ราชวิทยาลัยจุฬาภรณ์
CHULABHORN ROYAL ACADEMY
วิทยาลัยวิทยาศาสตร์การแพทย์เจ้าฟ้าจุฬาภรณ์
HRH Princess Chulabhorn College of Medical Science
คณะแพทยศาสตร์และการสาธารณสุข
Faculty of Medicine and Public Health

2019

ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

คณะแพทยศาสตร์และการสาธารณสุข
วิทยาลัยวิทยาศาสตร์การแพทย์เจ้าฟ้าจุฬาภรณ์
ราชวิทยาลัยจุฬาภรณ์

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
คณะแพทยศาสตร์และการสาธารณสุข
วิทยาลัยวิทยาศาสตร์การแพทย์เจ้าฟ้าจุฬาภรณ์ ราชวิทยาลัยจุฬาภรณ์

1. วัตถุประสงค์

1.1 เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์และการสาธารณสุข วิทยาลัยวิทยาศาสตร์การแพทย์เจ้าฟ้าจุฬาภรณ์ ราชวิทยาลัยจุฬาภรณ์

1.2 เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้แก่บุคลากร ผู้ปฏิบัติงานในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงาน ร่วมทั้งการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

1.3 เพื่อให้การใช้เทคโนโลยีสารสนเทศและการสื่อสาร เป็นไปตามจริยธรรม จรรณบรรณ และกฎหมายเทคโนโลยีสารสนเทศ พระราชบัญญัติว่าด้ายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์

1.4 เพื่อให้มีกระบวนการสำรองข้อมูลสารสนเทศ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ ให้สามารถกู้คืนระบบได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง เหมาะสม และสอดคล้องกับการใช้งาน

1.5 เพื่อให้มีการตรวจประเมินความมั่นคงปลอดภัยสารสนเทศและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

1.6 เพื่อความความรู้และความตระหนัก ความเข้าใจ และส่งเสริมให้มีการอบรม ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่บุคลากรและนักศึกษาของคณะแพทยศาสตร์และการสาธารณสุข

2. หลักการและเหตุผล

คณะแพทยศาสตร์และการสาธารณสุข มีการนำระบบเทคโนโลยีสารสนเทศเข้ามาใช้ในการเรียนการสอนและการปฏิบัติงานของบุคลากร เพื่อให้เกิดนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยสารสนเทศที่สอดคล้องกับจรรยาบรรณ จริยธรรมและกฎหมาย จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยสารสนเทศในระดับคณะแพทยศาสตร์ขึ้น โดยอ้างอิงบริบทของแผนการปฏิบัติ วิทยาลัยวิทยาศาสตร์การแพทย์ เจ้าฟ้าจุฬาภรณ์ และราชวิทยาลัยจุฬาภรณ์ อีกทั้งมีความสอดคล้องกับแนวปฏิบัติของกระทรวงศึกษาธิการ และตามกฎหมายของประเทศที่เกี่ยวข้องกับสารสนเทศ

3. เป้าหมายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์และการสาธารณสุข

3.1 ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสารสนเทศ ให้ตอบสนองต่อพันธกิจและนโยบายของคณะแพทยศาสตร์และการสาธารณสุข และสอดคล้องกับวิทยาลัยวิทยาศาสตร์การแพทย์เจ้าฟ้าจุฬาภรณ์ ราชวิทยาลัยจุฬาภรณ์

3.2 กำหนดแนวทางปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งการติดตามและการตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

3.3 การกำกับดูแลการดำเนินงานเพื่อบริหารจัดการใช้ระบบเทคโนโลยีสารสนเทศที่มีความถูกต้องสมบูรณ์และพร้อมให้ใช้งานได้อยู่สม่ำเสมอ

3.4 เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากร เจ้าหน้าที่ และนักศึกษาของคณะแพทยศาสตร์และการสาธารณสุข ตลอดจนส่งเสริมให้มีการศึกษาหาความรู้เพิ่มเติมอย่างต่อเนื่อง

3.5 บุคลากรด้านสารสนเทศต้องจัดให้มีการควบคุมเข้าถึงข้อมูล และอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

4. ขอบเขตแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์และการสาธารณสุข

นโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศให้สอดคล้อง และเป็นไปตามนโยบายที่กำหนดไว้ โดยองค์ประกอบในการปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ แบ่งออกเป็น 5 ส่วน คือ Hardware, Software, Data, Procedures และ People โดยแสดงในรูปที่ 1

Hardware	Software	Data	Procedures	People

รูปที่ 1 องค์ประกอบในการรักษาความมั่นคงปลอดภัยสารสนเทศ ของคณะแพทยศาสตร์และการสาธารณสุข

อย่างไรก็ตามขอบเขตของการปฏิบัติงานด้านความปลอดภัยมั่นคงสารสนเทศของคณะแพทยศาสตร์ฯ อยู่ในมุมมองของผู้ใช้งาน (End-user) โดยความรับผิดชอบการดูแลระบบสารสนเทศและเครือข่าย เป็นความรับผิดชอบของเจ้าหน้าที่ ฝ่ายสารสนเทศในระดับราชวิทยาลัยจุฬาภรณ์ ดังนั้นในเอกสารเล่มนี้ จะเจาะจงเน้นไปยังแนวทางปฏิบัติของผู้ใช้งานเท่านั้น โดยสามารถแบ่งออกเป็นส่วน ๆ ดังต่อไปนี้

ส่วนที่ 1 ระเบียบปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ส่วนที่ 2 ระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และระบบเครือข่าย

ส่วนที่ 3 จรรยาบรรณในการใช้เทคโนโลยีสารสนเทศ และอินเตอร์เน็ต

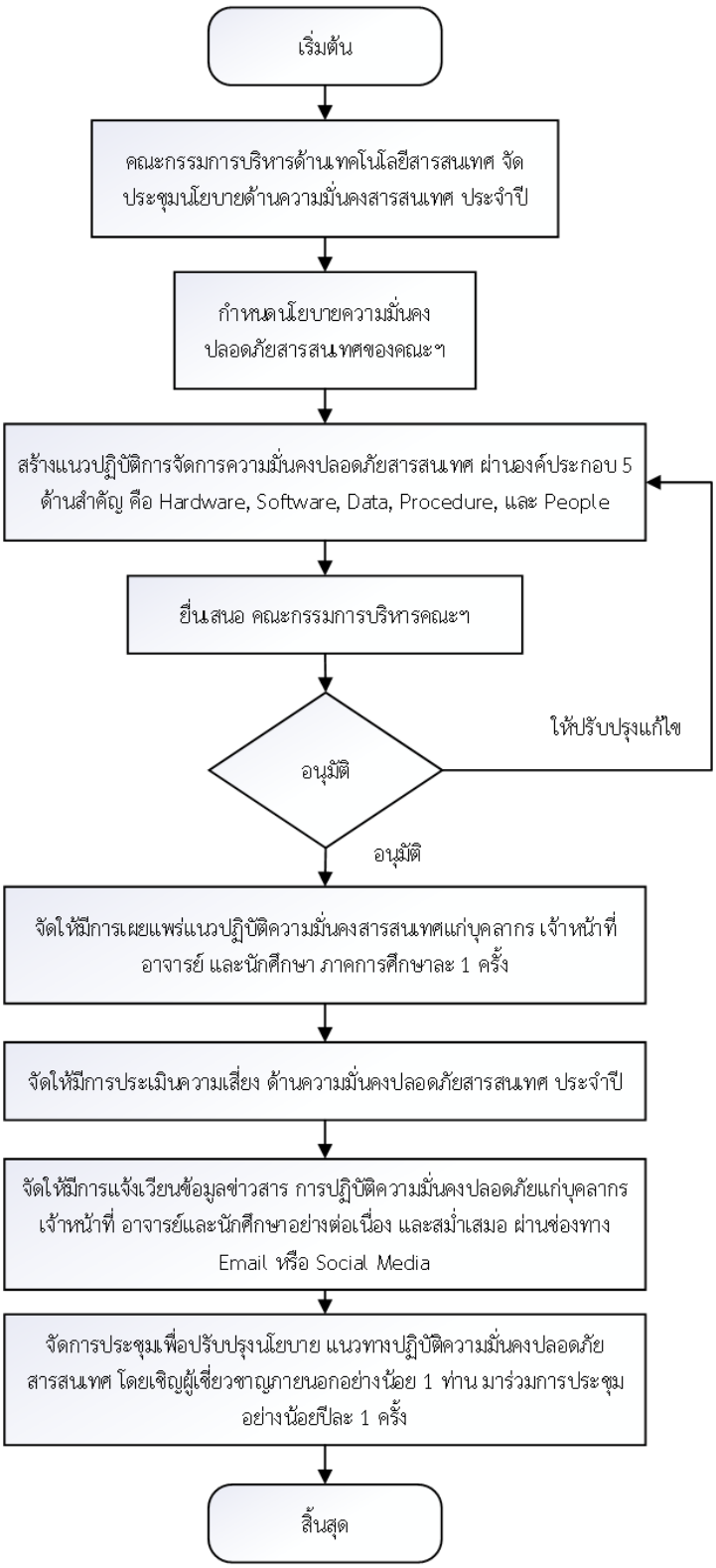
ระเบียบปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบ

คณะกรรมการบริหารด้านเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์และการสาธารณสุข

แนวปฏิบัติ

1. จัดให้มีการประเมินและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
2. ตระหนักและปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์และการสาธารณสุขอย่างเคร่งครัด
3. จัดให้มีการประชุมเกี่ยวกับด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง พร้อมทั้งเชิญผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ความเห็นประกอบ โดยหัวข้อการประชุมเกี่ยวข้องกับการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงฯ สู่แผนปฏิบัติเชิงป้องกัน หรือแก้ไขจากข้อบกพร่อง ปรับปรุงนโยบายให้ทันต่อเทคโนโลยีในปัจจุบัน การประเมินความเสี่ยง พร้อมแผนลดความเสี่ยงนั้น การจัดหาทรัพยากรทาด้านบุคลากร งบประมาณและบริหารจัดการ อุปกรณ์ เทคโนโลยีสารสนเทศ เพื่อให้เพียงพอต่อความต้องการในการปฏิบัติงานของบุคคลากร และการเรียนการสอนของอาจารย์และนักศึกษา
4. เผยแพร่แนวปฏิบัติความมั่นคงปลอดภัยให้กับบุคลากร และนักศึกษา อย่างน้อยปีละ 1 ครั้ง
5. จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง
6. จัดให้มีการแจ้งเวียนแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ และจริยธรรมการใช้เทคโนโลยีสารสนเทศ อย่างน้อยภาคการศึกษาละ 1 ครั้ง แก่บุคลากร และนักศึกษา



รูปที่ 2 SOP การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และระบบเครือข่าย

1. ระเบียบปฏิบัติสำหรับการใช้งานเครื่องคอมพิวเตอร์และเครือข่ายอย่างเหมาะสม

ผู้รับผิดชอบ

บุคลากร และนักศึกษา

แนวปฏิบัติ

1. ให้ผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น ในกรณีที่ทำเครื่องชำรุดหรือสูญหายไปโดยประมาท
2. ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองการใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 3 ชั่วโมง
3. ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อคหน้าจอ หลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาที
4. ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคล และระบบเครือข่ายเหมือนเช่น บุคคลทั่วไปพึงปฏิบัติในการใช้งานทรัพย์สินของตนเอง
5. ห้ามเจ้าหน้าที่ทั่วไปติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย
6. ห้ามเจ้าหน้าที่ทั่วไปติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในระบบเครือข่ายขององค์กร เพื่อป้องกันมิให้บุคคลอื่นสามารถเข้าถึง หรือเชื่อมต่อเข้าสู่ระบบเครือข่ายขององค์กร
7. ต้องขออนุมัติจากทางฝ่ายบริหารทรัพยากรคณะฯ หรือผู้มีอำนาจ ในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกสำนักงาน
8. ออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

2. ระเบียบปฏิบัติสำหรับการป้องกันไวรัสและมัลแวร์

ผู้รับผิดชอบ

บุคลากร และนักศึกษา

แนวปฏิบัติ

1. ตรวจสอบและยืนยันสิทธิ์การเข้าระบบที่สำคัญของบัญชีผู้ใช้ เมื่อเข้าใช้ระบบนั้น

2. เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบการป้องกันการโจมตี เช่น Web Application Firewall หรือ DDoS
3. แจ้งเจ้าหน้าที่ของหน่วยงาน ให้เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต เพื่อหลีกเลี่ยงการติดมัลแวร์ โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับ E-mail แนบจากคนที่ไม่รู้จัก, ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชทต่างๆ หรือช่องทาง Social Network
4. ติดตั้งโปรแกรมป้องกันไวรัส และตรวจสอบการทำงานของโปรแกรม พร้อมปรับปรุงฐานข้อมูลไวรัสอย่างสม่ำเสมอ โดยตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่ามีความผิดปกติให้รีบแจ้งเจ้าหน้าที่สารสนเทศราชวิทยาลัยจุฬาภรณ์ ให้ดำเนินการแก้ไขทันที
5. Scan Virus ที่ Removable Drive ทุกครั้งที่มีการเชื่อมต่อ
6. กรณีที่พบไวรัสหรือมัลแวร์ที่โปรแกรม Anti Virus ไม่สามารถกำจัดได้ รีบแจ้งเจ้าหน้าที่สารสนเทศราชวิทยาลัยจุฬาภรณ์ ให้ดำเนินการทันที

3. ระเบียบปฏิบัติสำหรับการป้องกันภัยคุกคามทางอินเตอร์เน็ต

ผู้รับผิดชอบ

บุคลากร และนักศึกษา

แนวปฏิบัติ

1. ทุกคนควรป้องกันการแอบดูรหัสการเข้าเครื่องคอมพิวเตอร์ เมื่อไม่ได้อยู่หน้าจอ ควรล็อคหน้าจอให้อยู่ในสถานะที่ต้องใส่ค่า Login และผู้ใช้งานไม่ควรประมาทในการใช้อินเตอร์เน็ต พร้อมทั้งตระหนักว่าข้อมูลส่วนบุคคลนั้นอาจถูกเปิดเผยในโลกของออนไลน์ได้เสมอ
2. กำหนด Password ที่ยากแก่การคาดเดา ควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร และใช้อักขระพิเศษ ไม่ใช้คำตรงกับความหมายในพจนานุกรม เช่น ASDFG@# เพื่อให้เดาได้ยากมากขึ้น และการใช้งานอินเตอร์เน็ตทั่วไป เช่น การ Login ระบบ email ระบบสนทนาออนไลน์ (Chat) หรือระบบเว็บไซต์ที่เราเป็นสมาชิกอยู่ ควรใช้ Password ที่แตกต่างกัน หรือใช้เครื่องมือในการจำรหัสเข้ามาช่วย
3. ผู้ใช้งานควรสังเกตว่ามีโปรแกรมไม่พึงประสงค์รันมาพร้อมๆ กันกับการเปิดเครื่องคอมพิวเตอร์หรือไม่
4. หมั่นตรวจสอบและอัพเดทระบบปฏิบัติการ (Operating System) เช่น Window ซอฟต์แวร์ที่ใช้ มั่นตรวจสอบและอัพเดท OS หรือซอฟต์แวร์ที่ใช้ ให้เป็นเวอร์ชั่นปัจจุบัน โดยเฉพาะโปรแกรมป้องกันใน

เครื่อง เช่น โปรแกรมป้องกันไวรัส หรือโปรแกรมไฟร์วอลล์ และควรใช้ระบบปฏิบัติการและซอฟต์แวร์ที่มีลิขสิทธิ์

5. หมั่นตรวจสอบและอัพเดทอินเตอร์เน็ตบราวเซอร์ให้ทันสมัยอยู่เสมอ เนื่องจาก Application Software สมัยใหม่มักพึ่งพาอินเตอร์เน็ตบราวเซอร์ก่อน ทำให้เกิดช่องโหว่ในการเข้าถึงข้อมูลจากผู้ไม่พึงประสงค์
6. ไม่ลงซอฟต์แวร์มากเกินความจำเป็น
7. ไม่ควรเข้าเว็บไซต์เสี่ยงภัย เช่น เว็บไซต์ลามกอนาจาร เว็บไซต์การพนัน เว็บไซต์แนบไฟล์ .EXE เว็บไซต์ที่ Pop-up หลายเพจ เว็บไซต์ที่มี Link ไม่ตรงกับชื่อ
8. สังเกตความปลอดภัยของเว็บไซต์ที่ให้บริการ ธุรกรรมออนไลน์ Web e-Commerce ที่ปลอดภัย ควรมีลักษณะดังนี้ มีการทำ HTTPS เนื่องจาก HTTPS จะมีการเข้ารหัสข้อมูล และมีใบรับรองทางอิเล็กทรอนิกส์ CA (Certificate Authority) เช่น https://www.facebook.com
9. ไม่เปิดเผยข้อมูลส่วนตัวผ่าน Social Network เลขที่บัตรประชาชน หนังสือเดินทาง ประวัติการทำงาน เบอร์โทรศัพท์ส่วนตัว ข้อมูลทางการแพทย์ และหมายเลขบัตรเครดิต
10. ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้อินเทอร์เน็ต ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้สื่ออินเทอร์เน็ต ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
11. ไม่หลงเชื่อโดยง่าย อย่าเชื่อในสิ่งที่เห็น และงมงายกับข้อมูลบนอินเทอร์เน็ต ควรหมั่นศึกษาหาความรู้จากเทคโนโลยีอินเทอร์เน็ต และศึกษาข้อมูลให้รอบด้าน ก่อนเชื่อในสิ่งที่ได้รับรู้

4. ระเบียบปฏิบัติสำหรับการป้องกันการละเมิดลิขสิทธิ์และสิทธิทางปัญญา

ผู้รับผิดชอบ

บุคลากร และนักศึกษา

แนวปฏิบัติ

1. ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของบุคคลอื่น
2. ระมัดระวังการใช้งานเอกสารหรือข้อมูลต่างๆ ซึ่งอยู่ในรูปแบบใดก็ตาม และได้มีการกำหนด เงื่อนไขการใช้งานเอาไว้ ต้องปฏิบัติตามเงื่อนไขดังกล่าวอย่างเคร่งครัด เพื่อไม่ให้เป็นการ ละเมิดทรัพย์สินทางปัญญาของบุคคลอื่น

5. ระเบียบปฏิบัติสำหรับการใช้งานอีเมล์

ผู้รับผิดชอบ

บุคลากร และนักศึกษา

แนวปฏิบัติ

1. ห้ามเข้าถึงข้อมูลอีเมล์ของบุคคลอื่นโดยไม่ได้รับอนุญาต
2. ห้ามลงทะเบียนด้วย E-mail Address ที่องค์กรมอบให้ไว้ตามที่อยู่เว็บไซต์ต่างๆ ที่ไม่เกี่ยวข้องกับงานขององค์กร
3. ห้ามทำการส่งอีเมล์ที่เนื้อหาเกี่ยวข้องกับงานขององค์กรด้วย E-mail Address อื่นที่นอกเหนือจากที่องค์กรจัดให้
4. ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
5. ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
6. ห้ามส่งอีเมล์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น
7. ห้ามส่งอีเมล์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
8. ห้ามปลอมแปลงอีเมล์ของบุคคลอื่น
9. ห้ามรับ หรือส่งอีเมล์แทนบุคคลอื่นโดยไม่ได้รับอนุญาต
10. ห้ามส่งอีเมล์ที่มีไฟล์ขนาดใหญ่เกินกว่า 25 เมกกะไบต์ หากไฟล์เกินให้แชร์ผ่าน google drive
11. ห้ามส่งอีเมล์ข้อมูลที่เป็นความลับขององค์กร เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลอีเมล์ที่องค์กรกำหนดไว้
12. ใช้ความระมัดระวังในการระบุชื่อที่อยู่อีเมล์ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิด
13. ใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับอีเมล์เท่าที่มีความจำเป็นต้องรับรู้ รับทราบในข้อมูลที่ส่งไป
14. ใช้คำที่สุภาพในการส่งอีเมล์
15. ให้ระบุชื่อของผู้ส่งในอีเมล์ทุกฉบับที่ส่งไป
16. ให้ทำการสำรองข้อมูลอีเมล์ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าองค์กรจะทำการสำรองข้อมูลอีเมล์ไว้ให้ แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้นอีเมล์ที่เก่ามากๆ นั้น หากจำเป็นต้องใช้งาน จึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

6. ระเบียบปฏิบัติสำหรับการป้องกันใช้ทรัพยากรผิดวัตถุประสงค์

ผู้รับผิดชอบ

บุคลากร และอาจารย์

<u>แนวปฏิบัติ</u>

บุคลากร และนักศึกษา ต้องไม่ใช่ระบบเครือข่าย โดยมีวัตถุประสงค์ดังต่อไปนี้

1. เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
2. เพื่อการกระทำที่ขัดต่อ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
3. เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
4. เพื่อการค้าขาย หรือผลประโยชน์ส่วนตัว หรือผลประโยชน์ทางการเมือง
5. เพื่อการเข้าถึง แสดง จัดเก็บ แจกจ่าย แก้ไข จัดทำ หรือบันทึกข้อมูลที่มีเนื้อหาไม่เหมาะสม เช่น ข้อมูลอันเป็นเท็จ ข้อมูลที่มีผลต่อความมั่นคงของสถาบันชาติ ศาสนา และพระมหากษัตริย์ ภาพลามกอนาจาร ภาพตัดต่อของบุคคลอื่น หรือข้อมูลที่ก่อให้เกิดความ เสื่อมเสียอับอาย แก่องค์กรหรือบุคคลอื่น เป็นต้น
6. เพื่อทำการเผยแพร่ข้อมูล หรืออนุญาตให้ผู้อื่นเผยแพร่ข้อมูลเพื่อการกล่าวร้าย หมิ่นประมาท หรือพาดพิงบุคคลอื่น จนทำให้องค์กรถูกฟ้องร้องหรือก่อให้เกิดความเสียหายแก่องค์กร
7. เพื่อการเปิดเผยข้อมูลลับซึ่งได้มาจากการปฏิบัติงานให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กรหรือบุคคลภายนอกก็ตาม
8. เพื่อขัดขวางหรือโจมตี การใช้งานระบบเครือข่ายขององค์กร หรือของหน่วยงานภายนอกอื่น
9. เพื่อแพร่กระจายไวรัส หนอน ม้าโทรจัน สปายแวร์ สแปมเมล์ หรือโปรแกรมไม่ประสงค์ดีอื่นๆ
10. เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กรไปยังที่อยู่เว็บ หรือห้องสนทนาใดๆ ในลักษณะที่อาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไป จากความเป็นจริง
11. เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อองค์กร

7. ระเบียบปฏิบัติสำหรับการใช้งานสื่อสังคมออนไลน์ (Social Network)

<u>ผู้รับผิดชอบ</u>

บุคลากร และนักศึกษา

<u>แนวปฏิบัติ</u>

1. พึงตระหนักว่า ข้อความหรือความเห็นที่เผยแพร่บนสื่อสังคมออนไลน์ เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบ ทั้งทางด้านสังคมและด้านกฎหมาย นอกจากนี้ ยังอาจมีผลกระทบต่อชื่อเสียง การทำงานและอนาคตของวิชาชีพของตนได้
2. ใช้ความระมัดระวังอย่างยิ่ง ในการเผยแพร่ความคิดเห็นส่วนบุคคลที่อาจจะกระตุ้น หรือนำไปสู่การโต้แย้งที่รุนแรงในวงกว้าง โดยเฉพาะอย่างยิ่ง เกี่ยวกับด้านการเมืองและศาสนา เป็นต้น

3. พึงระลึกว่า พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลผูกพันต่อการเผยแพร่ข้อมูลและแสดงความคิดเห็นบนสื่อออนไลน์ ทั้งนี้ การละเมิดพระราชบัญญัติดังกล่าวคือเป็นความผิดทางวินัยอย่างร้ายแรงและผู้ละเมิดสามารถถูกดำเนินทางวินัยได้ด้วย
4. ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน
5. พึงตระหนักว่า การใช้สื่อสังคมออนไลน์นั้นในการเผยแพร่ข้อมูลเกี่ยวกับเรื่องหน้าที่การงานหรือข้อมูลเกี่ยวกับหน่วยงาน ควรแยกบัญชีผู้ใช้ (Account) ระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออกจากกัน
6. หากต้องการสร้าง Page หรือ Account ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการของส่วนงานหรือคณะฯ ต้องแจ้งให้หัวหน้างานของตนทราบ
7. การเผยแพร่ข้อมูล หรือแสดงความคิดเห็นที่อาจเข้าใจว่า เป็นความเห็นจากทางคณะฯ ส่วนงาน หรือหน่วยงาน ต้องมีการแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของคณะฯ ส่วนงาน หรือหน่วยงานที่ตนสังกัด เว้นแต่จะเป็นความเห็นของคณะฯ ส่วนงานหรือหน่วยงานอย่างแท้จริง หรือได้รับอนุญาตจากผู้มีอำนาจที่เกี่ยวข้องแล้วแต่กรณี
8. ผู้บริหารในระดับใดๆ พึงระมัดระวังในการเผยแพร่ข้อมูล หรือการแสดงความเห็นเนื่องจากจะถูกมองว่าเป็นความเห็นของหน่วยงานของตนได้ง่าย และอาจมีผลกระทบต่อความเข้าใจของผู้ใต้บังคับบัญชาได้ ทั้งนี้ให้มีการแสดงข้อความจำกัดความรับผิดชอบอย่างชัดเจนเช่นเดียวกับข้อ 7
9. ห้ามเผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญาของมหาวิทยาลัย หรือข้อมูลที่ใช้ภายในมหาวิทยาลัย ก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้มีอำนาจ
10. ผู้ปฏิบัติงานในคณะฯ ไม่ควรใช้ตราสัญลักษณ์ (logo) ของหน่วยงาน ส่วนงาน หรือราชวิทยาลัย บนรูปประกอบ profile ของตน ใน Account ส่วนตัว
11. บุคลากรหรือนักศึกษาที่ปฏิบัติงานวิชาชีพ หรือเป็นผู้ให้บริการสุขภาพหรือบริการอื่นใด พึงตระหนักถึงความรับผิดชอบในการเผยแพร่ ข้อมูลเกี่ยวกับผู้รับบริการ เนื่องจากผลของการเผยแพร่ข้อมูล อาจมีผลกระทบต่อผู้รับบริการ หน่วยงาน และวิชาชีพของตนได้ โดยที่ต้องระมัดระวังอย่างยิ่งในการใช้สื่อสังคมออนไลน์ในการปฏิสัมพันธ์กับผู้รับบริการ โดยไม่ควรใช้ Account ส่วนตัวในการติดต่อสื่อสาร เนื่องจากไม่มีวิธีที่ได้ผลสมบูรณ์ในการปกปิดความลับของผู้รับบริการบนสื่อสังคมออนไลน์ บุคลากรหรือนักศึกษาควรปฏิบัติตามจริยธรรมของวิชาชีพอย่างเคร่งครัด อีกทั้งเคารพและระมัดระวังอย่างยิ่ง ไม่ให้มีการละเมิดความเป็นส่วนตัว (Privacy) และความลับ (Confidentiality) ของผู้รับบริการ

12. ในกรณีที่บุคลากรหรือนักศึกษาที่ปฏิบัติงานวิชาชีพต้องการเผยแพร่ข้อมูลเพื่อวัตถุประสงค์ในการศึกษา ต้องขออนุญาตจากผู้รับบริการนั้นๆ ก่อนเสมอ และต้องลบข้อมูลที่อาจจะทำให้มีการทราบถึงตัวตนของผู้รับบริการนั้นทั้งหมด เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้รับบริการ ทั้งนี้ให้รวมถึงการเผยแพร่ข้อมูลในกลุ่มปิดเฉพาะด้วย
13. หากพบเพื่อนร่วมงานใช้สื่อสังคมออนไลน์ไม่เหมาะสมที่เกี่ยวข้องกับผู้รับบริการ ขอให้ตักเตือนโดยตรง หากไม่ได้รับการตอบสนองที่ดี ให้แจ้งต่อผู้บังคับบัญชาของผู้นั้น
14. บุคลากรและนักศึกษาควรป้องกันการถูกละเมิดความเป็นส่วนตัว ในฐานะที่เป็นผู้ใช้สื่อสังคมออนไลน์จึงควรศึกษา “การตั้งค่าความเป็นส่วนตัว (Privacy Setting) ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสม
15. บุคลากรและนักศึกษา พึงระวังการใช้ถ้อยคำและภาษาในการสื่อสารให้มีความเหมาะสม โดยใช้ภาษาที่ถูกต้องและสุภาพ หลีกเลี่ยงการใช้ภาษาไม่สุภาพ ไม่สร้างสรรค์ หรือบ่อนทำลายหน่วยงาน องค์กร หรือบุคคลอื่นๆ ในสื่อสังคมออนไลน์
16. ในกรณีการแชร์ข้อมูลในสื่อสังคมออนไลน์ บุคลากรและนักศึกษาต้องให้ความสำคัญของข้อมูลที่เป็นความจริง ร่วมถึงการแยกแยะให้เกิดความชัดเจนของข้อมูล และต้องคำนึงถึงผลกระทบต่อการแชร์ข้อมูลนั้นๆ ที่อาจเกิดขึ้นในอนาคต

จรรยาบรรณในการใช้เทคโนโลยีสารสนเทศ และอินเตอร์เน็ต

จรรยาบรรณต่อตนเอง

1. มีความซื่อสัตย์สุจริตต่อตนเอง ทำหน้าที่และใช้ชีวิตตามหลักธรรมาภิบาล
    - ประกอบอาชีพนักคอมพิวเตอร์ด้วยความ สุจริต ซื่อสัตย์ มีความยุติธรรม ใฝ่หาความรู้ใหม่ๆ อยู่เสมอ เพื่อพัฒนาตนเอง และความรับผิดชอบ ซึ่งจะเพิ่มความสามารถจริยธรรมวิชาชีพคอมพิวเตอร์ให้กับตัวเราเอง
    - ผู้ที่ประกอบอาชีพทางคอมพิวเตอร์ ต้องมีความตั้งใจ ขยันและอดทนในการทำงาน เพื่อให้เกิดความสำเร็จ

จรรยาบรรณต่อผู้ร่วมงาน

2. ปฏิบัติตนให้อยู่ในความถูกต้อง
    - ไม่ทำการ Copy ผลงานของผู้อื่นที่ ที่เรียกกันว่าละเมิดลิขสิทธิ์ไม่ว่าจะเป็นลายลักษณ์อักษรหรือ Software ต่างๆ
    - ให้ความเคารพนับถือผู้ร่วมงาน ให้เกียรติซึ่งกันและกัน และมีความเอื้อเฟื้อเผื่อแผ่
    - ดูแลรักษาความผูกพันของผู้ร่วมงานด้วยกันเอง

จรรยาบรรณต่อวิชาชีพ

3. ไม่กระทำสิ่งใดๆ ที่ทำให้วิชาชีพของตนเองนั้นเสื่อมเสีย
    - ใช้ความรู้ที่ได้เรียนมาอย่างสร้างสรรค์ ไม่ทำลายผู้อื่นหรือทำให้ผู้อื่นนั้นต้องเดือดร้อน
    - ไม่ดูหมิ่นอาชีพอื่นๆ
    - ให้ความร่วมมือกับส่งเสริมวิชาชีพของตนเอง เพื่อก่อให้เกิดการพัฒนา

จรรยาบรรณต่อสังคม

4. เป็นตัวอย่างที่ดีในการประกอบอาชีพสายงานคอมพิวเตอร์ เพื่อเป็นตัวอย่างของสังคม
    - ไม่เรียกร้องหรือรับสิ่งของทรัพย์สินใดที่ได้รับมาอย่างมิชอบ
    - ไม่ใช้อำนาจหรือวิชาชีพเอื้ออำนวยให้ประโยชน์แก่ตนเองหรือบุคคลอื่นโดยมิชอบ
    - ไม่ใช้วิชาชีพความรู้ต่างๆ เพื่อทำการล่อลวงหรือหลอกลวงผู้อื่นจนก่อให้เกิดความเสื่อมเสียหรือเสียหาย

จรรยาบรรณต่อผู้รับบริการ

5. เคารพในสิทธิเสรีภาพ และความเสมอภาคของผู้อื่น ปฏิบัติหน้าที่ด้วยความโปร่งใส เป็นธรรม
    - รับฟังความคิดเห็นแลกเปลี่ยนประสบการณ์ระหว่างบุคคล เครือข่าย และองค์กรที่เกี่ยวข้อง
    - เปิดโอกาสให้ประชาชนเข้ามามีส่วนร่วมและสามารถตรวจสอบการปฏิบัติงานได้

มารยาทของผู้ใช้อินเทอร์เน็ตผ่านมุมมองบุคคลที่เข้าไปใช้บริการ

1. ด้านการติดต่อสื่อสารกับเครือข่าย
    - ในการเชื่อมต่อเข้าสู่เครือข่ายควรใช้ชื่อบัญชี (Internet Account Name) และรหัสผ่าน (Password) ของตนเอง ไม่ควรนำของผู้อื่นมาใช้ รวมทั้งนำไปกรอกแบบฟอร์มต่างๆ
    - ควรเก็บรักษารหัสผ่านของตนเองเป็นความลับ และทำการเปลี่ยนรหัสผ่านเป็นระยะๆ รวมทั้งไม่ควรแอบดูหรือถอดรหัสผ่านของผู้อื่น
    - ควรวางแผนการใช้งานล่วงหน้าก่อนการเชื่อมต่อกับเครือข่ายเพื่อเป็นการประหยัดเวลา
    - เลือกถ่ายโอนเฉพาะข้อมูลและโปรแกรมต่างๆ เท่าที่จำเป็นต่อการใช้งานจริง
    - ก่อนเข้าใช้บริการต่างๆ ควรศึกษากฎ ระเบียบ ข้อกำหนด รวมทั้งธรรมเนียมปฏิบัติของแต่ละเครือข่ายที่ต้องการติดต่อ
2. ด้านช่องทางการรับส่งข้อมูลบนเครือข่ายที่จะส่งผลกระทบต่อผู้อื่นในช่วงเวลาที่มีการใช้บริการบนระบบเครือข่ายจำนวนมาก
    - ไม่ควรโหลดบิททอเร้นท์ (Bit Torrent)
    - ไม่ควรเล่นเกมส์ออนไลน์
3. ด้านการใช้ข้อมูลบนเครือข่าย
    - เลือกใช้ข้อมูลที่มีความน่าเชื่อถือ มีแหล่งที่มาของผู้เผยแพร่ และที่ติดต่อ
    - เมื่อนำข้อมูลจากเครือข่ายมาใช้ ควรอ้างอิงแหล่งที่มาของข้อมูลนั้น และไม่ควรแอบอ้างผลงานของผู้อื่นมาเป็นของตนเอง
    - ไม่ควรนำข้อมูลที่เป็นเรื่องส่วนตัวของผู้อื่นไปเผยแพร่ก่อนได้รับอนุญาต
4. ด้านการติดต่อสื่อสารระหว่างผู้ใช้
    - ใช้ภาษาที่สุภาพในการติดต่อสื่อสาร และใช้คำให้ถูกความหมาย เขียนถูกต้องตามหลักไวยากรณ์
    - ใช้ข้อความที่สั้น กะทัดรัดเข้าใจง่าย

- ไม่ควรนำความลับ หรือเรื่องส่วนตัวของผู้อื่นมาเป็นหัวข้อในการสนทนา รวมทั้งไม่ใส่ร้ายหรือทำให้บุคคลอื่นเสียหาย
- หลีกเลี่ยงการใช้ภาษาที่ดูถูก เหยียดหยามศาสนา วัฒนธรรมและความเชื่อของผู้อื่น
- ในการติดต่อสื่อสารกับผู้อื่นควรสอบถามความสมัครใจของผู้ที่ติดต่อด้วย ก่อนที่จะส่งแฟ้มข้อมูล หรือโปรแกรมที่มีขนาดใหญ่ไปยังผู้ที่เราติดต่อด้วย
- ไม่ควรส่งไปรษณีย์อิเล็กทรอนิกส์ (E-mail) ที่ก่อความรำคาญ และความเดือดร้อนแก่ผู้อื่น เช่น จดหมายลูกโซ่

5. ด้านระยะเวลาในการใช้บริการ
   - ควรคำนึงถึงระยะเวลาในการติดต่อกับเครือข่าย เพื่อเปิดโอกาสให้ผู้ใช้คนอื่นๆ บ้าง
   - ควรติดต่อกับเครือข่ายเฉพาะช่วงเวลาที่ต้องการใช้งานจริงเท่านั้น

มารยาทของผู้ใช้อินเทอร์เน็ตผ่านมุมมองบุคคลที่ทำหน้าที่เผยแพร่ข้อมูลทางอินเตอร์เน็ต

1. ควรตรวจสอบความถูกต้องของข้อมูล และข่าวสารต่างๆ ก่อนนำไปเผยแพร่บนเครือข่าย เพื่อให้ได้ข้อมูลที่เป็นจริง
2. ควรใช้ภาษาที่สุภาพ และเป็นทางการในการเผยแพร่สิ่งต่างๆ บนอินเทอร์เน็ต และควรเผยแพร่ข้อมูลข่าวสารต่างๆ ทั้งภาษาไทยและภาษาอังกฤษ
3. ควรเผยแพร่ข้อมูล และข่าวสารที่เป็นประโยชน์ในทางสร้างสรรค์ ไม่ควรนำเสนอข้อมูลข่าวสารที่ขัดต่อศีลธรรมและจริยธรรมอันดี รวมทั้งข้อมูลที่ก่อให้เกิดความเสียหายต่อผู้อื่น
4. ควรบีบอัดภาพหรือข้อมูลขนาดใหญ่ก่อนนำไปเผยแพร่บนอินเทอร์เน็ต เพื่อประหยัดเวลาในการดึงข้อมูลของผู้ใช้
5. ควรระบุแหล่งที่มา วันเดือนปีที่ทำการเผยแพร่ข้อมูล ที่อยู่ เบอร์โทรศัพท์ของผู้เผยแพร่ รวมทั้งควรมีคำแนะนำ และคำอธิบายการใช้ข้อมูลที่ชัดเจน
6. ควรระบุข้อมูล ข่าวสารที่เผยแพร่ให้ชัดเจนว่าเป็นโฆษณา ข่าวลือ ความจริง หรือความคิดเห็น
7. ไม่ควรเผยแพร่ข้อมูล ข่าวสาร รวมทั้งโปรแกรมของผู้อื่นก่อนได้รับอนุญาตจากเจ้าของ และที่สำคัญคือไม่ควรแก้ไข เปลี่ยนแปลงข้อมูลของผู้อื่นที่เผยแพร่บนเครือข่าย