ประกาศวิทยาลัยเทคนิคอุบลราชธานี
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของวิทยาลัยเทคนิคอุบลราชธานี พ.ศ. 2569

โดยที่เป็นการสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของวิทยาลัยเทคนิคอุบลราชธานี เพื่อให้การบริหารจัดการข้อมูล ระบบสารสนเทศ และโครงสร้างพื้นฐานทางเทคโนโลยีดิจิทัลของวิทยาลัย มีความมั่นคงปลอดภัย มีความพร้อมใช้งาน สามารถรักษาความลับและความถูกต้องครบถ้วนของข้อมูล ตลอดจนป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายแก่ทางราชการ ผู้เรียน ครู บุคลากร และผู้มีส่วนได้ส่วนเสียของวิทยาลัย

อาศัยอำนาจตามความในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 ประกอบกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 วิทยาลัยเทคนิคอุบลราชธานี จึงออกประกาศไว้ ดังต่อไปนี้

หมวด 1
บททั่วไป

1. ประกาศนี้เรียกว่า “ประกาศวิทยาลัยเทคนิคอุบลราชธานี เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของวิทยาลัยเทคนิคอุบลราชธานี พ.ศ. 2569”
2. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป
3. ในประกาศนี้
    3.1 “วิทยาลัย” หมายความว่า วิทยาลัยเทคนิคอุบลราชธานี
    3.2 “ผู้อำนวยการ” หมายความว่า ผู้อำนวยการวิทยาลัยเทคนิคอุบลราชธานี
    3.3 “ข้อมูล” หมายความว่า ข้อเท็จจริงหรือสิ่งที่ถือได้ว่าเป็นข้อเท็จจริงในรูปแบบอิเล็กทรอนิกส์หรือรูปแบบอื่นใด ซึ่งอยู่ในความครอบครองหรือควบคุมดูแลของวิทยาลัย
    3.4 “ระบบสารสนเทศ” หมายความว่า ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบฐานข้อมูล ระบบงานประยุกต์ ระบบบริการคลาวด์ อุปกรณ์ประกอบ และซอฟต์แวร์ที่วิทยาลัยจัดหา พัฒนา หรือใช้งาน

3.5 “ผู้ใช้งาน” หมายความว่า ผู้บริหาร ครู บุคลากรทางการศึกษา ลูกจ้าง นักเรียน นักศึกษา ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคคลอื่นใดซึ่งได้รับอนุญาตให้เข้าถึงข้อมูลหรือระบบสารสนเทศของวิทยาลัย

3.6 “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

3.7 “เหตุการณ์ผิดปกติ” หมายความว่า เหตุการณ์ที่อาจกระทบต่อความลับ ความถูกต้องครบถ้วน หรือความพร้อมใช้งานของข้อมูลหรือระบบสารสนเทศ

3.8 “คณะกรรมการ” หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของวิทยาลัย

4. ให้ผู้อำนวยการรักษาการตามประกาศนี้ และมีอำนาจตีความวินิจฉัยปัญหาอันเกิดจากการปฏิบัติตามประกาศนี้

หมวด 2

นโยบายและโครงสร้างการกำกับดูแล

5. วิทยาลัยยึดถือหลักการพื้นฐานสามประการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ได้แก่

5.1 การรักษาความลับ (Confidentiality) ข้อมูลต้องเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

5.2 ความถูกต้องครบถ้วน (Integrity) ข้อมูลต้องถูกต้อง ครบถ้วน และไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต

5.3 ความพร้อมใช้งาน (Availability) ข้อมูลและระบบสารสนเทศต้องพร้อมใช้งานเมื่อผู้ได้รับอนุญาตต้องการใช้

6. ให้มีคณะกรรมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของวิทยาลัย ประกอบด้วย

6.1 ผู้อำนวยการวิทยาลัย เป็นประธานกรรมการ

6.2 รองผู้อำนวยการฝ่ายแผนงานและความร่วมมือ เป็นรองประธานกรรมการ

6.3 รองผู้อำนวยการทุกฝ่าย หัวหน้าแผนกวิชาที่เกี่ยวข้อง และหัวหน้างานศูนย์ข้อมูลสารสนเทศ เป็นกรรมการ

6.4 เจ้าหน้าที่ผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ เป็นกรรมการและเลขานุการ

7. คณะกรรมการมีอำนาจหน้าที่ ดังนี้

7.1 กำหนด ทบทวน และเสนอปรับปรุงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

7.2 จัดทำและทบทวนทะเบียนทรัพย์สินสารสนเทศ และการประเมินความเสี่ยงด้านสารสนเทศ

7.3 กำกับ ติดตาม และประเมินผลการปฏิบัติตามประกาศนี้

7.4 พิจารณาและสั่งการเมื่อเกิดเหตุการณ์ผิดปกติหรือเหตุละเมิดความมั่นคงปลอดภัย

7.5 เสนอแผนการฝึกอบรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้ใช้งาน

8. ให้งานศูนย์ข้อมูลสารสนเทศเป็นหน่วยงานรับผิดชอบหลักในการปฏิบัติตามประกาศนี้ และเป็นศูนย์กลางการรับแจ้งเหตุการณ์ผิดปกติด้านสารสนเทศของวิทยาลัย

หมวด 3
การจำแนกชั้นความลับและการบริหารทรัพย์สินสารสนเทศ

9. ให้จำแนกชั้นความลับของข้อมูลของวิทยาลัยออกเป็นสี่ระดับ ดังนี้

9.1 ข้อมูลสาธารณะ (Public) ข้อมูลที่เปิดเผยได้ทั่วไป เช่น ข่าวประชาสัมพันธ์ ประกาศรับสมัคร ผลการจัดซื้อจัดจ้างที่ต้องเปิดเผยตามกฎหมาย

9.2 ข้อมูลใช้ภายใน (Internal) ข้อมูลที่ใช้ในการปฏิบัติงานภายในวิทยาลัย ซึ่งการเปิดเผยอาจก่อความเสียหายเล็กน้อย เช่น คู่มือปฏิบัติงาน รายงานการประชุมทั่วไป

9.3 ข้อมูลลับ (Confidential) ข้อมูลที่การเปิดเผยอาจก่อความเสียหายอย่างมีนัยสำคัญ เช่น ข้อมูลส่วนบุคคลของผู้เรียนและบุคลากร ข้อมูลผลการเรียน ข้อมูลสุขภาพ ข้อมูลทางการเงิน

9.4 ข้อมูลลับที่สุด (Highly Confidential) ข้อมูลที่การเปิดเผยอาจก่อความเสียหายร้ายแรง เช่น ข้อสอบก่อนใช้สอบ รหัสผ่านระบบ กุญแจเข้ารหัส ข้อมูลการสอบสวนทางวินัย

10. ให้ผู้รับผิดชอบข้อมูลแต่ละรายการกำหนดชั้นความลับ ระบุเจ้าของข้อมูล และบันทึกไว้ในทะเบียนทรัพย์สินสารสนเทศ ซึ่งต้องทบทวนอย่างน้อยปีละหนึ่งครั้ง

11. การนำข้อมูลชั้นความลับตั้งแต่ระดับข้อมูลลับขึ้นไปออกนอกวิทยาลัย ไม่ว่าโดยสื่อบันทึกข้อมูลไปรษณีย์อิเล็กทรอนิกส์ หรือบริการคลาวด์ ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการหรือผู้ที่ได้รับมอบหมาย และต้องเข้ารหัสข้อมูลก่อนทุกครั้ง

12. การทำลายข้อมูลและสื่อบันทึกข้อมูลที่มีชั้นความลับ ต้องดำเนินการด้วยวิธีที่ไม่สามารถกู้คืนข้อมูลได้ และจัดทำบันทึกการทำลายไว้เป็นหลักฐาน

หมวด 4
การควบคุมการเข้าถึงและการพิสูจน์ตัวตน

13. การให้สิทธิเข้าถึงข้อมูลและระบบสารสนเทศให้เป็นไปตามหลักความจำเป็นเท่าที่ต้องรู้ (Need to Know) และหลักสิทธิน้อยที่สุดเท่าที่จำเป็น (Least Privilege)

14. บัญชีผู้ใช้งาน

14.1 ผู้ใช้งานต้องมีบัญชีผู้ใช้งานเป็นของตนเอง ห้ามใช้บัญชีร่วมกัน และห้ามให้ผู้อื่นใช้บัญชีของตน

14.2 การขอมี แก้ไข หรือยกเลิกบัญชีผู้ใช้งาน ให้ยื่นตามแบบที่วิทยาลัยกำหนด และต้องได้รับอนุมัติจากผู้บังคับบัญชาชั้นต้น

14.3 เมื่อผู้ใช้งานพ้นจากหน้าที่ ย้าย ลาออก เกษียณอายุราชการ หรือสำเร็จการศึกษา ให้หน่วยงานต้นสังกัดแจ้งงานศูนย์ข้อมูลสารสนเทศเพื่อระงับหรือยกเลิกสิทธิภายในเจ็ดวันทำการ

14.4 ให้ทบทวนสิทธิการเข้าถึงของผู้ใช้งานทุกรายอย่างน้อยปีละหนึ่งครั้ง

15. รหัสผ่าน

15.1 รหัสผ่านต้องมีความยาวไม่น้อยกว่า 12 ตัวอักษร ประกอบด้วยตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษ

15.2 ห้ามใช้รหัสผ่านที่คาดเดาได้ง่าย เช่น เลขประจำตัวประชาชน วันเดือนปีเกิด ชื่อหน่วยงาน หรือรหัสผ่านที่เคยถูกเปิดเผยมาก่อน

15.3 ห้ามจดรหัสผ่านไว้ในที่เปิดเผย ห้ามบันทึกรหัสผ่านในรูปแบบข้อความธรรมดา และห้ามส่งรหัสผ่านผ่านช่องทางที่ไม่มีการเข้ารหัส

15.4 ต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่ารหัสผ่านรั่วไหล และต้องเปลี่ยนรหัสผ่านเริ่มต้นที่ระบบกำหนดให้ในการเข้าใช้งานครั้งแรก

15.5 ระบบต้องจัดเก็บรหัสผ่านในรูปแบบที่ผ่านการเข้ารหัสทางเดียว (Hash) พร้อมค่าสุ่ม (Salt) ห้ามจัดเก็บเป็นข้อความธรรมดา

16. ให้ใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) สำหรับบัญชีผู้ดูแลระบบ บัญชีที่เข้าถึงข้อมูลลับหรือลับที่สุด และการเข้าถึงระบบจากภายนอกเครือข่ายของวิทยาลัย

17. การเข้าถึงระบบจากระยะไกลต้องกระทำผ่านช่องทางที่มีการเข้ารหัส เช่น เครือข่ายส่วนตัวเสมือน (VPN) และต้องบันทึกข้อมูลการเข้าใช้งานไว้ทุกครั้ง

หมวด 5
ความมั่นคงปลอดภัยของระบบเครือข่ายและเครื่องคอมพิวเตอร์

18. ให้แบ่งแยกเครือข่ายของวิทยาลัยออกเป็นส่วน ๆ ตามลักษณะการใช้งานและระดับความเสี่ยง อย่างน้อยต้องแยกเครือข่ายสำหรับงานบริหาร เครือข่ายสำหรับการเรียนการสอน เครือข่ายสำหรับผู้มาติดต่อ และเครือข่ายสำหรับเครื่องแม่ข่ายออกจากกัน

19. ให้ติดตั้งและกำหนดค่าอุปกรณ์ป้องกันการบุกรุกและระบบกรองข้อมูล เช่น ไฟร์วอลล์ ระบบตรวจจับและป้องกันการบุกรุก ให้เหมาะสมกับความเสี่ยง และทบทวนกฎการอนุญาตอย่างน้อยปีละสองครั้ง

20. เครื่องคอมพิวเตอร์และอุปกรณ์ปลายทางที่เชื่อมต่อเครือข่ายของวิทยาลัย ต้อง

20.1 ติดตั้งโปรแกรมป้องกันมัลแวร์ที่มีการปรับปรุงฐานข้อมูลอย่างสม่ำเสมอ

20.2 ปรับปรุงระบบปฏิบัติการและซอฟต์แวร์ให้เป็นรุ่นที่ผู้พัฒนายังให้การสนับสนุนด้านความมั่นคงปลอดภัย

20.3 ตั้งค่าการล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานเกิน 15 นาที

20.4 ใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

21. ห้ามผู้ใช้งานติดตั้งอุปกรณ์เครือข่ายใด ๆ เช่น อุปกรณ์กระจายสัญญาณไร้สาย เราเตอร์ หรืออุปกรณ์แปลงที่อยู่เครือข่าย เข้ากับเครือข่ายของวิทยาลัย โดยไม่ได้รับอนุญาตจากงานศูนย์ข้อมูลสารสนเทศ

22. ให้จัดให้มีการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า 90 วัน ตามมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม โดยข้อมูลดังกล่าวต้องมีความถูกต้อง สามารถระบุตัวผู้ใช้งานได้ มีการเทียบเวลากับแหล่งเวลามาตรฐาน และต้องมีมาตรการป้องกันการแก้ไขเปลี่ยนแปลง

23. การเข้าถึงห้องเครื่องแม่ข่ายและห้องอุปกรณ์เครือข่าย ต้องมีการควบคุมทางกายภาพ มีบันทึกการเข้าออก มีระบบควบคุมอุณหภูมิ ระบบไฟฟ้าสำรอง และระบบป้องกันอัคคีภัยที่เหมาะสม

หมวด 6
การสำรองข้อมูลและการบริหารความต่อเนื่อง

24. ให้สำรองข้อมูลของระบบสารสนเทศที่สำคัญตามหลักการสำรองข้อมูลสามชุด สองรูปแบบสื่อ และเก็บนอกสถานที่อย่างน้อยหนึ่งชุด (3-2-1) โดยกำหนดรอบการสำรองข้อมูลตามความสำคัญของระบบ แต่ต้องไม่น้อยกว่าสัปดาห์ละหนึ่งครั้ง

25. ข้อมูลสำรองที่มีชั้นความลับตั้งแต่ระดับข้อมูลลับขึ้นไป ต้องเข้ารหัสทั้งขณะจัดเก็บและขณะรับส่ง

26. ให้ทดสอบการกู้คืนข้อมูลจากข้อมูลสำรองอย่างน้อยปีละหนึ่งครั้ง และจัดทำรายงานผลการทดสอบเสนอคณะกรรมการ

27. ให้จัดทำแผนบริหารความต่อเนื่องของระบบสารสนเทศ ซึ่งอย่างน้อยต้องระบุระบบงานสำคัญ ระยะเวลาเป้าหมายในการกู้คืนระบบ ระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหาย ผู้รับผิดชอบ และขั้นตอนการปฏิบัติ

หมวด 7
การบริหารจัดการเหตุการณ์ผิดปกติและเหตุละเมิด

28. ผู้ใช้งานที่พบหรือสงสัยว่ามีเหตุการณ์ผิดปกติ เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การติดมัลแวร์หรือแรนซัมแวร์ การสูญหายของอุปกรณ์ที่มีข้อมูลของวิทยาลัย หรือการได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง ต้องแจ้งงานศูนย์ข้อมูลสารสนเทศโดยทันที และอย่างช้าต้องไม่เกิน 24 ชั่วโมงนับแต่ทราบเหตุ

29. เมื่อได้รับแจ้งเหตุ ให้งานศูนย์ข้อมูลสารสนเทศดำเนินการตามลำดับ ดังนี้

29.1 ประเมินและจำแนกระดับความรุนแรงของเหตุการณ์

29.2 จำกัดขอบเขตความเสียหาย เช่น ตัดการเชื่อมต่อระบบที่ได้รับผลกระทบออกจากเครือข่าย

29.3 เก็บรักษาพยานหลักฐานดิจิทัลโดยไม่ทำให้เสียหายหรือเปลี่ยนแปลง

29.4 กำจัดสาเหตุและกู้คืนระบบให้กลับสู่สภาพปกติ

29.5 รายงานผู้อำนวยการและคณะกรรมการ พร้อมจัดทำรายงานบทเรียนที่ได้รับ

30. ในกรณีที่เหตุการณ์ผิดปกตินั้นเป็นการละเมิดข้อมูลส่วนบุคคล ให้ดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และหากการละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเจ้าของข้อมูลส่วนบุคคลทราบพร้อมแนวทางเยียวยาโดยไม่ชักช้า ทั้งนี้ ตามมาตรา 37 (4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

31. ในกรณีที่เหตุการณ์ผิดปกติเข้าข่ายเป็นภัยคุกคามทางไซเบอร์ ให้ประสานงานและรายงานต่อหน่วยงานที่เกี่ยวข้องตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

หมวด 8
ผู้ให้บริการภายนอกและการพัฒนาระบบ

32. การจัดซื้อจัดจ้างพัฒนาระบบสารสนเทศหรือใช้บริการจากผู้ให้บริการภายนอก ต้องกำหนดข้อตกลงด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลไว้ในสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคล อย่างน้อยต้องครอบคลุมขอบเขตการเข้าถึงข้อมูล มาตรการรักษาความมั่นคงปลอดภัย การรักษาความลับ การแจ้งเหตุละเมิด และการส่งคืนหรือทำลายข้อมูลเมื่อสิ้นสุดสัญญา

33. การพัฒนาระบบสารสนเทศต้องคำนึงถึงความมั่นคงปลอดภัยตั้งแต่ขั้นออกแบบ (Security by Design) และการคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบและโดยค่าเริ่มต้น (Privacy by Design and by Default)

34. ห้ามนำข้อมูลจริงที่มีข้อมูลส่วนบุคคลไปใช้ในสภาพแวดล้อมสำหรับการพัฒนาหรือทดสอบ เว้นแต่ได้ผ่านกระบวนการทำให้ไม่สามารถระบุตัวบุคคลได้แล้ว

35. ระบบสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ ต้องผ่านการตรวจสอบช่องโหว่ก่อนเปิดให้บริการและตรวจสอบซ้ำอย่างน้อยปีละหนึ่งครั้ง

หมวด 9

การสร้างความตระหนักรู้ การตรวจสอบ และบทกำหนดโทษ

36. ให้วิทยาลัยจัดการฝึกอบรมหรือกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลแก่ครู บุคลากร และผู้เรียน อย่างน้อยปีการศึกษาละหนึ่งครั้ง

37. ให้มีการตรวจสอบการปฏิบัติตามประกาศนี้อย่างน้อยปีละหนึ่งครั้ง และรายงานผลต่อผู้อำนวยการ

38. ผู้ใช้งานซึ่งฝ่าฝืนหรือไม่ปฏิบัติตามประกาศนี้ ให้ดำเนินการดังนี้

    38.1 กรณีเป็นข้าราชการครูหรือบุคลากรทางการศึกษา ให้ดำเนินการทางวินัยตามกฎหมายว่าด้วยระเบียบข้าราชการครูและบุคลากรทางการศึกษา

    38.2 กรณีเป็นนักเรียนหรือนักศึกษา ให้ดำเนินการตามระเบียบว่าด้วยการปกครองนักเรียนนักศึกษาของวิทยาลัย

    38.3 กรณีเป็นลูกจ้างหรือผู้รับจ้าง ให้ดำเนินการตามสัญญาจ้างหรือข้อตกลงที่เกี่ยวข้อง

    38.4 หากการกระทำนั้นเข้าข่ายเป็นความผิดตามกฎหมาย ให้ดำเนินคดีตามกฎหมายต่อไป ทั้งนี้ไม่เป็นการตัดสิทธิของวิทยาลัยในการเรียกร้องค่าเสียหายทางแพ่ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป