" id="kpru-keyword"
placeholder="พิมพ์ค าค้นที่นี่" type="text">
      </td>
      <td>
         <button class="btn" type="submit" name="kpru-submit" value="Google_Search"
id="sbb"> ค้นหา</button>
         <input type="hidden" name="hl" value="th"/>
         <input type="hidden" name="sitesearch" value="www.kpru.ac.th"
checked="checked" id="ss1"/>
      </td>
   </tr>
</table>
</form>
```

1

2

ภาพที่ 1 ตัวอย่าง code ส าหรับการค้นหาข้อมูลภายในเว็บไซต์

โดยให้ผู้ดูแลเว็บไซต์แต่ละหน่วยงาน ปรับแก้ค่า value ในต าแหน่งที่ 1 และ 2 ให้เป็น URL ของหน่วยงานตนเองแทน

การสร้าง XML Sitemap

การสร้าง XML Sitemap ให้กับเว็บไซต์มีด้วยกัน 2 ส่วน

ส่วนที่ 1 การสร้างไฟล์ XML Sitemap

ส่วนที่ 2 การยืนยันไฟล์ XML Sitemap ให้กับ Google

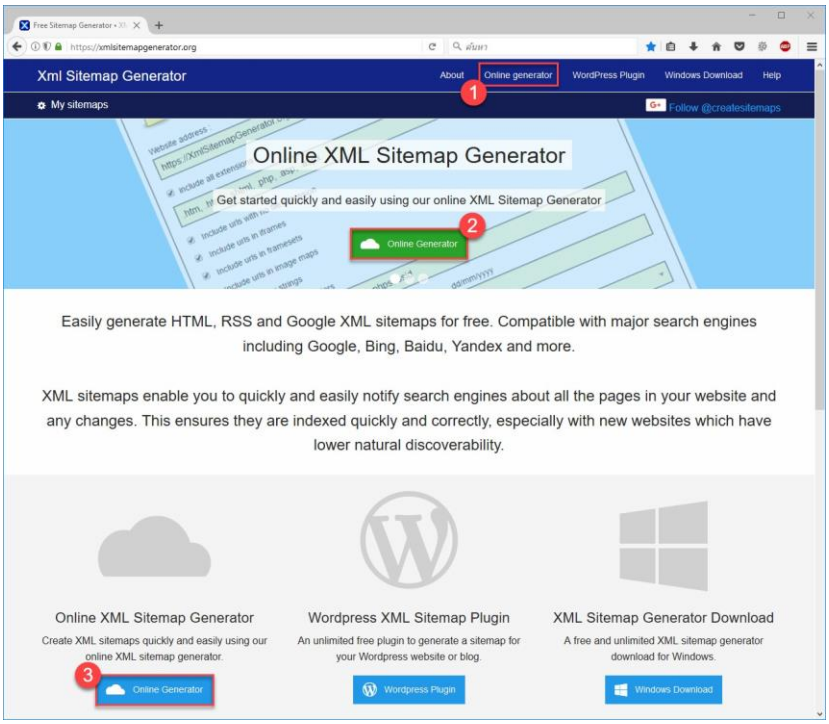
ส่วนที่ 1 การสร้าง XML Sitemap

การสร้าง XML Sitemap จากเว็บไซต์ที่ให้บริการโดยมีทั้งให้บริการฟรีและไม่ฟรี แต่จะต้องเป็นไปตามเงื่อนไขที่กำหนดไว้ของแต่ละเว็บไซต์ เช่น การจำกัดจำนวนเว็บเพจในการสร้าง XML Sitemap และหากต้องการใช้งานแบบไม่มีการจำกัดจะต้องเสียค่าใช้จ่าย

ในที่นี้ขอยกตัวอย่างเว็บไซต์ที่ให้บริการฟรี คือ https://xmlsitemapgenerator.org เนื่องจากเป็นเว็บไซต์จากองค์กรอิสระที่ไม่แสวงหาผลกำไร (.org) ที่ให้บริการฟรีไม่ต้องเสียค่าใช้จ่าย มีการบริการในรูปแบบออนไลน์ แบบลงทะเบียนสมาชิกและไม่ต้องลงทะเบียนสมาชิก แต่มีการจำกัดจำนวนเว็บเพจ 2,000 เพจ และแบบโปรแกรมสำเร็จรูปสำหรับติดตั้งในเครื่องคอมพิวเตอร์ ซึ่งสามารถใช้งานได้แบบ Unlimited คือ ไม่จำกัดจำนวนเว็บเพจ

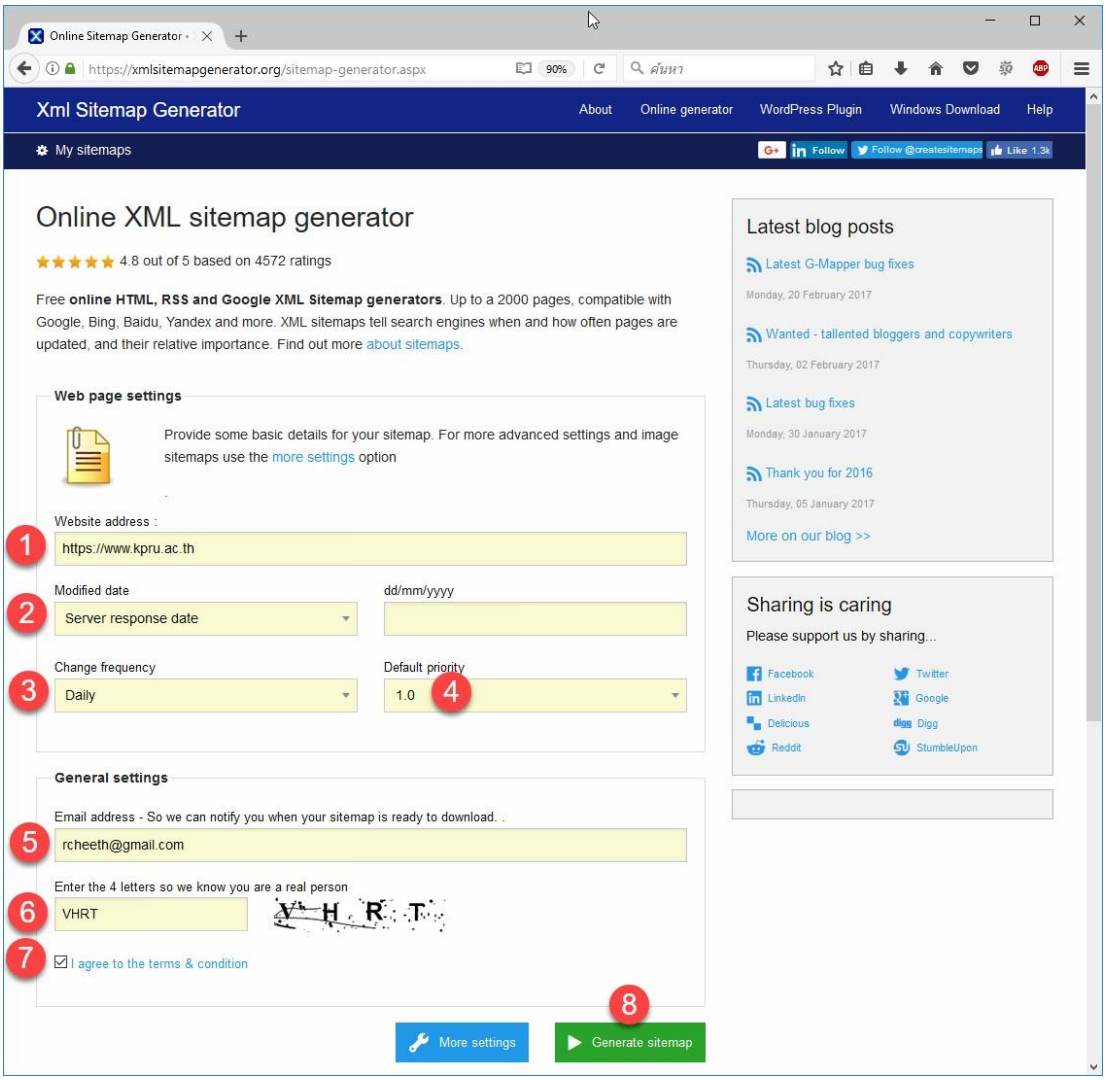
การสร้าง XML Sitemap แบบออนไลน์ โดยไม่ลงทะเบียนเป็นสมาชิก

1. เข้าสู่เว็บไซต์ https://xmlsitemapgenerator.org คลิกที่เมนู **Online generator** มี 3 จุด ดังภาพที่ 2



ภาพที่ 2 หน้าจอเว็บไซต์ https://xmlsitemapgenerator.org

2. กรอกข้อมูลรายละเอียดส าหรับสร้าง XML sitemap ของเว็บไซต์ ดังภาพที่ 3



ภาพที่ 3 หน้าจอการตั้งค่าเพื่อสร้าง sitemap

หมายเลข 1 คือ URL ของเว็บไซต์

หมายเลข 2 คือ วันที่ล่าสุดที่มีการปรับปรุงข้อมูล

หมายเลข 3 คือ ความถี่ของการปรับปรุงข้อมูล

หมายเลข 4 คือ การกำหนดความสำคัญของเพจเริ่มจาก 0-1

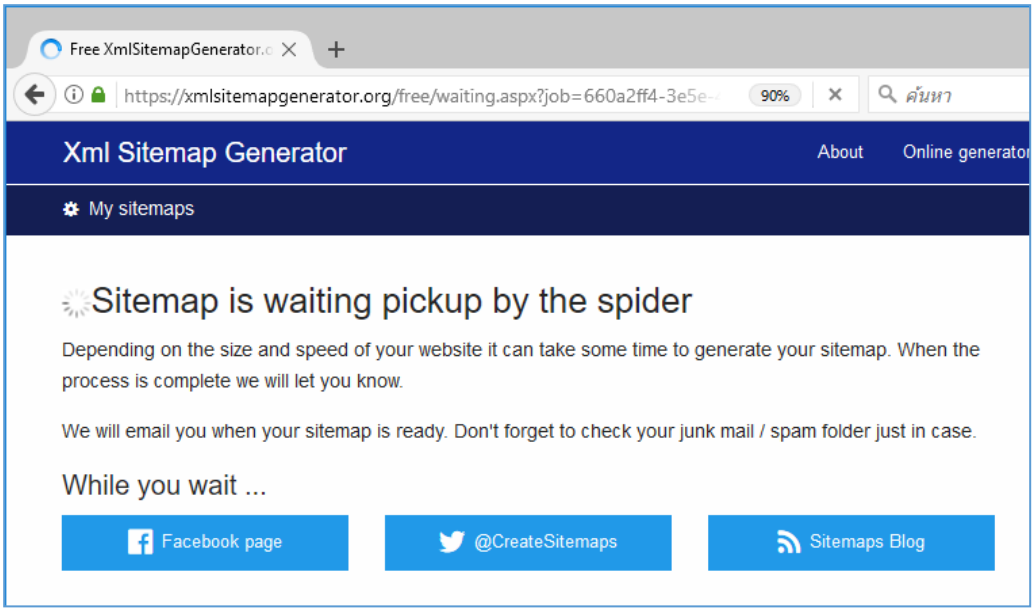
หมายเลข 5 คือ email สำหรับการรับแจ้งข้อความจากผู้ให้บริการ

หมายเลข 6 คือ การยืนยันตัวตนว่าเป็นผู้ใช้งานจริง

หมายเลข 7 คือ ทำเครื่องหมายถูกเพื่อยอมรับเงื่อนไขของผู้ให้บริการ

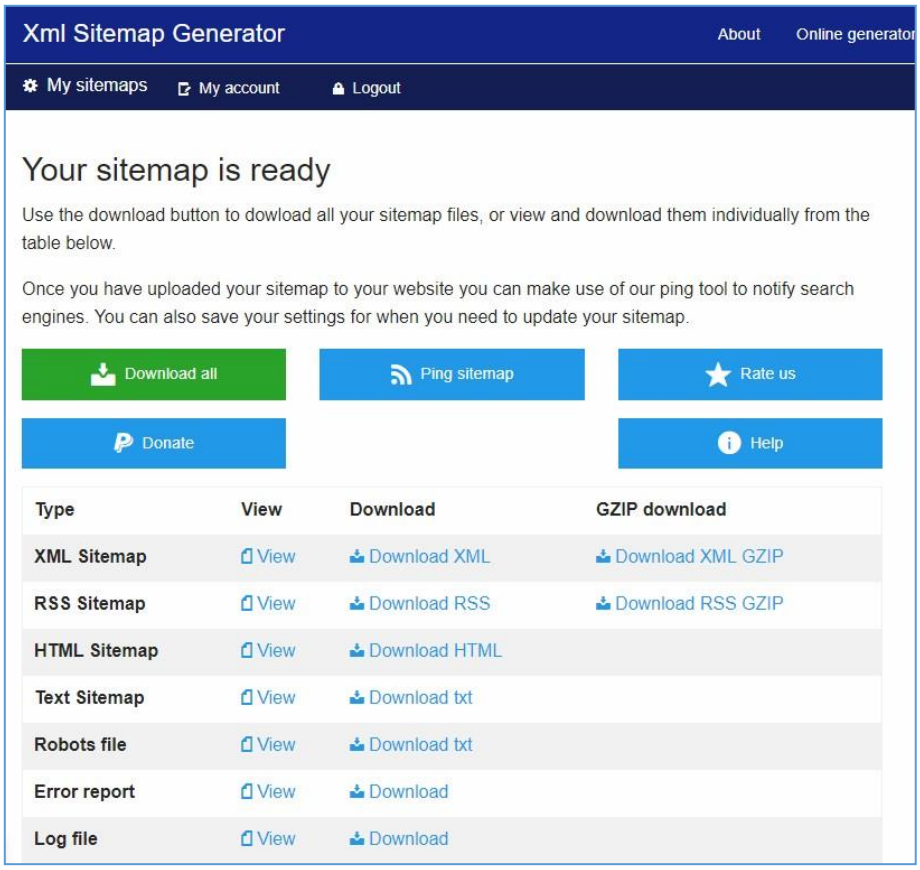
หมายเลข 8 คือ ปุ่มคำสั่งให้ประมวลผล XML Sitemap

3. ระบบจะประมวลผลการสร้าง XML Sitemap แบบออนไลน์ โดยเวลาในการประมวลผลจะมากหรือน้อย ขึ้นอยู่กับปัจจัยพื้นฐาน คือ ความเร็วของระบบเครือข่ายอินเทอร์เน็ต และจำนวนเว็บเพจของแต่ละเว็บไซต์



ภาพที่ 4 หน้าจอเว็บไซต์ขณะประมวลผลเพื่อสร้าง sitemap

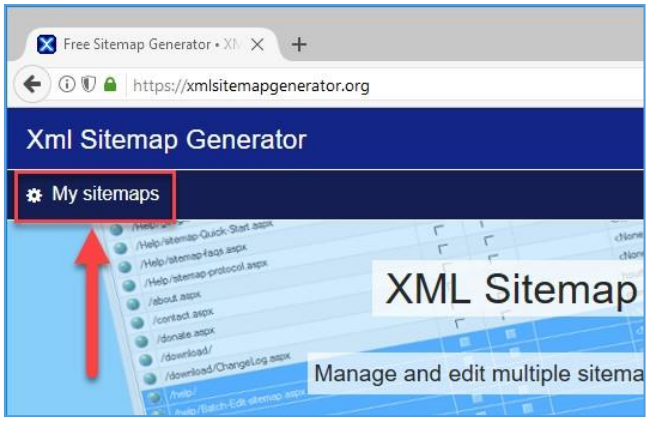
4. เมื่อประมวลผลเสร็จเรียบร้อยแล้ว จะแสดงรายละเอียดและไฟล์ sitemap.xml และอื่นๆ จากนั้นสามารถดาวน์โหลดไฟล์ต่างๆ ไปใช้งานต่อไป ดังภาพที่ 5



ภาพที่ 5 หน้าจอเว็บไซต์เมื่อการสร้าง sitemap เสร็จสิ้น

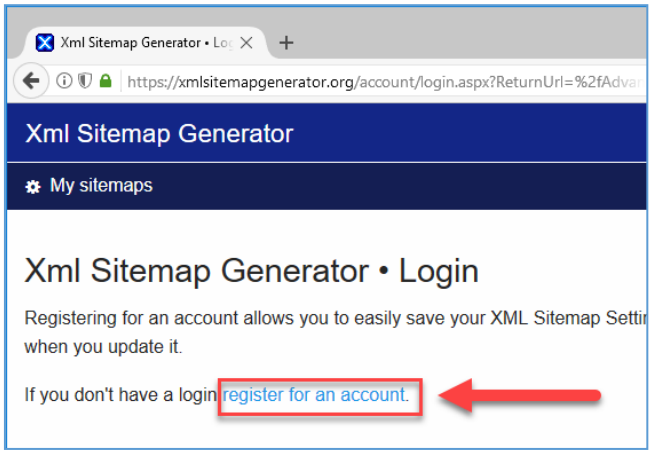
การสร้าง XML Sitemap แบบออนไลน์ โดยลงทะเบียนเป็นสมาชิก

1. คลิกที่เมนู **My sitemap**



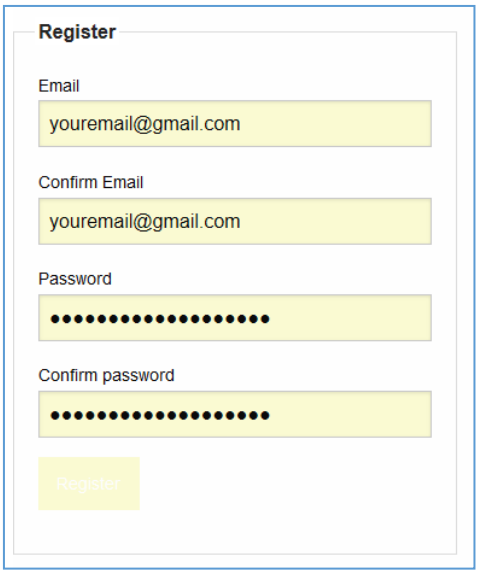
ภาพที่ 6 ส่วนของหน้าสำหรับการลงทะเบียนสมาชิกเพื่อสร้าง sitemap

2. คลิกที่เมนู register for an account



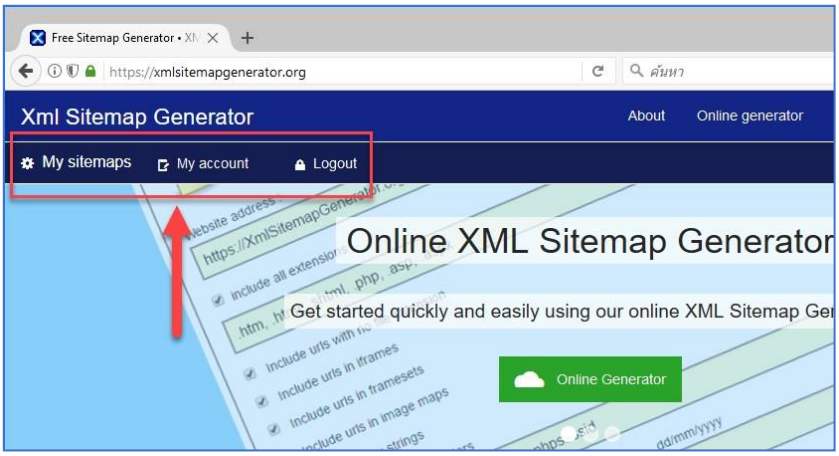
ภาพที่ 7 ส่วนของหน้าจอสำหรับการลงทะเบียนสมาชิก

3. กรอกข้อมูลในฟอร์ม **Register**



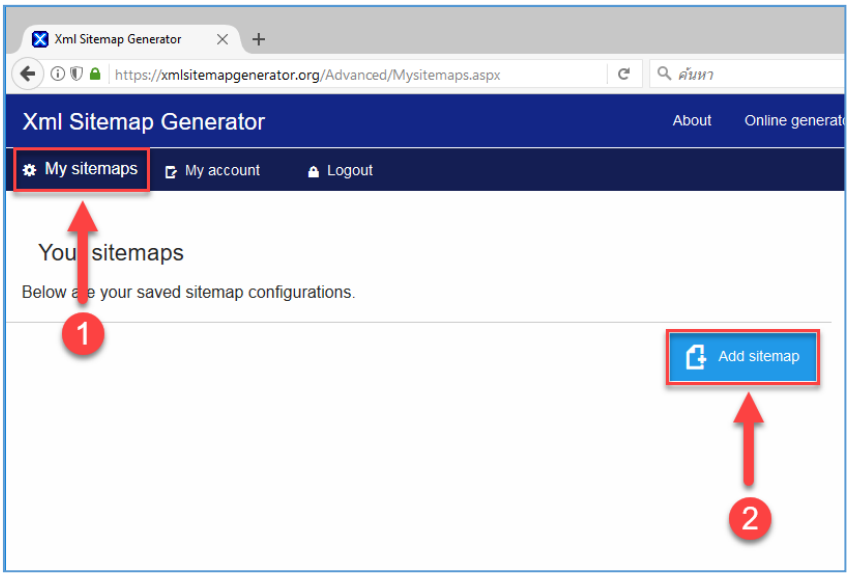
ภาพที่ 8 ส่วนของหน้าจอส าหรับการกรอกข้อมูลการลงทะเบียนสมาชิก

4. เมื่อลงทะเบียนแล้ว ระบบจะ Login เข้าใช้งานโดยอัตโนมัติ และจะเห็นเมนูส าหรับ Account ดังภาพที่ 9



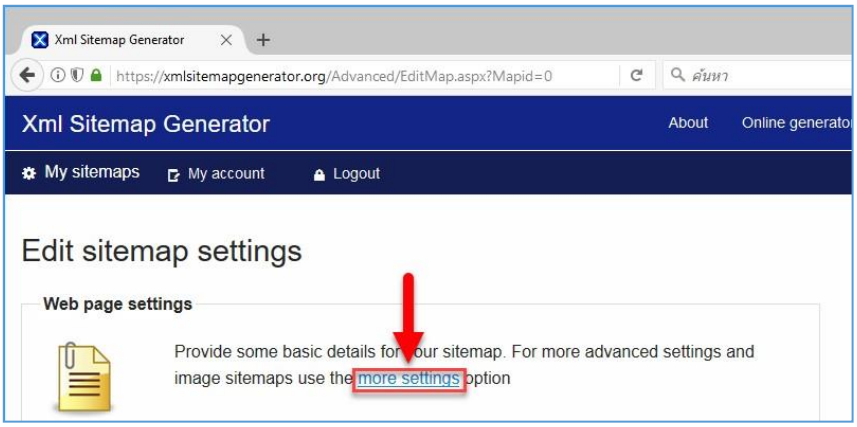
ภาพที่ 9 ส่วนของหน้าจอเว็บไซต์ เมื่อผ่านการ login เข้ามาใช้งาน

5. เพิ่ม sitemap โดยคลิกที่เมนู **My sitemap** และ คลิกที่ปุ่ม **Add sitemap**



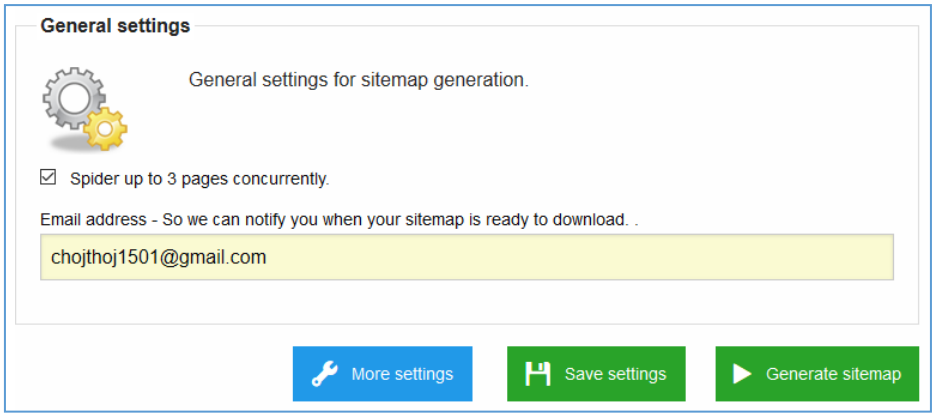
ภาพที่ 10 หน้าจอเว็บไซต์ส าหรับการเพิ่ม sitemap

6. จะแสดงฟอร์มสำหรับกรอกข้อมูลเพื่อกำหนดค่าให้กับ sitemap และหากต้องการการกำหนดค่าอื่นๆ เพิ่มเติม ให้คลิกที่ข้อความลิงค์ **more settings**



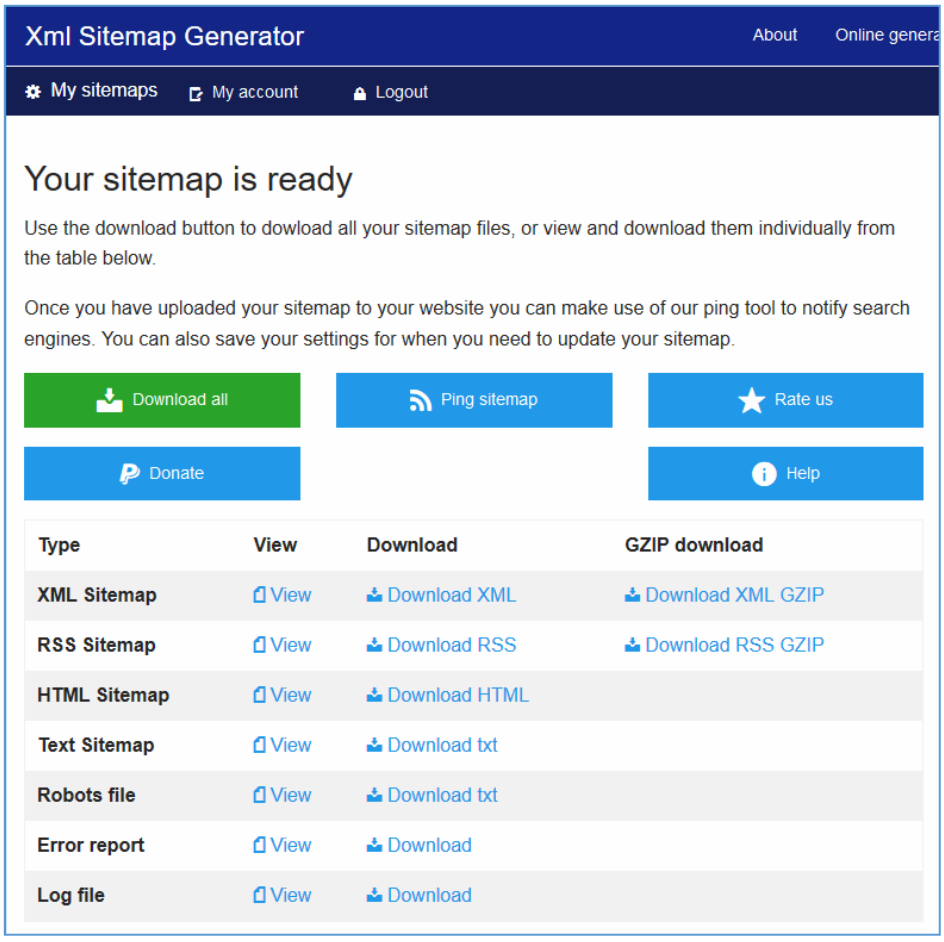
ภาพที่ 11 ส่วนของหน้าจอเว็บไซต์ ส าหรับการก าหนดค่า sitemap

7. กรอกข้อมูลตามฟอร์มให้ครบถ้วน จากนั้นคลิกที่ปุ่ม **Save settings** เพื่อบันทึกค่า และคลิกที่ปุ่ม **Generate sitemap** เพื่อท าการประมวลผล sitemap



ภาพที่ 12 ส่วนของหน้าจอเว็บไซต์ส าหรับการประมวลผลเพื่อสร้าง sitemap

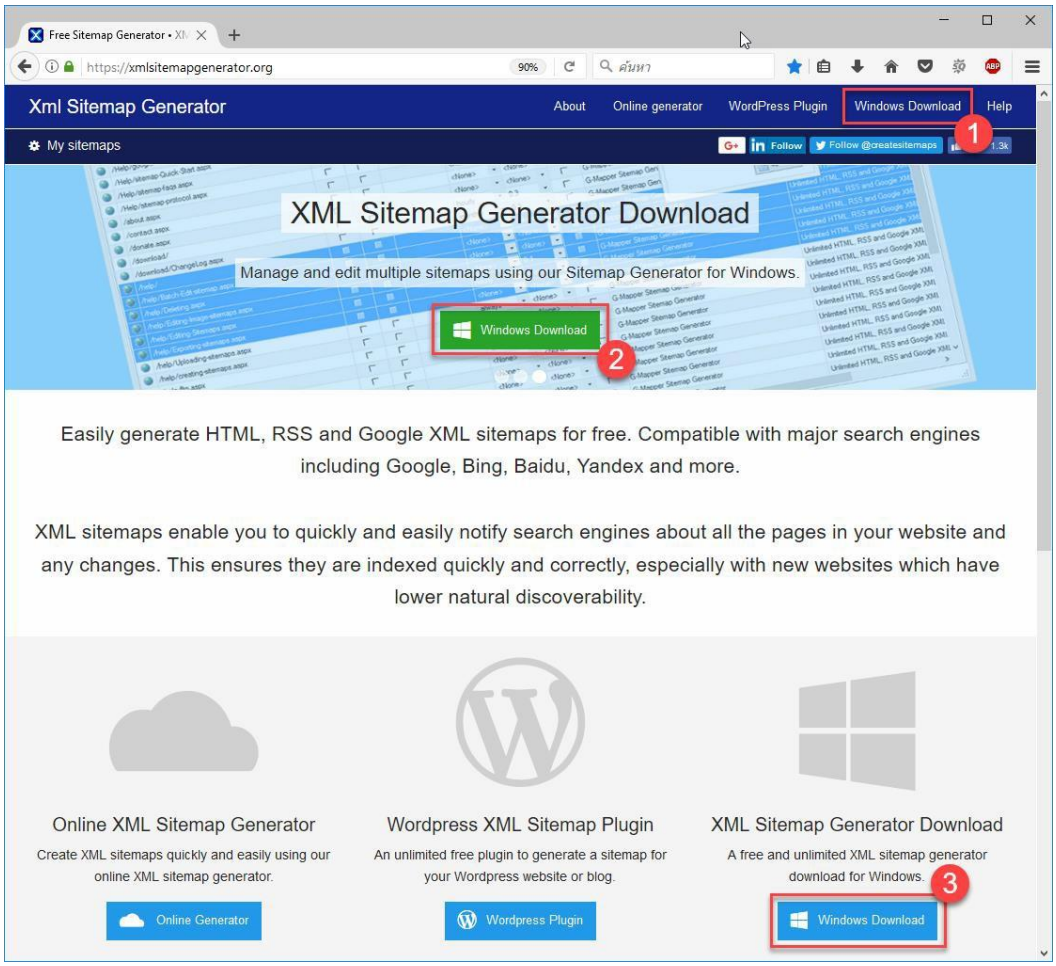
8. เมื่อประมวลผลเสร็จเรียบร้อยแล้ว จะได้ sitemap แบบต่างๆ สามารถดาวน์โหลดไปใช้งานได้ทันที ดังภาพที่ 13



ภาพที่ 13 หน้าจอเว็บไซต์เมื่อการสร้าง sitemap แบบลงทะเบียน เสร็จสิ้น

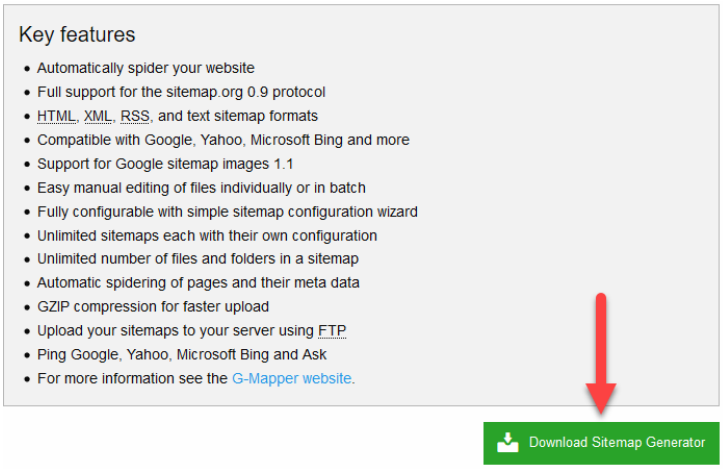
การสร้าง XML Sitemap ด้วยโปรแกรมสำเร็จรูป gmapper

1. เข้าเว็บไซต์ **https://xmlsitemapgenerator.org** คลิกที่เมนู **Windows Download** โดยมี 3 จุด สามารถคลิกที่จุดใดจุดหนึ่ง ดังภาพที่ 14



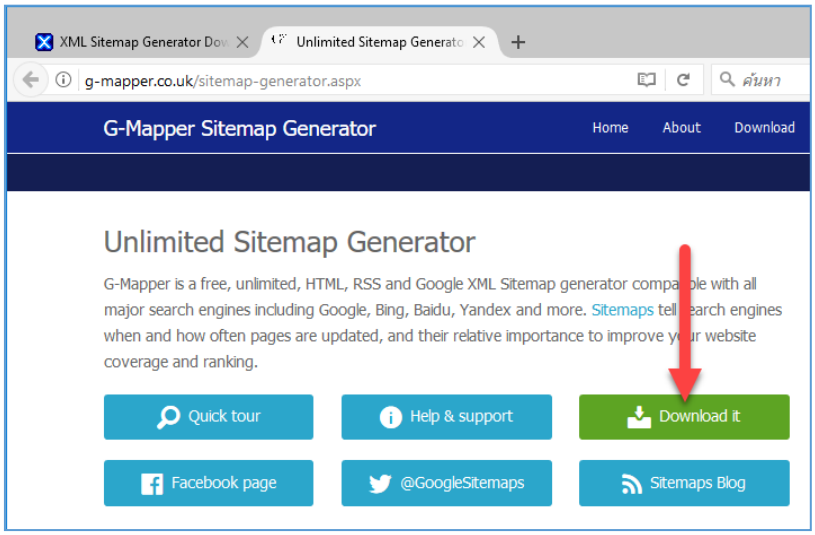
ภาพที่ 14 หน้าจอเว็บไซต์การดาวน์โหลดโปรแกรม

2. คลิกที่เมนู Download Sitemap Generator



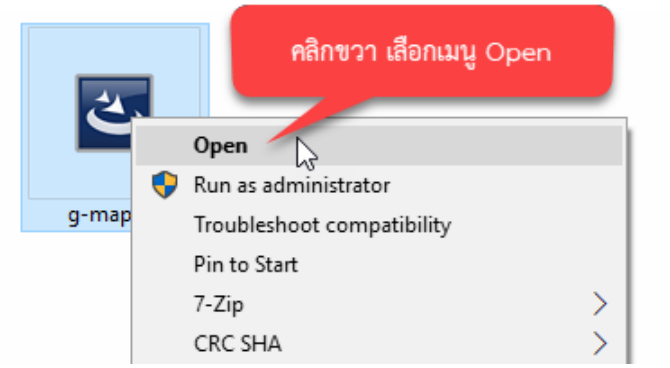
ภาพที่ 15 ส่วนของหน้าจอเว็บไซต์สำหรับการดาวน์โหลดโปรแกรม

3. คลิกที่เมนู **Download it** และบันทึกไฟล์โปรแกรม **gmapper.exe** ไว้ในเครื่องคอมพิวเตอร์



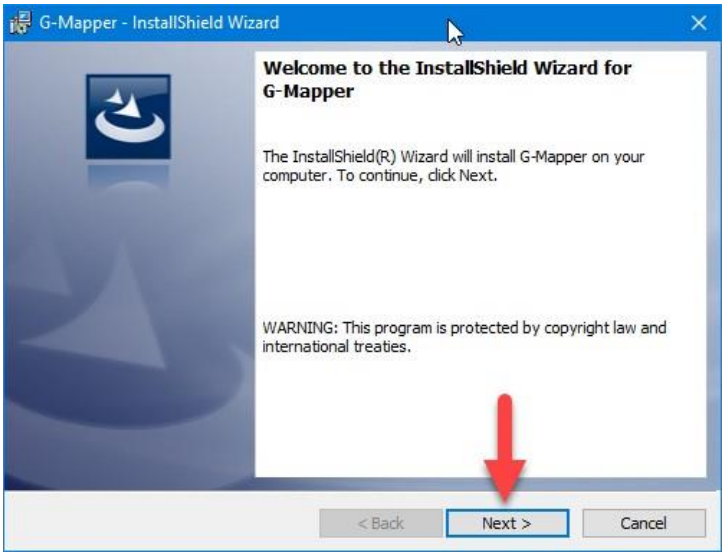
ภาพที่ 16 ปุ่มสำหรับดาวน์โหลดโปรแกรม

4. ทำการติดตั้งโปรแกรมโดยดับเบิ้ลคลิก หรือ คลิกขวาที่ไฟล์ โปรแกรม g-mapper เลือกเมนู **Open**



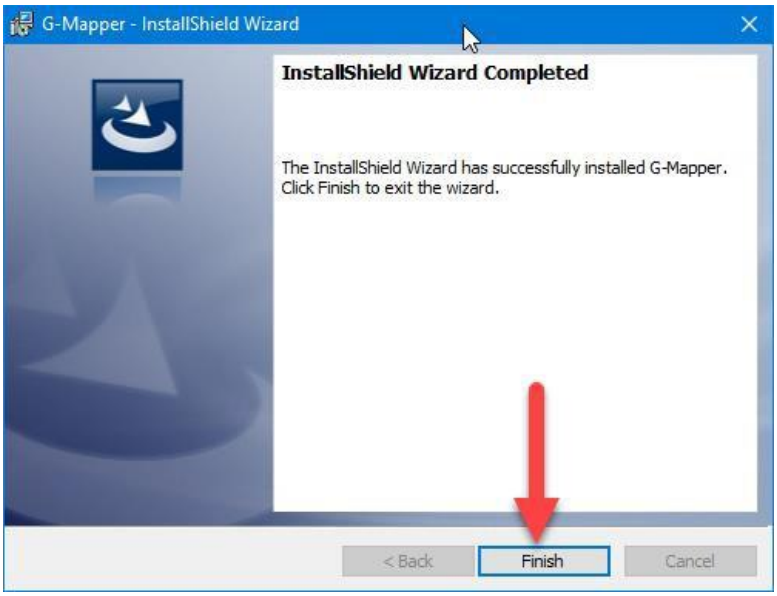
ภาพที่ 17 การติดตั้งโปรแกรม g-mapper

5. คลิกที่ปุ่ม **Next** เพื่อดำเนินการต่อ



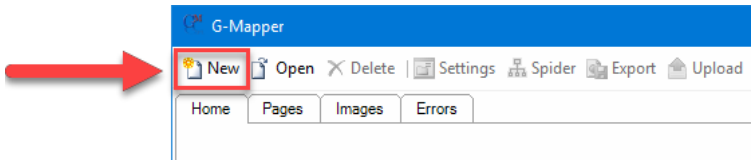
ภาพที่ 18 หน้าจอการติดตั้งโปรแกรม g-mapper

6. คลิกที่ปุ่ม **Finish** เพื่อเสร็จสิ้นการติดตั้งโปรแกรมสำเร็จรูป gmapper



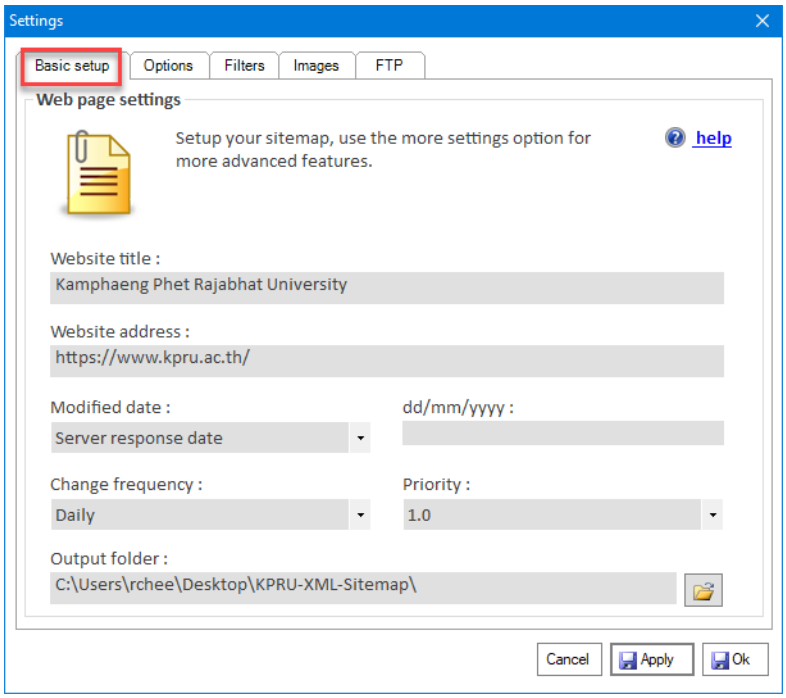
ภาพที่ 19 หน้าจอการติดตั้งโปรแกรม g-mapper เสร็จสิ้น

7. เปิดโปรแกรม **gmapper** จากนั้นสร้างใหม่ สำหรับกำหนดรายละเอียดของ XML Sitemap โดย ไปที่เมนู **New**



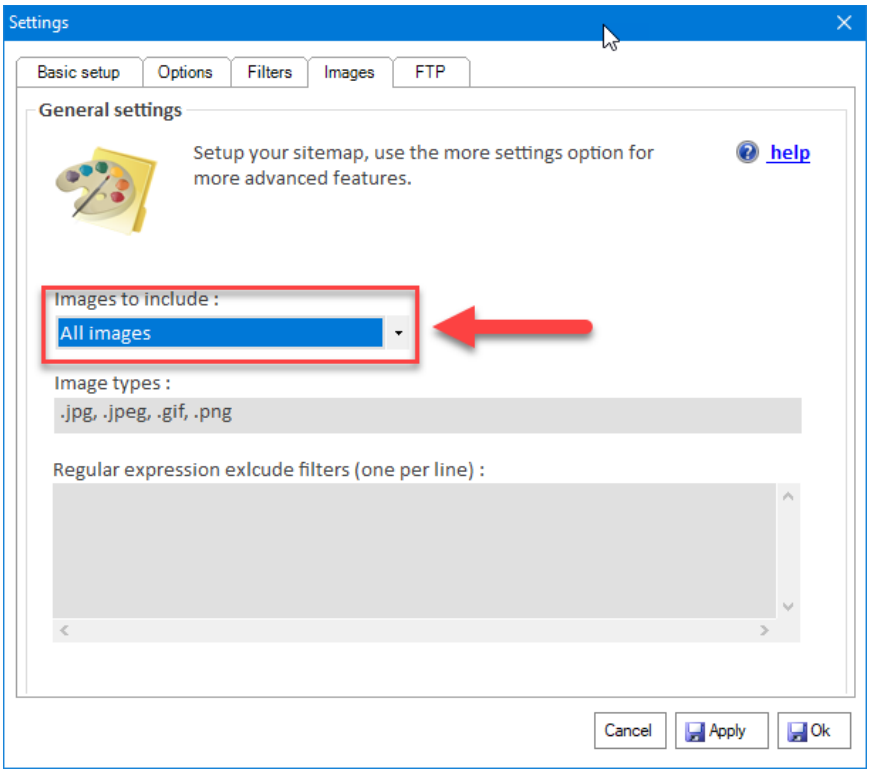
ภาพที่ 20 การเริ่มต้นการสร้าง sitemap

8. คลิกที่แถบเมนู **Basic setup** กรอกข้อมูลและกำหนดรายละเอียดตามต้องการ



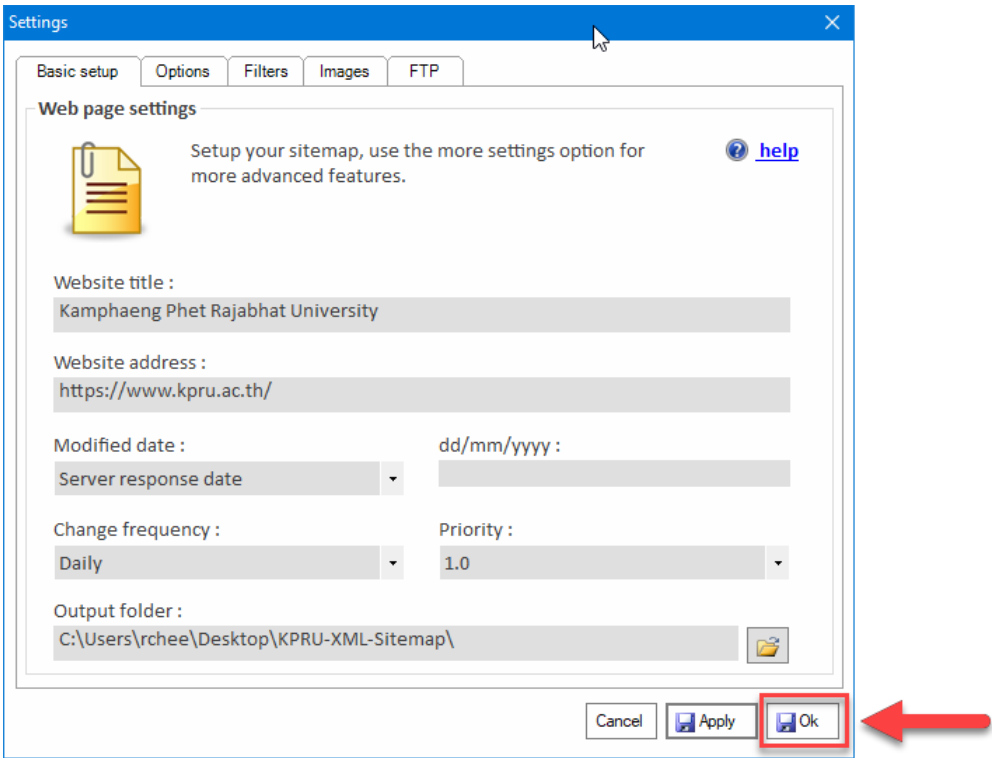
ภาพที่ 21 หน้าจอกำหนดรายละเอียดการตั้งค่า

9. คลิกที่แถบเมนู **Images** เลือกรูปแบบการสร้าง sitemap ให้กับรูปภาพในส่วนของ **Images to include**



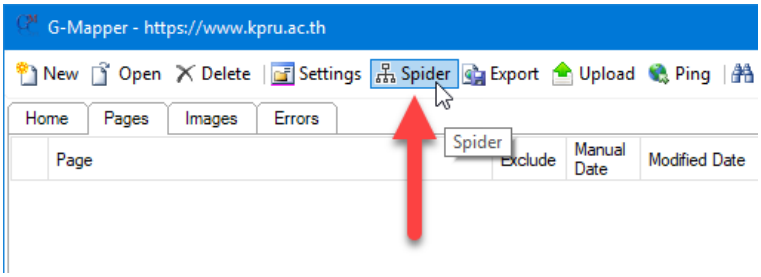
ภาพที่ 22 หน้าจอเลือกรูปแบบการสร้าง sitemap

10. เมื่อกรอกข้อมูลและกำหนดรายละเอียดตามต้องการเรียบร้อยแล้ว จากนั้นคลิกที่ปุ่ม OK



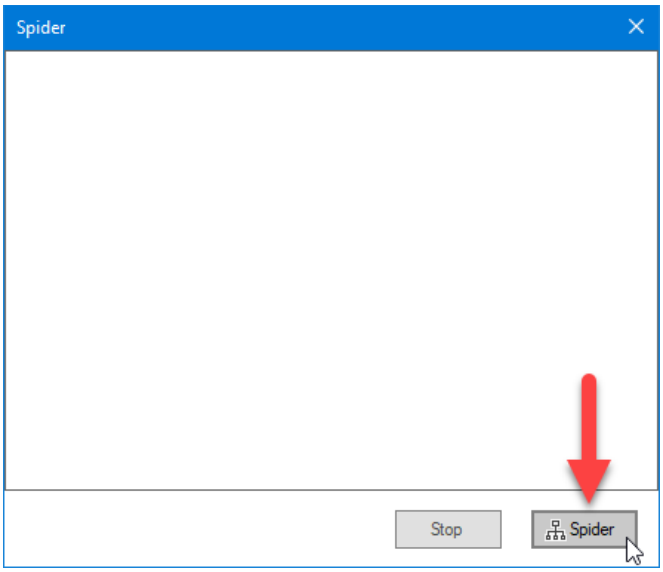
ภาพที่ 23 หน้าจอการดำเนินการสร้าง sitemap ต่อไป

11. ทำการประมวลผล XML sitemap จากข้อมูลรายละเอียดที่กำหนดไปแล้ว โดยคลิกที่เมนู **Spider**



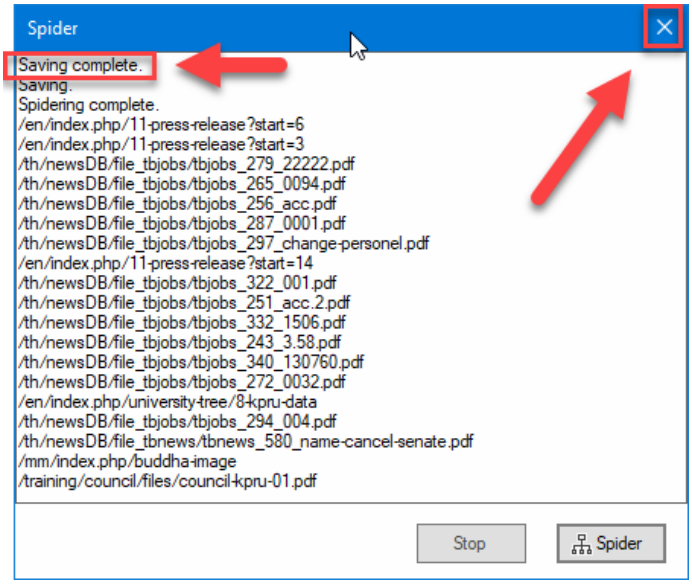
ภาพที่ 24 ส่วนของหน้าจอในการประมวลผลเพื่อสร้าง sitemap

12. จากนั้นจะปรากฏหน้าต่าง Spider ขึ้นมา ให้คลิกที่ปุ่ม **Spider** เพื่อเริ่มประมวลผล



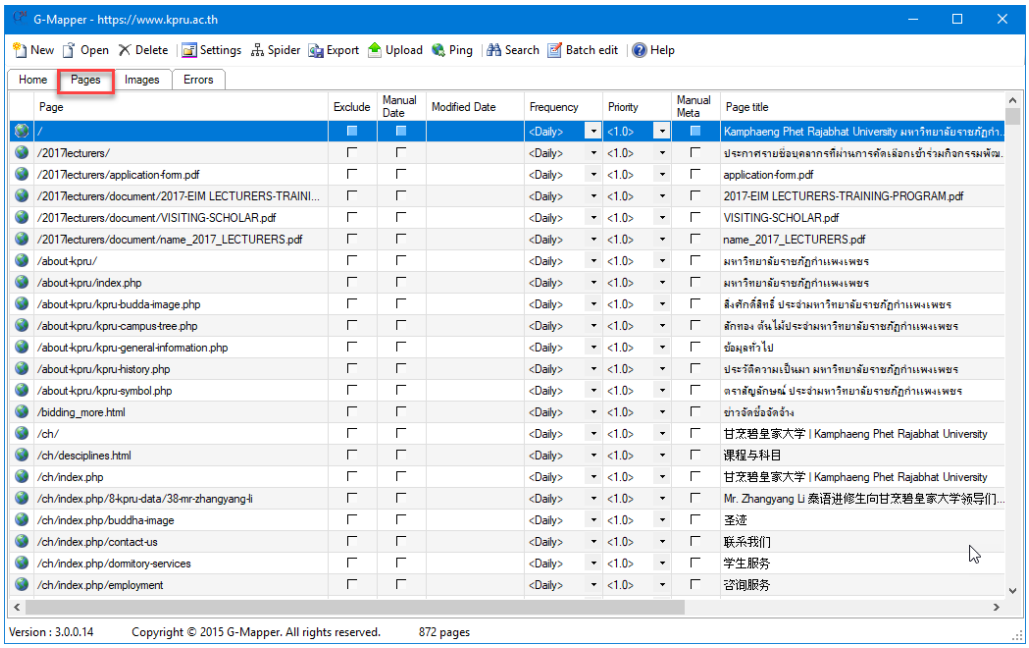
ภาพที่ 25 หน้าจอการสร้าง sitemap ด้วยปุ่ม Spider

13. ระบบจะประมวล เมื่อเสร็จแล้วจะปรากฏข้อความว่า **Saving Complete.** จากนั้น คลิกที่ปุ่ม X เพื่อปิดหน้าต่าง Spider



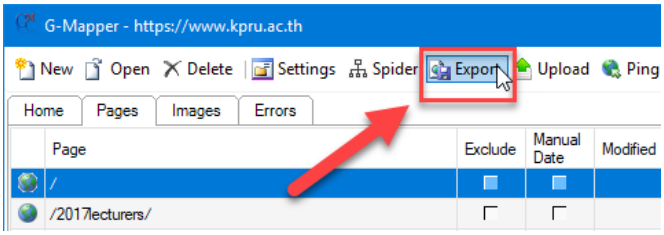
ภาพที่ 26 หน้าจอเมื่อการสร้าง sitemap เสร็จสิ้น

14. เมื่อประมวลผล XML Sitemap เรียบร้อยแล้ว จะแสดงรายละเอียดในตาราง สามารถคลิกดู รายละเอียดได้ตามแถบเมนู **Pages, Images, Errors**



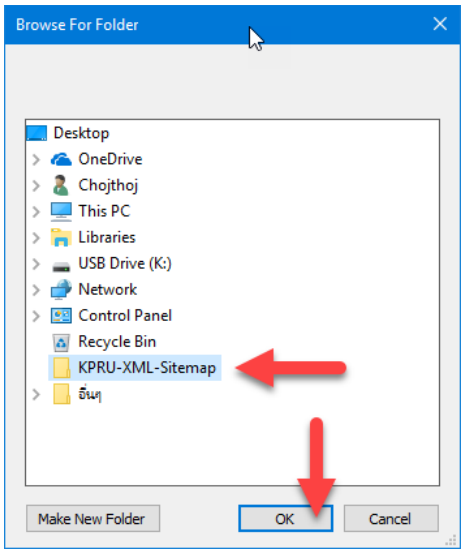
ภาพที่ 27 หน้าจอแสดงรายละเอียดเมื่อเสร็จสิ้นการสร้าง sitemap

15. การนำไฟล์ **XML Sitemap** ออกมาใช้งาน โดยคลิกที่เมนู **Export**



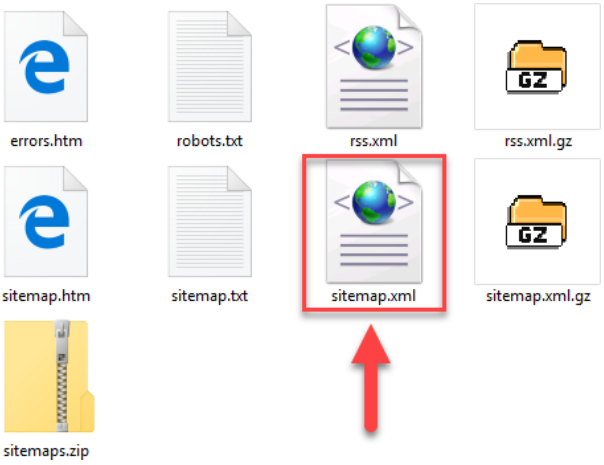
ภาพที่ 28 ปุ่ม Export เพื่อการนำ sitemap มาใช้งาน

16. กำหนดตำแหน่งสำหรับเก็บข้อมูลไฟล์ **XML Sitemap** เมื่อกำหนดเรียบร้อยแล้วคลิกที่ปุ่ม **OK**



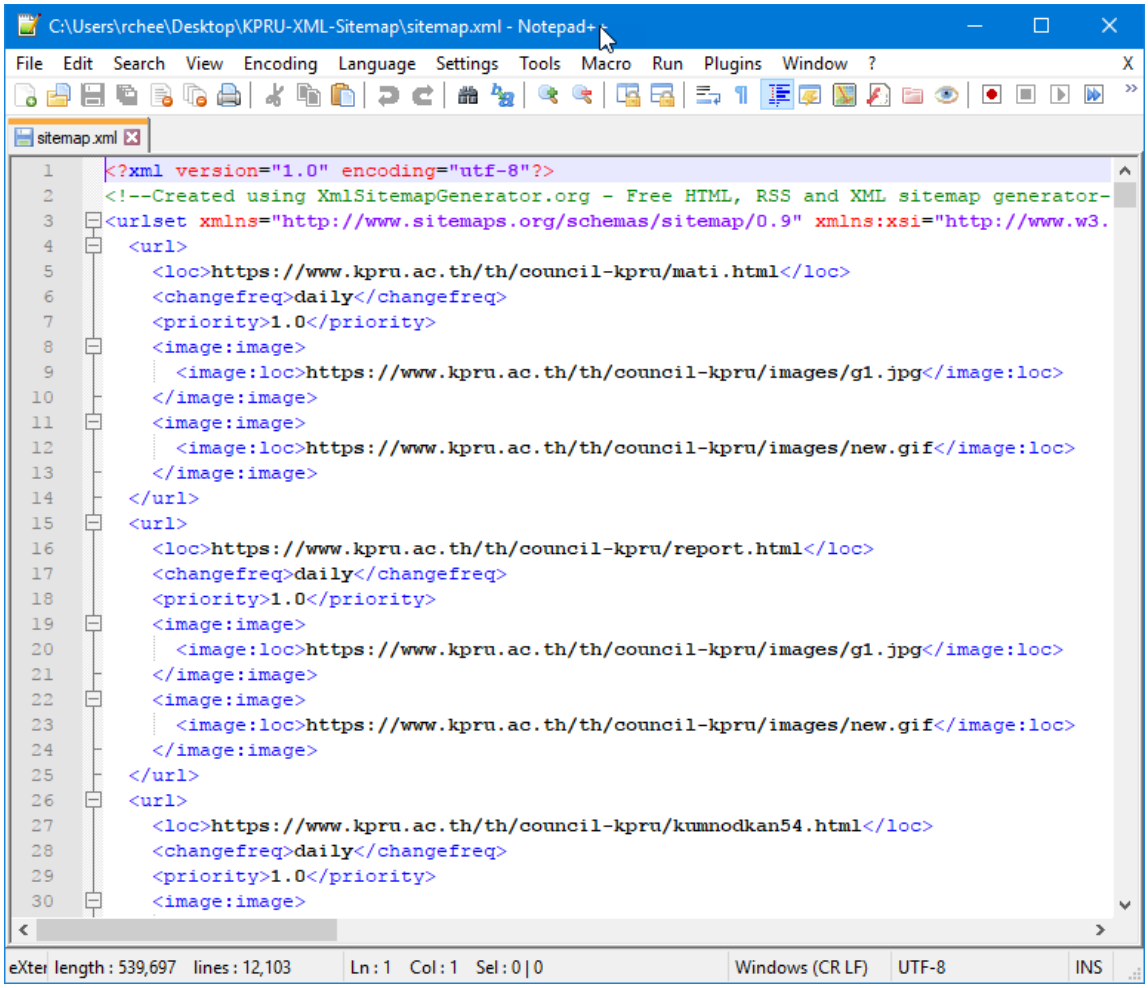
ภาพที่ 29 ส่วนของหน้าจอในการระบุตำแหน่งการเก็บไฟล์ XML sitemap

17. เปิดดูไฟล์ข้อมูลในโฟลเดอร์ที่ได้จากการ Export จะได้ไฟล์ sitemap.xml และไฟล์อื่นๆ รวมเป็น 9 ไฟล์



ภาพที่ 30 ไฟล์ sitemap.xml ในโฟลเดอร์ที่กำหนด

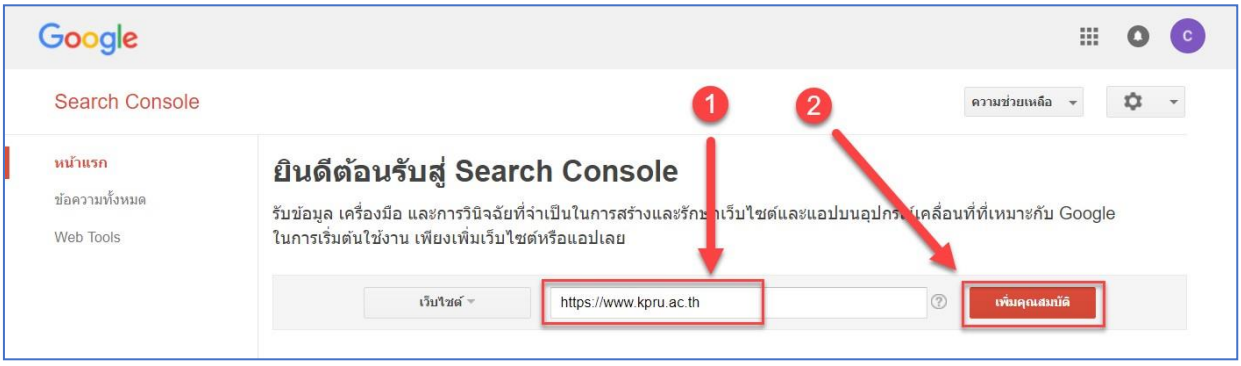
เมื่อเปิดไฟล์ sitemap.xml จะได้ดังภาพ



ภาพที่ 31 รายละเอียดไฟล์ sitemap.xml

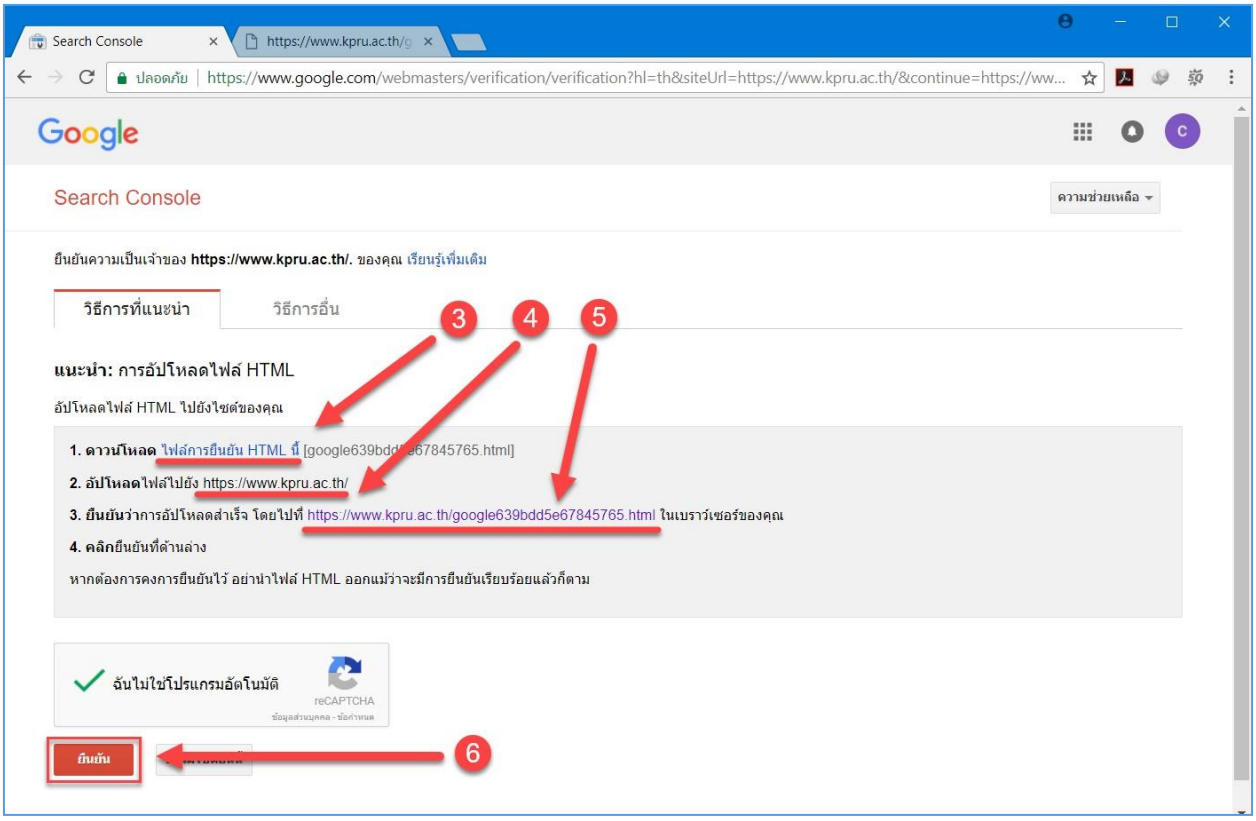
ส่วนที่ 2 การยืนยันไฟล์ XML Sitemap ให้กับ Google

1. เข้าไปที่เว็บไซต์ https://www.google.com/webmasters/sitemaps/ (ถ้าหากยังไม่เคยสมัครใช้บริการ ให้คลิกที่ https://www.google.com/accounts/NewAccount?) จากนั้น กรอกชื่อ **URL** เว็บไซต์ ในช่องที่กำหนดให้
2. คลิกที่ปุ่ม เพิ่มคุณสมบัติ



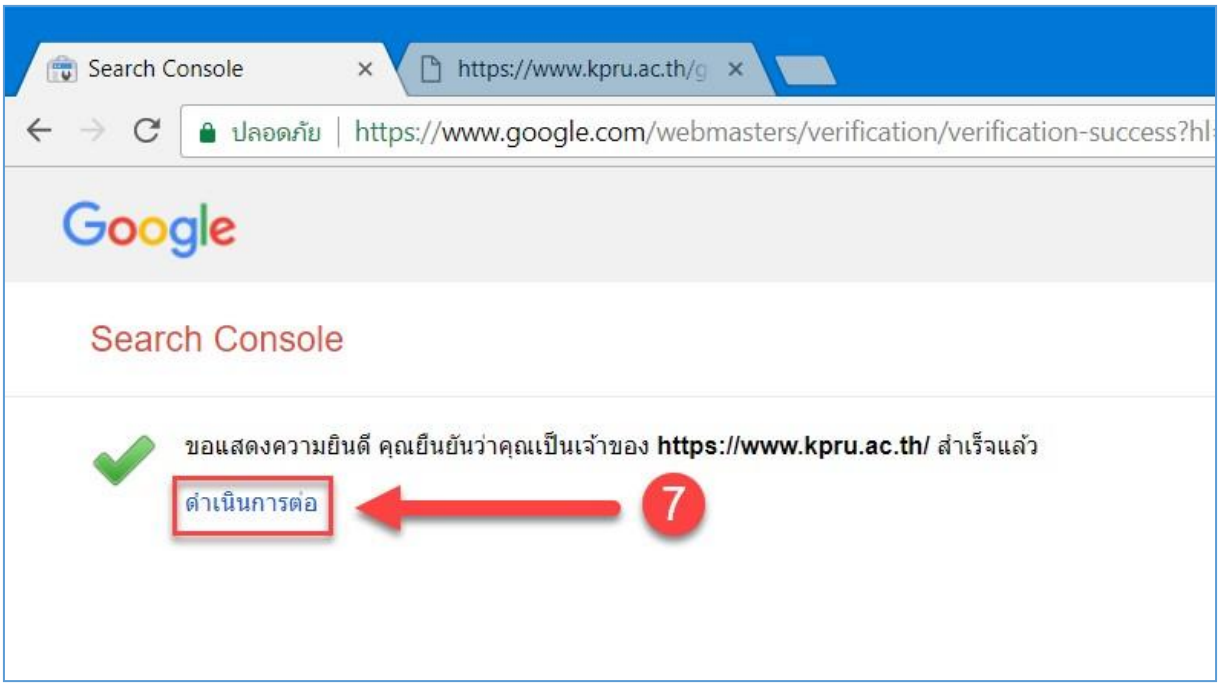
ภาพที่ 32 ส่วนของหน้าจอเพื่อยืนยันไฟล์ sitemap.xml ให้กับ Google

3. คลิกดาวน์โหลด ไฟล์การยืนยัน HTML
4. ทำการอัพโหลด **ไฟล์การยืนยัน HTML** ไปไว้ยังเว็บไซต์
5. คลิกที่ลิงค์สำหรับการยืนยันว่าอัพโหลดไฟล์เรียบร้อยแล้ว
6. คลิกที่ปุ่ม **ยืนยัน**



ภาพที่ 33 ขั้นตอนการยืนยันไฟล์ sitemap.xml ให้กับ Google

7. จะแสดงข้อความ ยืนยันความเป็นเจ้าของเว็บไซต์ จากนั้นคลิกที่เมนู **ดำเนินการต่อ**

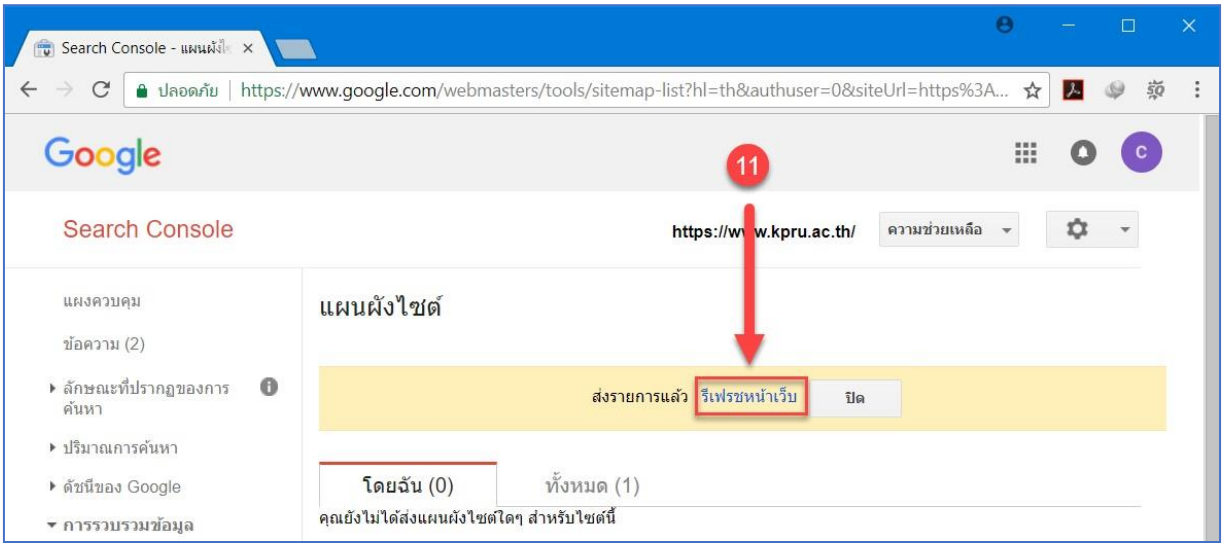


ภาพที่ 34 หน้าจอการยืนยันความเป็นผู้ดูแลเว็บไซต์

8. คลิกที่ปุ่ม เพิ่ม/ทดสอบแผนผังเว็บไซต์
9. กรอกชื่อไฟล์ XML Sitemap คือ **sitemap.xml**
10. คลิกที่ปุ่ม **ส่ง**

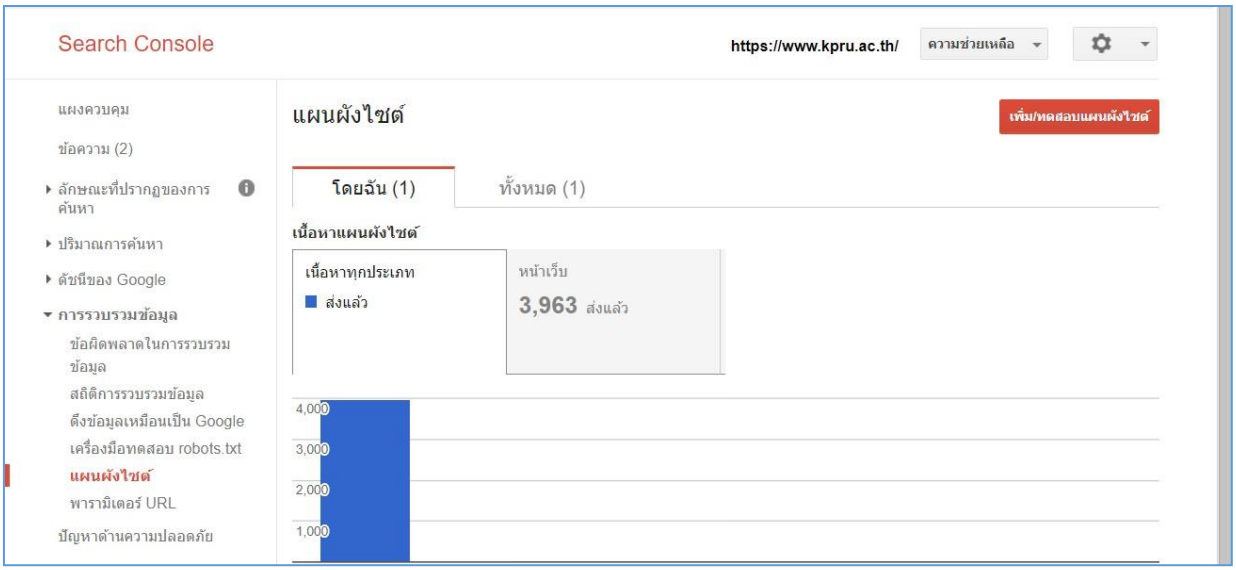
ภาพที่ 35 หน้าจอการเพิ่มแผนผังเว็บไซต์

11. คลิกที่เมนู **รีเฟรชหน้าเว็บ** เป็นอันเสร็จสิ้นการยืนยัน Sitemap ให้กับ Google



ภาพที่ 36 หน้าจอเพื่อระบุให้แสดงผลหน้าเว็บที่ปรับปรุงแล้ว

หลังจากยืนยันเรียบร้อยแล้ว ได้ผลดังภาพที่ 37



ภาพที่ 37 หน้าจอเมื่อเสร็จสิ้นกระบวนการยืนยัน Sitemap ให้กับ Google

นโยบายรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร

มหาวิทยาลัยราชภัฏกำแพงเพชร

ประกาศมหาวิทยาลัยราชภัฏกำแพงเพชร
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร

.....

เพื่อให้การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏกำแพงเพชร เป็นไปตามมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา 31(1) แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. 2547 ประกอบ มาตรา 5 และมาตรา 7 แห่งพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 และหนังสือสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ 0209/ว2927 ลงวันที่ 13 ตุลาคม 2554 เรื่อง ขอความร่วมมือดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศมหาวิทยาลัยราชภัฏกำแพงเพชรเรื่อง นโยบายการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร ความดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า "ประกาศมหาวิทยาลัยราชภัฏกำแพงเพชรเรื่อง นโยบายการรักษาและการสื่อสาร"

ข้อ 2 ประกาศนี้ ให้ใช้บังคับเมื่อพ้นกำหนดเก้าสิบวัน นับแต่วันประกาศใช้ประกาศฉบับนี้เป็นต้นไป

ข้อ 3 ในประกาศนี้

"**มหาวิทยาลัย**" หมายถึง มหาวิทยาลัยราชภัฏกำแพงเพชร

"**หน่วยงาน**" หมายถึง คณะ วิทยาลัย สำนัก ศูนย์ และกอง ที่เป็นหน่วยงานภายในมหาวิทยาลัยราชภัฏกำแพงเพชร

"**ผู้ใช้งาน**" หมายถึง บุคลากร นักศึกษา ลูกจ้าง ผู้ดูแลระบบหรือผู้ที่มหาวิทยาลัยอนุญาตให้ใช้สินทรัพย์ของมหาวิทยาลัย

"**บุคลากร , ลูกจ้าง**" หมายถึง บุคคลซึ่งได้รับการจัดจ้างตามสัญญาจ้างให้ทำงานในมหาวิทยาลัยราชภัฏกำแพงเพชร โดยได้รับค่าตอบแทนจากเงินงบประมาณแผ่นดินหรือเงินรายได้ของมหาวิทยาลัยฯ

"**สิทธิของผู้ใช้งาน**" หมายถึง สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัยราชภัฏกำแพงเพชรหรือ เพื่อการเข้าถึงเข้าใช้สารสนเทศและทรัพย์สินสารสนเทศของมหาวิทยาลัยราชภัฏกำแพงเพชร

"**สินทรัพย์**" หมายถึง เครื่องคอมพิวเตอร์ของมหาวิทยาลัย เครือข่ายย่อย และระบบสารสนเทศต่าง ๆ ที่มหาวิทยาลัยพัฒนาขึ้นหรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

"**เครื่องคอมพิวเตอร์**" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่งซึ่งทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"**ห้องคอมพิวเตอร์แม่ข่าย**" หมายถึง สถานที่ติดตั้งอุปกรณ์แม่ข่ายหรืออุปกรณ์เครือข่ายของมหาวิทยาลัยภายในมหาวิทยาลัย

"**การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ**" หมายถึง ความสามารถในการเข้าถึงระบบสารสนเทศที่ได้รับการอนุญาต จากการกำหนดสิทธิหรือได้รับมอบอำนาจในการเข้าถึงระบบ ในการอ่าน สร้าง สำเนา และแก้ไขสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการทางกายภาพ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง ความมั่นคงและความปลอดภัยในบริบทของการรักษาความลับ ความเชื่อถือได้ และความพร้อมใช้งานของระบบสารสนเทศมหาวิทยาลัยราชภัฏกำแพงเพชร โดยมีเป้าหมายเพื่อปกป้องสินทรัพย์ของมหาวิทยาลัยจากเหตุการณ์หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ ซึ่งอาจทำให้เกิดความเสียหายต่อสินทรัพย์ของมหาวิทยาลัย

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพใช้งานการให้บริการเครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏกำแพงเพชร ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"เครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏกำแพงเพชร" หรือเรียกอีกนามหนึ่ง "เครือข่าย KPRUNet" หมายถึง ระบบเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย ฯ โดยมีวัตถุประสงค์การเข้าใช้งานเพื่อการบริหารงาน การบริการวิชาการการศึกษาและงานวิจัยที่เป็นพันธกิจของมหาวิทยาลัย

"ผู้ดูแลเครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏกำแพงเพชร" หมายถึง บุคลากรที่ได้รับมอบหมายจากกมหาวิทยาลัยเพื่อปฏิบัติงานให้ดูแลบริหารจัดการระบบเครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏกำแพงเพชรให้พร้อมสำหรับการใช้งานของมหาวิทยาลัย

"ผู้ปฏิบัติงานระบบสารสนเทศ" หมายถึง บุคลากรที่ได้รับมอบหมายจากหน่วยงาน เพื่อทำการป้อนข้อมูล และแก้ไขข้อมูลของระบบสารสนเทศของมหาวิทยาลัย

"เครือข่ายย่อย" หมายถึง อุปกรณ์ต่อพ่วงต่าง ๆ รวมถึงอุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่าง ๆ ภายในเครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏกำแพงเพชรตลอดจนถึงโปรแกรมและข้อมูลต่าง ๆ

"ผู้ดูแลระบบเครือข่ายย่อย" หมายถึง บุคลากรหรือลูกจ้างได้รับมอบหมายจากหัวหน้าหน่วยงานเพื่อปฏิบัติงานให้ระบบเครือข่ายของหน่วยงานพร้อมสำหรับการใช้งานของมหาวิทยาลัย

"ผู้ใช้บริการเครือข่าย" หมายถึง บุคคล หน่วยงานที่ต่อเชื่อมและรับบริการจากเครือข่ายสารสนเทศมหาวิทยาลัย

"ผู้บริหารระดับสูงสุด" หมายถึง อธิการบดีมหาวิทยาลัยราชภัฏกำแพงเพชร

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง" หมายถึง ผู้ที่ได้รับการแต่งตั้งจากมหาวิทยาลัยราชภัฏกำแพงเพชร ให้รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

"คณะกรรมการนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร" หมายถึง คณะกรรมการที่ได้รับการแต่งตั้งจากมหาวิทยาลัยราชภัฏกำแพงเพชรเพื่อทำหน้าที่ในการกำหนด ตรวจสอบ ทบทวน ปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งตรวจสอบและประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

"ผู้ตรวจสอบภายใน" หมายถึง บุคลากรภายในมหาวิทยาลัยที่ได้รับการแต่งตั้งจากมหาวิทยาลัยเพื่อทำหน้าที่ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

"ผู้ตรวจสอบจากภายนอก" หมายถึง เป็นบุคคลภายนอกที่มีความรู้ ความสามารถทางด้านเทคโนโลยีสารสนเทศที่ได้รับเชิญเป็นผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

"บทลงโทษ" หมายถึง บทลงโทษที่มหาวิทยาลัยเป็นผู้กำหนดหรือบทลงโทษตามกฎหมาย

ข้อ 4 การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้ มี 2 ส่วน ดังนี้

4.1 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ 5

4.2 แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ 6 -14

ข้อ 5 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี 2 ส่วน ดังนี้

5.1 ส่วนที่ว่าด้วยการจัดทำนโยบาย

(1) ผู้บริหาร บุคลากรทางด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏกำแพงเพชร

(2) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัยราชภัฏกำแพงเพชร

(3) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(4) ทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง

5.2 ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้ง มีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(2) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(3) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีนโยบายในมีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง

(4) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ 6 มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อย ดังนี้

(1) ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(2) กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(3) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ 7. บริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(1) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(2) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทำปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(3) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(4) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ 8. กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(1) การใช้งานรหัสผ่าน (Password Usage) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(2) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(3) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ อันได้แก่ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(4) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544

ข้อ 9. ควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(1) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(2) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(3) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(4) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(5) การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(6) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(7) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ 10. ควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(1) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(2) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(3) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(4) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(5) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

(6) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ 11. ควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่น และสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึง

สารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(2) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน

(3) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(4) การปฏิบัติงานจากภายนอกหน่วยงาน ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ 12. จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทาง ต่อไปนี้

(1) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

(2) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(3) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งทำหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(4) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

(5) ปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

ข้อ 13. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

(1) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ 1 ครั้ง

(2) ในการตรวจสอบและประเมินความเสี่ยง จะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ 14. ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ดังนี้

(1) ระดับนโยบาย

1.1 ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบในการกำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏกำแพงเพชรโดยมีหน้าที่กำกับ ดูแล รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนว

ปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้การสนับสนุนและส่งเสริมการดำเนินงานด้านสารสนเทศอย่างมีประสิทธิภาพ

1.2 ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ทำหน้าที่ติดตาม กำกับดูแล ควบคุม ตรวจสอบ และประเมินผลการดำเนินงานผู้รับผิดชอบระดับปฏิบัติงาน กำกับดูแลให้มีการปฏิบัติ และดำเนินการตามประกาศ ฉบับนี้

(2) ระดับปฏิบัติงาน ได้แก่

2.1 ผู้ดูแลรับผิดชอบเครือข่ายของมหาวิทยาลัยราชภัฏกำแพงเพชรในตำแหน่งนักวิชาการคอมพิวเตอร์ รับผิดชอบงานพัฒนาระบบเครือข่ายและสารสนเทศ กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตาม การปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

2.1.1 ควบคุมการเข้า - ออก ห้องคอมพิวเตอร์แม่ข่าย (Server) ตามการกำหนดสิทธิการเข้าถึง คอมพิวเตอร์แม่ข่าย (Server)

2.1.2 กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัยราชภัฏกำแพงเพชรให้สามารถใช้งานได้ตามปกติตลอด 24 ชั่วโมง

2.1.3 กำกับดูแล การติดตั้ง รื้อถอน ตรวจสอบการเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Internet, Intranet ที่ให้บริการในมหาวิทยาลัยราชภัฏกำแพงเพชร

2.1.4 กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของห้องคอมพิวเตอร์แม่ข่าย (Server) ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

2.1.5 แก้ไขปัญหาที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

2.1.6 รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาทราบทุกเดือน

2.1.7 กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

2.1.8 กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2.1.9 กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของระบบฐานข้อมูลทั้งหมดที่ให้บริการให้สามารถใช้งานได้ตามปกติตลอด 24 ชั่วโมง

2.1.10 กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของระบบ

2.1.11 ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

2.1.12 รายงานผลการปฏิบัติงานตามแผนการบริหารความเสี่ยงฯ ให้ผู้บังคับบัญชาทราบ

2.1.13 ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Back up and Recovery) ตามรอบระยะเวลาที่กำหนด

2.1.14 บริหารจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Management) ระบบสารสนเทศแต่ละระบบของมหาวิทยาลัย เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

2.2 ผู้ดูแลระบบ จากบริษัทที่จัดจ้างให้ดูแลระบบเครือข่ายและคอมพิวเตอร์ รับผิดชอบ ดังนี้

2.2.1 แก้ไขปัญหา อุปสรรค จากสถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศที่เกิดจากการถูกเจาะระบบจากบุคคลภายนอก (Hack) และการถูกทำลายจากโปรแกรมไวรัส

2.2.2 กำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่าย

2.2.3 รายงานสภาพปัญหา และสถานการณ์ความเสียหายของระบบฐานข้อมูลและสารสนเทศที่ถูกทำลายจากบุคคลภายนอก (Hacker) และจากไวรัส (Virus)

2.2.4 บำรุงรักษาอุปกรณ์ และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัยราชภัฏกำแพงเพชรให้สามารถใช้งานได้ตามปกติตลอด 24 ชั่วโมง (แก้ไขปัญหาขัดข้องของการเชื่อมโยงเครือข่ายในองค์กร)

ประกาศ ณ วันที่ 31 มกราคม พ.ศ. 2560

(รองศาสตราจารย์สุวิทย์ วงษ์บุญมาก)
อธิการบดีมหาวิทยาลัยราชภัฏกำแพงเพชร