



ประกาศวิทยาลัยเทคนิคบางสะพาน
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของวิทยาลัยเทคนิคบางสะพาน พ.ศ. ๒๕๖๘

อาศัยอำนาจตามความในมาตรา ๓๐ แห่งพระราชบัญญัติระเบียบบริหารราชการกระทรวงศึกษาธิการ พ.ศ. ๒๕๔๖ มาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของภาครัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ วิทยาลัยเทคนิคบางสะพานโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศวิทยาลัยเทคนิคบางสะพาน เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของวิทยาลัยเทคนิคบางสะพาน พ.ศ. ๒๕๖๘"

ข้อ ๒ ประกาศนี้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้มี ๒ ส่วน ดังนี้

๓.๑ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ โดยรายละเอียดประกอบด้วยเนื้อหาสาระสำคัญในประเด็นดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย โดยจะต้องครอบคลุมเนื้อหาอย่างน้อย ดังนี้

- การเข้าถึงระบบสารสนเทศต้องดำเนินการยืนยันตัวตนโดยใช้รหัสผ่านหรือรหัสประจำตัวที่สถานศึกษากำหนดเท่านั้น เพื่อรักษาความมั่นคงปลอดภัยของระบบและข้อมูลสารสนเทศ และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

- การเข้าถึงระบบเครือข่ายต้องดำเนินการยืนยันตัวตนด้วยรหัสผ่านทุกครั้งก่อนการใช้งาน เพื่อรักษาความมั่นคงปลอดภัยของระบบเครือข่ายและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

- การเข้าถึงระบบปฏิบัติการต้องดำเนินการยืนยันตัวตนโดยใช้รหัสผ่านหรือรหัสประจำตัวที่สถานศึกษากำหนดเท่านั้น ทั้งนี้เพื่อรักษาความมั่นคงปลอดภัยของระบบและข้อมูล และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

- การเข้าถึงระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) ผู้ใช้งานระบบคอมพิวเตอร์และโปรแกรมประยุกต์ (Application) ทุกคน ต้องดำเนินการยืนยันตัวตนก่อนการใช้งานระบบทุกครั้ง ทั้งนี้เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูล ความถูกต้องในการใช้งาน และเพื่อป้องกันการเข้าถึงระบบโดยมิชอบ

หรือไม่...

“เรียนดี มีคุณธรรม”

หรือไม่ได้รับอนุญาต ผู้ใช้งานต้องปฏิบัติตามระเบียบและข้อกำหนดด้านความปลอดภัยสารสนเทศของหน่วยงานอย่างเคร่งครัด

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน

วิทยาลัยเทคนิคบางสะพาน มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และอยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติต่อเนื่อง

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วิทยาลัยเทคนิคบางสะพาน มีนโยบายในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง โดยหน่วยงานตรวจสอบภายในของวิทยาลัยเทคนิคบางสะพาน หรือหน่วยงานตรวจสอบภายในของสำนักงานคณะกรรมการการอาชีวศึกษา

(๔) การสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วิทยาลัยเทคนิคบางสะพาน มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของวิทยาลัยเทคนิคบางสะพาน

ข้อ ๕ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) ดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบหมายอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๕.๑ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและผ่านการฝึกอบรมหลักสูตรการสร้างความรู้ความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตโดยมีเนื้อหาอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึง สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มี

กระบวนการ...

“เรียนดี มีคุณธรรม”

กระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

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

ข้อ ๕.๒ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึง โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้รหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับของสารสนเทศ โดยให้ปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่นใดที่ได้ประกาศใช้บังคับในภายหลัง

ข้อ ๕.๓ มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connection) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือประยุกต์ใช้งานตามภารกิจ

ข้อ ๕.๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีเนื้อหาอย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้มีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๕.๕ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๕.๕ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ๑ ครั้ง

(๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) เพื่อให้หน่วยงานได้ทราบถึงจุดอ่อนความเสี่ยงและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ

(๓) ในกรณีที่หน่วยงานไม่มีผู้ทำหน้าที่ในการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคง

ข้อ ๕.๔...

ปลอดภัยสารสนเทศ ให้ผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยสารสนเทศจากภายนอกดำเนินการดังกล่าว

ข้อ ๖ กรณีระบบหรือคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรือข้อมูลสูญหาย ใดๆ แก่หน่วยงานหรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแผนปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พึงมีบทวิทยาระดับสูงสุดของหน่วยงานเป็นผู้มีอำนาจดำเนินการความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๗ ตามประกาศในฉบับนี้ ให้วิทยาลัยเทคนิคบางสะพาน ในสังกัดสำนักงานคณะกรรมการการอาชีวศึกษา ทั้งภาครัฐและเอกชน ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๖

ข้อ ๘ ให้งานศูนย์ข้อมูลสารสนเทศ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้รวมถึงที่กำหนดให้มีการปฏิบัติที่ชัดเจน

ประกาศ ณ วันที่ ๒๗ เดือน มกราคม พ.ศ. ๒๕๖๙

(ลงชื่อ)



(นายนิมิตร ศรียาภัย)

ผู้อำนวยการวิทยาลัยเทคนิคบางสะพาน