ประกาศราชวิทยาลัยจุฬาภรณ์
เรื่อง กรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ

.....

เพื่อให้การปฏิบัติงานทุกส่วนงานที่ดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ผ่านทรัพยากรด้านเทคโนโลยีสารสนเทศของราชวิทยาลัยจุฬาภรณ์มีความมั่นคงปลอดภัย เป็นไปตามกฎหมายและระเบียบปฏิบัติต่างๆ ที่เกี่ยวข้อง จึงได้กำหนดกรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้ใช้กับทุกส่วนงานของราชวิทยาลัยจุฬาภรณ์ โดยมีรายละเอียดดังนี้

1. **ประกาศนี้เรียกว่า ประกาศราชวิทยาลัยจุฬาภรณ์** เรื่อง กรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ

2. **วัตถุประสงค์**

2.1 เพื่อให้มีกรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศให้เป็นไปตามกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

2.2 เพื่อให้มีแนวปฏิบัติในการใช้งานสารสนเทศการปฏิบัติงานด้านสารสนเทศ การกำหนดผู้รับผิดชอบ และการตรวจสอบด้านสารสนเทศ

2.3 เพื่อให้มีการป้องกันความเสี่ยงและรักษาซึ่งความมั่นคงปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของข้อมูลและทรัพยากรด้านสารสนเทศของราชวิทยาลัยจุฬาภรณ์

2.4 เพื่อให้มีการปกป้องและรักษาซึ่งความมั่นคงปลอดภัยในการให้บริการเครือข่ายและระบบงานสารสนเทศของราชวิทยาลัยจุฬาภรณ์มีเสถียรภาพ รวมทั้งให้มีมาตรการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

2.5 เพื่อให้มีการเผยแพร่ การส่งเสริมความเข้าใจ การสร้างความตระหนักและการมีส่วนร่วมรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศแก่บุคลากรของราชวิทยาลัยจุฬาภรณ์รวมถึงบุคคลที่เข้าใช้งานระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

3. ขอบเขตของนโยบาย

นโยบายนี้ใช้กับผู้ปฏิบัติงานของราชวิทยาลัยจุฬาภรณ์ทุกคนได้แก่ ผู้บริหาร แพทย์ พยาบาล อาจารย์ นักวิจัย เจ้าหน้าที่ รวมถึง นักศึกษา และผู้ใช้งานที่เข้าใช้ระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์ทุกคน ทั้งที่อยู่ในพื้นที่ของราชวิทยาลัยจุฬาภรณ์และการเข้าถึงระบบสารสนเทศจากระยะไกล

4. หน้าที่และความรับผิดชอบ

4.1 คณะกรรมการนโยบายและบริหารจัดการด้านเทคโนโลยีสารสนเทศมีหน้าที่กำหนดกรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ ติดตามผลการดำเนินนโยบาย และมีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง

4.2 ฝ่ายเทคโนโลยีสารสนเทศ ราชวิทยาลัยจุฬาภรณ์ มีหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศดูแลรักษาความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องและเป็นไปตามกรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ และมีหน้าที่เผยแพร่ การส่งเสริมความเข้าใจ การสร้างความตระหนักและการมีส่วนร่วมรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศแก่บุคลากรของ ราชวิทยาลัยจุฬาภรณ์ รวมถึงบุคคลที่เข้าใช้งานระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์ และต้องมีการประเมินความเสี่ยงระบบ และสอบทานให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องอย่างน้อยปีละ 1 ครั้ง

4.3 ผู้ปฏิบัติงานของราชวิทยาลัยจุฬาภรณ์ทุกคนได้แก่ ผู้บริหาร แพทย์ พยาบาล อาจารย์ นักวิจัย เจ้าหน้าที่ รวมถึง นักศึกษา และผู้ใช้งานที่เข้าใช้ระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์ทุกคนมีหน้าที่ปฏิบัติตามกรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ

4.4 คณะกรรมการหรือส่วนงานที่ตั้งขึ้นมาใหม่หลังจากประกาศใช้นโยบายฉบับนี้มีหน้าที่ปฏิบัติตามกรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ

5. กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

กรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศของราชวิทยาลัยจุฬาภรณ์อ้างอิงตาม กฎหมาย ระเบียบและมาตรฐานที่เกี่ยวข้องได้แก่

1) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
2) พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
3) พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ.2562
4) พระราชบัญญัติ การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.2562
5) พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560
6) พระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549

7) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.2555

หากในอนาคตมีการแก้ไขเปลี่ยนแปลงบทบัญญัติกฎหมาย ระเบียบ ข้อกำหนดหรือข้อบังคับใด ๆ ให้ถือตามที่แก้ไขเพิ่มเติมภายหลัง

6. การละเมิดหรือฝ่าฝืนนโยบาย

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรือสูญหาย รวมถึงการทำให้เกิดอันตรายๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกำหนดให้ “ผู้ก่อความเสียหาย” จะต้องเป็นผู้รับผิดชอบตามกฎหมายต่อความเสียหายหรืออันตรายที่เกิดขึ้น

7. ข้อยกเว้น

กรณีที่มีความจำเป็นสำหรับการปฏิบัติงานหรือใช้ระบบสารสนเทศที่มีความเสี่ยงที่จะขัดแย้งหรือละเมิดกรอบนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ปฏิบัติงานต้องขออนุญาตเป็นลายลักษณ์อักษร และต้องผ่านการเห็นชอบจากผู้บริหารสูงสุดของส่วนงานนั้น และได้รับการอนุมัติจากเลขาธิการราชวิทยาลัยจุฬาภรณ์ หรือผู้ที่ได้รับมอบหมาย

8. รายละเอียดนโยบาย

กรอบนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ราชวิทยาลัยจุฬาภรณ์ปฏิบัติตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.2555 มีสาระสำคัญครอบคลุมและสอดคล้องตามมาตรา 5 และมาตรา 7 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2549 กล่าวคือ

8.1 นโยบายเพื่อการควบคุมการเข้าถึงสารสนเทศ

8.1.1 วัตถุประสงค์

8.1.1.1 เพื่อการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

8.1.1.2 เพื่อรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่การยืนยันตัวบุคคล (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

8.1.2 แนวปฏิบัติที่เกี่ยวข้อง

8.1.2.1 แนวปฏิบัติการใช้บัญชีผู้ใช้งานระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

8.1.2.2 แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ Laptop และโทรศัพท์เคลื่อนที่ของราชวิทยาลัยจุฬาภรณ์

8.1.2.3 แนวปฏิบัติการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอกเข้ามาใช้ในพื้นที่ราชวิทยาลัยจุฬาภรณ์

8.1.2.4 แนวปฏิบัติในการเข้าใช้ระบบ WIFI และ Internet ราชวิทยาลัยจุฬาภรณ์

8.1.2.5 แนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก

8.1.2.6 แนวปฏิบัติการใช้งานระบบสารสนเทศทางการแพทย์

8.1.2.7 แนวปฏิบัติการใช้งานระบบสารสนเทศการศึกษา

8.1.2.8 แนวปฏิบัติการใช้งานระบบสารสนเทศเพื่อการวิจัยและพัฒนา

8.1.2.9 แนวปฏิบัติการใช้ E-Mail, Social Media และ Chat Application

8.2 นโยบายเพื่อป้องกันความเสียหายของระบบ และข้อมูลสารสนเทศการสำรองและกู้คืนข้อมูล

8.2.1 วัตถุประสงค์

8.2.1.1 เพื่อรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่การยืนยันตัวบุคคล (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

8.2.1.2 เพื่อกำหนดให้มีแผนการดำเนินงานด้านการรักษาความปลอดภัยของระบบเครือข่ายและระบบข้อมูลทั้งแผนดำเนินการดูแลระบบและแผนป้องกันการโจมตีทางไซเบอร์

8.2.1.3 เพื่อกำหนดให้มีแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อป้องกันการหยุดชะงักในการดำเนินงานขององค์กรที่เป็นผลมาจากความเสียหายทางกายภาพ ความเสียหายจากภัยคุกคามทางไซเบอร์หรือภัยพิบัติ

8.2.1.4 เพื่อจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

8.2.2 แนวปฏิบัติที่เกี่ยวข้อง

8.2.2.1 แนวปฏิบัติในการควบคุมสินทรัพย์สารสนเทศ

8.2.2.2 แนวปฏิบัติการรักษามั่นคงปลอดภัยระบบเครือข่ายของราชวิทยาลัยจุฬาภรณ์

8.2.2.3 แนวปฏิบัติการรักษามั่นคงปลอดภัยศูนย์ข้อมูลหลักของราชวิทยาลัยจุฬาภรณ์

8.2.2.4 แนวปฏิบัติการป้องกันการโจมตีทางไซเบอร์

8.2.2.5 แนวปฏิบัติการจัดทำระบบสำรองสำหรับงานสารสนเทศ

8.2.2.6 แนวปฏิบัติการเตรียมความพร้อมกรณีฉุกเฉินในกรณีไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์

8.2.2.7 แนวปฏิบัติการการจัดหา การพัฒนา และการบำรุงรักษาระบบ

8.2.2.8 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเครื่องมือทางการแพทย์

8.2.2.9 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยอุปกรณ์ Internet of Things (IoT), กล้องวงจรปิด และระบบควบคุมอัตโนมัติ

8.3 นโยบายเพื่อการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

8.3.1 วัตถุประสงค์

8.3.1.1 เพื่อให้ราชวิทยาลัยจุฬาภรณ์ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

8.3.1.2 เพื่อทบทวนถึงความสอดคล้องของนโยบายกับกฎหมายหรือระเบียบปฏิบัติที่เกี่ยวข้อง

8.3.2 แนวปฏิบัติที่เกี่ยวข้อง

8.3.2.1 แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ

ประกาศ ณ วันที่ 26 เดือน กรกฎาคม พ.ศ. 2562

(ศาสตราจารย์ นายแพทย์นิธิ มหานนท์)

เลขาธิการราชวิทยาลัยจุฬาภรณ์