# ประกาศวิทยาลัยเทคนิคปัว
## เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่าย

---

นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่าย จัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของวิทยาลัยเทคนิคปัว ให้อยู่ระดับมาตรฐานสากล และเป็นแนวทางปฏิบัติของผู้ใช้งานเทคโนโลยีสารสนเทศและเครือข่าย วิทยาลัยเทคนิคปัว โดยมีรายละเอียดดังต่อไปนี้

**๑. หลักการและเหตุผล**

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและเครือข่าย เพื่อให้ระบบต่าง ๆ ของวิทยาลัยเทคนิคปัว สามารถดำเนินการได้ต่อเนื่องและมั่นคงปลอดภัย รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศและเครือข่ายที่ไม่ถูกต้อง ขาดความตระหนักในปัญหาที่อาจจะเกิดขึ้นของผู้ใช้งานภายในเอง หรือจากการถูกคุกคามจากภายนอก

วิทยาลัยเทคนิคปัว จึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่าย โดยกำหนดให้มี มาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านต่าง ๆ

**๒. วัตถุประสงค์**

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ โดยการคงไว้ด้วยความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และมีสภาพพร้อมใช้งาน (Availability) โดยจะต้องสามารถตรวจสอบความถูกต้อง (Authenticity) ความรับผิดชอบ (Accountability) ไม่สามารถปฏิเสธความรับผิดชอบ (Non-repudiation) และมีความน่าเชื่อถือ (Reliability)

๒.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่มีมาตรฐานและมีการปรับปรุงอย่างต่อเนื่อง

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับวิทยาลัยเทคนิคปัว ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศและเครือข่ายของวิทยาลัยเทคนิคปัว

**๓. นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่าย**

๓.๑ ส่งเสริมความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่ายของวิทยาลัยเทคนิคปัว ให้สามารถตอบสนองต่อพันธกิจและนโยบายของวิทยาลัยเทคนิคปัว

๓.๒ มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอเพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓.๓ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๔ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

๓.๕ ติดตาม ตรวจสอบการดำเนินงานและปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่ายให้สอดคล้องตามการเปลี่ยนแปลงของโลก

**๔. องค์ประกอบของนโยบาย**

๔.๑ คำนิยาม

๔.๒ นโยบายการเข้าถึงหรือควบคุมการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย

๔.๒.๑ ระบบสารสนเทศ

๔.๒.๒ ระบบเครือข่าย

๔.๒.๓ โปรแกรมประยุกต์และโปรแกรมอรรถประโยชน์

๔.๒.๔ ระบบปฏิบัติการ

๔.๒.๕ ด้านกายภาพ

๔.๓ นโยบายในการรักษาความมั่นคงปลอดภัยของผู้ใช้งาน

๔.๓.๑ แนวปฏิบัติของผู้ใช้งาน

๔.๓.๒ ข้อห้ามสำหรับผู้ใช้งาน

๔.๓.๓ บทลงโทษเมื่อกระทำผิด

๔.๔ แผนสำรองข้อมูลสารสนเทศและเตรียมความพร้อมกรณีฉุกเฉิน

๔.๔.๑ แผนสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน

๔.๔.๒ แผนเตรียมพร้อมกรณีฉุกเฉิน

## คำนิยาม

**คำนิยามโดยทั่วไปที่ใช้ในนโยบายนี้ ประกอบด้วย:**

**ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของวิทยาลัยเทคนิคปัว

**ผู้อำนวยการวิทยาลัยเทคนิคปัว** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของวิทยาลัยเทคนิคปัว ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

**รองผู้อำนวยการวิทยาลัยเทคนิคปัว** หมายถึง ผู้บังคับบัญชาในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของวิทยาลัยเทคนิคปัว และมีอำนาจควบคุมดูแลความเป็นระเบียบเรียบร้อยของสารสนเทศภายในวิทยาลัยเทคนิคปัว

**ศูนย์ข้อมูลสารสนเทศ** หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในวิทยาลัยเทคนิคปัว

**การรักษาความมั่นคง** ปลอดภัย หมายถึง การรักษา ข้อมูล สารสนเทศ และระบบคอมพิวเตอร์ของวิทยาลัยเทคนิคปัว ให้คงไว้ด้วยความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และมีสภาพพร้อมใช้งาน (Availability) โดยจะต้องสามารถตรวจสอบความถูกต้อง (Authenticity) ความรับผิดชอบ (Accountability) ไม่สามารถปฏิเสธความรับผิดชอบ (Non-repudiation) และมีความน่าเชื่อถือ (Reliability)

**มาตรฐาน** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

**ขั้นตอนการปฏิบัติ** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

**แนวปฏิบัติ** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

**ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงของวิทยาลัยเทคนิคปัว เช่น ผู้อำนวยการสถาบัน/สำนัก/กอง เป็นต้น

**ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ความรับผิดชอบที่ได้รับมอบหมายจากผู้บริหารของวิทยาลัยเทคนิคปัว

**ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ความรับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น

**นักศึกษา** หมายถึง นักศึกษาที่กำลังศึกษาอยู่ในวิทยาลัยเทคนิคปัว

**ศิษย์เก่า** หมายถึง นักศึกษาเคยศึกษาอยู่ในวิทยาลัยเทคนิคปัว

**อาจารย์** หมายถึง ข้าราชการ พนักงานราชการครู ลูกจ้างชั่วคราว ที่ทำงานในสายวิชาการของวิทยาลัยเทคนิคปัว

**เจ้าหน้าที่** หมายถึง ลูกจ้างชั่วคราว บุคลากรทางการศึกษา ที่ทำงานในสายสนับสนุนของวิทยาลัยเทคนิคปัว

**หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่วิทยาลัยเทคนิคปัว อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

**ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ให้ข้อมูลในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

**สารสนเทศ** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

**ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

**ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ เช่น ระบบแลน ระบบอินทราเน็ต ระบบอินเตอร์เน็ต เป็นต้น

**ระบบแลน และระบบอินเทอร์เน็ต** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

**ระบบอินเทอร์เน็ต** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

**ระบบเทคโนโลยีสารสนเทศ** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้าง การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

**เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

**สิทธิ์ของผู้ใช้งาน** หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

**สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

**การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางภายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

**เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

**สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

**จดหมายอิเล็กทรอนิกส์** หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหวและเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน

**รหัสผ่าน** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

**ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

**บัญชีผู้ใช้งานคอมพิวเตอร์** หมายถึง บัญชีผู้ใช้งาน นักศึกษา บุคลากร และบุคคลภายนอก เพื่อใช้ในการตรวจสอบยืนยันตัวตน (Authentication) ก่อนเข้าใช้งานระบบสารสนเทศและเครือข่ายภายในวิทยาลัยเทคนิคปัว

**ระบบเครือข่ายเสมือน (Virtual Private Network: VPN)** หมายถึง เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับ-ส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเตอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

**คำนิยามของประเภทข้อมูล และชั้นความลับ**

**นิยามประเภทของข้อมูล**

**ข้อมูลนักศึกษา** หมายถึง ข้อมูลที่เกี่ยวข้องกับนักศึกษาทั้งหมด เช่น ประวัติ ข้อมูลส่วนตัว ข้อมูลลงทะเบียน ข้อมูลการวิจัยของนักศึกษาที่ยังไม่เผยแพร่ ผลการเรียน และกิจกรรมนักศึกษา เป็นต้น จัดเป็นข้อมูลที่เป็นความลับ

**ข้อมูลบุคลากร** หมายถึง ข้อมูลที่เกี่ยวข้องกับอาจารย์ และเจ้าหน้าที่ทั้งหมด เช่น ประวัติ ข้อมูลส่วนตัว เงินเดือน ข้อมูลการวิจัยของอาจารย์ที่ยังไม่เผยแพร่ การลา การเลื่อนขั้น และตำแหน่ง เป็นต้น จัดเป็นข้อมูลที่เป็นความลับ

**ข้อมูลการเงิน** หมายถึง ข้อมูลที่เกี่ยวข้องกับการเงิน เช่น งบประมาณ การเงิน บัญชี เบิกจ่าย และพัสดุ เป็นต้น จัดเป็นข้อมูลที่เป็นความลับ

**ข้อมูลการบริหาร** หมายถึง ข้อมูลที่เกี่ยวข้องกับการบริหารวิทยาลัยเทคนิคปัว นโยบาย โครงการ และการดำเนินงานต่าง ๆ ที่ยังไม่ควรเปิดเผยในขณะนี้ เช่น ร่างนโยบายที่อยู่ระหว่างการจัดทำ หนังสือแต่งตั้งคณะทำงาน ร่างหนังสือบันทึกข้อตกลง เป็นต้น จัดเป็นข้อมูลที่เป็นความลับ

**ข้อมูลสาธารณะ** หมายถึง ข้อมูลที่สามารถเผยแพร่ได้โดยไม่ก่อให้เกิดความเสียหาย และอาจจะช่วยในการส่งเสริมภาพลักษณ์ของวิทยาลัยเทคนิคปัว

**นิยามชั้นความลับของข้อมูล**

**ข้อมูลความลับ** หมายถึง ข้อมูลในระบบคอมพิวเตอร์ของวิทยาลัยเทคนิคปัว ที่เมื่อถูกเผยแพร่ออกไปแล้วก่อให้เกิดความเสียหายหรือเสียประโยชน์ต่อวิทยาลัยเทคนิคปัว หรือเกิดความเสียหายหรือเสียประโยชน์ต่อบุคคลใดบุคคลหนึ่ง

## นโยบายการเข้าถึงหรือควบคุมการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย

**๑. วัตถุประสงค์**

เพื่อกำหนดเป็นมาตรฐานในการควบคุมและรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย จากการเข้าถึงของผู้ใช้งานที่ถูกต้องตามบทบาทหน้าที่หรือภารกิจที่ได้รับมอบหมาย

**๒. นโยบายการเข้าถึงหรือควบคุมการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย**

ในการควบคุมและรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย สามารถแบ่งออกเป็น ๕ ด้าน ประกอบด้วย

๒.๑ ระบบสารสนเทศ

๒.๒ ระบบเครือข่าย

๒.๓ โปรแกรมประยุกต์และโปรแกรมอรรถประโยชน์

๒.๔ ระบบปฏิบัติการ

๒.๕ ด้านกายภาพ

# นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

## ๑. วัตถุประสงค์

๑.๑ เพื่อควบคุมการเข้าถึง ระบบคอมพิวเตอร์ ข้อมูล หรืออุปกรณ์ต่าง ๆ โดยคำนึงถึงการใช้งานตามภารกิจและความรับผิดชอบของผู้ใช้งาน

๑.๒ เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์และการมอบอำนาจของหน่วยงานที่รับผิดชอบ

๑.๓ เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจ สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

## ๒. แนวปฏิบัติ

แนวปฏิบัติในการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ เป็นแนวปฏิบัติที่ระบุถึงแนวทางในภาพรวมในการควบคุมการเข้าใช้งานของผู้ใช้ที่มีหน้าที่รับผิดชอบต่อระบบคอมพิวเตอร์ ข้อมูล หรืออุปกรณ์ต่าง ๆ ดังนี้

### ๒.๑ ผู้ใช้งานภายใน

๒.๑.๑ ระบบสารสนเทศใด ๆ ภายในวิทยาลัยเทคนิคปัว จะต้องมีผู้รับผิดชอบ เจ้าของ หรือผู้ดูแลระบบที่จะต้องทำหน้าที่ในการรักษาความมั่นคงปลอดภัยและกำหนดสิทธิ์การเข้าถึงให้แก่ผู้ใช้งานตามภารกิจ หรือตามความรับผิดชอบที่ได้รับมอบหมายอย่างเหมาะสม

๒.๑.๒ ผู้ใช้งานที่ได้รับสิทธิ์เท่านั้นจึงจะสามารถเข้าถึงระบบสารสนเทศนั้น ๆ ได้ โดยจะต้องมีกระบวนการตรวจสอบยืนยันตัวตนของผู้ใช้งาน (Authentication) ที่ปลอดภัย น่าเชื่อถือและเหมาะสมก่อนการเข้าใช้งานระบบสารสนเทศ

๒.๑.๓ ผู้ใช้งานที่ได้รับสิทธิ์เข้าถึงระบบสารสนเทศ จะต้องได้รับมอบสิทธิ์ที่อยู่ในขอบเขตที่ตรงกับภาระหน้าที่ของผู้ใช้งานแต่ละคนและจะต้องไม่มอบสิทธิ์ที่มากกว่าภาระหน้าที่ความรับผิดชอบ (Authorization)

๒.๑.๔ ในกรณีที่ผู้ใช้งานเข้าใช้งานระบบสารสนเทศที่มีความสำคัญ หรือระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลที่จัดอยู่ในชั้นความลับ เช่น ข้อมูลการเงิน ข้อมูลบุคลากร ข้อมูลการบริหารและข้อมูลนักศึกษา จะต้องมีการจำกัดเวลาในการเชื่อมต่อเมื่อไม่มีการใช้งานระยะเวลาหนึ่ง จะต้องถูกบังคับให้ออกจากระบบ

๒.๑.๕ ในกรณีที่เป็นระบบสารสนเทศเฉพาะที่ถูกใช้งานผ่านเครือข่ายภายในเท่านั้น หรือใช้ผ่านระบบอินเทอร์เน็ตจะต้องมีกระบวนการตรวจสอบยืนยันตัวตนของผู้ใช้งาน (Authentication) และมีกระบวนการเข้ารหัสข้อมูลอีกชั้นหนึ่ง (SSL VPN) เมื่อผู้ใช้เข้าจากเครือข่ายภายนอก

๒.๑.๖ ผู้ใช้งานที่นำคอมพิวเตอร์ส่วนตัว โทรศัพท์ หรืออุปกรณ์ ใด ๆ เข้ามาเชื่อมต่อกับระบบสารสนเทศหรือเครือข่ายภายในวิทยาลัยเทคนิคปัว จะต้องเป็นผู้รับผิดชอบผลที่เกิดจากการกระทำผ่านคอมพิวเตอร์ส่วนตัว โทรศัพท์ หรืออุปกรณ์ใด ๆ เหล่านั้น

### ๒.๒ ผู้ใช้งานภายนอก (ผู้รับเหมาดำเนินการ หรือบุคคลจากหน่วยงานภายนอก)

๒.๒.๑ ในกรณีที่ผู้ใช้งานภายนอกต้องการเข้าถึงหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศที่มีความสำคัญ ประกอบด้วย ระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลที่จัดอยู่ในชั้นความลับ เช่น ข้อมูลการเงิน ข้อมูลบุคลากร ข้อมูลการบริหารและข้อมูลนักศึกษา จะต้องได้รับสิทธิ์อนุญาตเป็นลายลักษณ์อักษร หรือมีหนังสือสัญญาที่เกี่ยวข้อง ที่ถูกอนุมัติโดย ผู้อำนวยการ ประจำหน่วยงานที่เป็นเจ้าของระบบสารสนเทศนั้น

๒.๒.๒ ในกรณีที่ผู้ใช้งานภายนอกต้องการเข้าถึงหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศทั่วไป เช่น เว็บไซต์ อุปกรณ์ต่าง ๆ หรือข้อมูลกล้องวงจรปิด จะต้องได้รับสิทธิ์อนุญาตจากผู้รับผิดชอบ หรือผู้ดูแลระบบอาจเป็นลายลักษณ์อักษรหรือไม่ขึ้นกับความเหมาะสม และควรมีการบันทึกข้อมูลการเข้าถึงหรือแก้ไขในแต่ละครั้ง

๒.๒.๓ ผู้ใช้งานภายนอกที่ได้รับสิทธิ์เท่านั้น จึงจะสามารถเข้าใช้เครื่องคอมพิวเตอร์ หรืออุปกรณ์ของวิทยาลัยเทคนิคปัวได้ โดยสิทธิ์ที่ได้รับนั้นให้พิจารณาเป็นกรณี ๆ ไป เช่น เมื่อจำเป็นต้องมีการประชุมพูดคุยกับบุคคลจากหน่วยงานภายนอก หรือเมื่อมีการเช่าพื้นที่ห้องอบรมจากหน่วยงานภายนอก โดยกำหนดให้ผู้รับผิดชอบเครื่องคอมพิวเตอร์ หรืออุปกรณ์ของวิทยาลัย เป็นผู้รับผิดชอบในการมอบสิทธิ์แก่ผู้ใช้งานภายนอก

๒.๒.๔ ผู้ใช้งานภายนอกที่ได้รับสิทธิ์เท่านั้น จึงจะสามารถนำคอมพิวเตอร์ส่วนตัว โทรศัพท์ หรืออุปกรณ์ใด ๆ เข้ามาเชื่อมต่อกับระบบสารสนเทศ หรือเครือข่ายภายในวิทยาลัยเทคนิคปัว โดยสิทธิ์ที่ได้รับนั้นให้พิจารณาเป็นกรณี ๆ ไป เช่น เมื่อจำเป็นต้องมีการประชุมพูดคุยกับบุคคลจากหน่วยงานภายนอก หรือเมื่อมีการเช่าพื้นที่ห้องอบรมจากหน่วยงานภายนอก โดยกำหนดให้ผู้รับผิดชอบระบบสารสนเทศ นั้น ๆ เป็นผู้รับผิดชอบในการมอบสิทธิ์แก่ผู้ใช้งานภายนอก

## นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเครือข่าย

**๑. วัตถุประสงค์**

๑.๑ เพื่อควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์แบบมีสายและไร้สายทั้งภายนอกและภายในองค์กร รวมถึงเครือข่ายเสมือน โดยคำนึงถึงการใช้งานตามภารกิจและความรับผิดชอบของผู้ใช้งาน

๑.๒ เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจของหน่วยงานที่รับผิดชอบ

๑.๓ เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

**๒. แนวทางปฏิบัติ**

๒.๑ ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ

๒.๒ หน่วยงาน บริษัทหรือบุคคลภายนอกจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ของวิทยาลัยเทคนิคปัว ต้องได้รับอนุญาตจากผู้อำนวยการวิทยาลัยเทคนิคปัว

๒.๓ ห้ามผู้ใดทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณเครือข่าย (Switch) หรืออุปกรณ์ที่เกี่ยวข้องกับระบบเครือข่ายโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๒.๔ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ

๒.๔.๑ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๒.๔.๒ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังเครือข่ายอื่นๆ ภายนอก หน่วยงานควรมีการเชื่อมต่ออุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๒.๔.๓ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายหน่วยงานในลักษณะที่ผิดปกติ

๒.๔.๔ การเข้าสู่ระบบเครือข่ายภายในหน่วยงานโดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้องมีการบันทึกเข้า (Login) และมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๒.๔.๕ หมายเลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานจากภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๒.๔.๖ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๔.๗ การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะที่จำเป็นเท่านั้น

๒.๕ วิทยาลัยเทคนิคปัว กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๒.๕.๑ ความเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้เสมือนกับข้อมูลที่สามารถรักษาความถูกต้อง คงครบถ้วน แท้จริงและระบุตัวบุคคลที่เข้าถึงข้อมูลดังกล่าวได้และข้อมูลที่จัดเก็บนั้น ต้องกำหนดชั้นความลับการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการใช้ข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

๒.๕.๒ ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๒.๕.๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกข้อมูลให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๒.๖ วิทยาลัยเทคนิคปัว กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากรายงานตามแนวทางดังนี้

๒.๖.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องแจ้งเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้อำนวยการวิทยาลัยเทคนิคปัว

๒.๖.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๒.๖.๓ วิธีการใด ๆ ที่สามารถเข้าถึงข้อมูลของผู้ใช้และระบบต้องได้รับการอนุญาตจากผู้อำนวยการวิทยาลัยเทคนิคปัว

๒.๖.๔ การเข้าสู่ระบบจากระยะไกลของผู้ใช้งานภายนอกหน่วยงาน ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๒.๖.๕ การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตนจากระบบของหน่วยงาน

**นโยบายการเข้าถึงหรือควบคุมการใช้งานโปรแกรมประยุกต์การใช้งานโปรแกรมอรรถประโยชน์**

**๑. วัตถุประสงค์**

๑.๑ เพื่อควบคุมการเข้าถึงโปรแกรมประยุกต์โดยคำนึงถึงภารกิจและความรับผิดชอบของผู้ใช้งาน

๑.๒ เพื่อกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงและกำหนดสิทธิ์เป็นลำดับชั้นที่สอดคล้องกับภารกิจและความรับผิดชอบของผู้ใช้งานในแต่ละตำแหน่ง

๑.๓ เพื่อให้ผู้ใช้งานรับทราบและปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัด รวมถึงตระหนักถึงความสำคัญของข้อมูลประเภทต่างๆ ที่อยู่ในโปรแกรมประยุกต์

**๒. แนวปฏิบัติ**

๒.๑ โปรแกรมประยุกต์ใดๆ ภายในวิทยาลัยเทคนิคปัว ต้องมีผู้รับผิดชอบ เจ้าของ หรือผู้ดูแลระบบที่ทำหน้าที่รักษาความปลอดภัยและกำหนดสิทธิ์การเข้าถึงให้แก่ผู้ใช้งานตามภารกิจและความรับผิดชอบที่ได้รับมอบหมาย

๒.๒ ผู้ใช้งานที่ได้รับสิทธิ์เท่านั้นจึงจะสามารถเข้าถึงโปรแกรมประยุกต์ได้ โดยต้องมีกระบวนการตรวจสอบยืนยันตัวตน (Authentication) ที่ปลอดภัย น่าเชื่อถือ และเหมาะสม เช่น การใช้ชื่อผู้ใช้และรหัสผ่าน

๒.๓ ผู้ใช้งานต้องได้รับมอบสิทธิ์ในขอบเขตที่ตรงกับภาระหน้าที่และต้องไม่ได้รับสิทธิ์เกินกว่าความรับผิดชอบ (Authorization)

๒.๔ โปรแกรมประยุกต์ที่มีความสำคัญหรือเกี่ยวข้องกับข้อมูลลับ (เช่น ข้อมูลการเงิน บุคลากร การบริหาร และนักศึกษา) จะต้องมีการจำกัดเวลาการเชื่อมต่อ และบังคับให้ออกจากระบบเมื่อไม่มีการใช้งานระยะหนึ่ง

๒.๕ โปรแกรมประยุกต์ที่ใช้ผ่านเครือข่ายภายในหรือระบบอินทราเน็ตเท่านั้น จะต้องมีกระบวนการตรวจสอบยืนยันตัวตน (Authentication) และการเข้ารหัสข้อมูลอีกชั้น (SSL VPN) สำหรับผู้ที่เข้าใช้งานจากภายนอก

๒.๖ โปรแกรมประยุกต์ที่มีความสำคัญหรือเกี่ยวข้องกับข้อมูลลับต้องมีเอกสารควบคุมการเข้าถึงและกำหนดสิทธิ์ที่ระบุหน่วยงานและผู้รับผิดชอบอย่างชัดเจน

๒.๗ เมื่อมีการเพิ่ม ปรับเปลี่ยน หรือออกจากงานของผู้ปฏิบัติงานที่เกี่ยวข้องกับโปรแกรมประยุกต์ จะต้องมีการเพิ่ม ปรับเปลี่ยน หรือถอดถอนสิทธิ์ของผู้ใช้งานนั้นๆ

๒.๘ โปรแกรมประยุกต์ที่แสดงหรือเชื่อมโยงกับฐานข้อมูลที่เป็นความลับ (เช่น ข้อมูลการเงิน บุคลากร และนักศึกษา) หน่วยงานที่รับผิดชอบต้องมีผู้ดูแลและกำหนดหลักเกณฑ์สำหรับการเข้าถึงข้อมูลสำหรับหน่วยงานอื่นหรือผู้ใช้งานจากภายนอก

๒.๙ นโยบายและเอกสารควบคุมการเข้าถึงในแต่ละโปรแกรมประยุกต์จะต้องแสดงให้ผู้ใช้งานรับทราบ

๒.๑๐ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ให้จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้:

- จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์
- กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป
- จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ
- มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้
- กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

## นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบปฏิบัติการ

**๑. วัตถุประสงค์**

๑.๑ เพื่อควบคุมการเข้าถึงระบบปฏิบัติการหรือคอมพิวเตอร์ตามภารกิจและความรับผิดชอบของผู้ใช้งาน

๑.๒ เพื่อกำหนดกฎเกณฑ์และแนวทางการใช้งานระบบปฏิบัติการหรือคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย

๑.๓ เพื่อให้ผู้ใช้งานรับทราบและปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัดและตระหนักถึงความรับผิดชอบของตนเอง

**๒. แนวปฏิบัติ**

๒.๑ คอมพิวเตอร์ที่เป็นของวิทยาลัยเทคนิคปัว ต้องมีผู้รับผิดชอบในการใช้งานและการเข้าถึงระบบปฏิบัติการให้เหมาะสมกับภารกิจ

๒.๒ ระบบปฏิบัติการที่เข้าถึงหรือใช้งานข้อมูลลับ หรือติดตั้งโปรแกรมที่เชื่อมต่อกับข้อมูลลับ ต้องมีกระบวนการตรวจสอบยืนยันตัวตน (Authentication) ที่ปลอดภัย น่าเชื่อถือ และเหมาะสม เช่น การใช้ชื่อผู้ใช้และรหัสผ่าน

๒.๓ ระบบปฏิบัติการที่เข้าถึงหรือใช้งานข้อมูลลับต้องมีการจำกัดเวลาการเชื่อมต่อและบังคับให้ออกจากระบบเมื่อไม่มีการใช้งาน

๒.๔ ผู้ใช้งานต้องรับผิดชอบคอมพิวเตอร์ในความดูแลของตนเอง และผู้ได้รับสิทธิ์เท่านั้นจึงจะสามารถเข้าถึงระบบปฏิบัติการได้ โดยควรมีกระบวนการตรวจสอบยืนยันตัวตน (Authentication) ที่ปลอดภัย น่าเชื่อถือและเหมาะสม

๒.๕ เมื่อมีการเพิ่ม, ปรับเปลี่ยน, หรือออกจากงานของผู้ใช้งาน จะต้องมีการทบทวนผู้รับผิดชอบและเพิ่ม, ปรับเปลี่ยน หรือถอดถอนสิทธิ์ของผู้ใช้งานนั้นๆ

๒.๖ ห้ามติดตั้งหรือใช้งานโปรแกรมประยุกต์หรือโปรแกรมอรรถประโยชน์ที่ไม่เกี่ยวข้องกับภารกิจหน้าที่ความรับผิดชอบ

๒.๗ ห้ามติดตั้งหรือใช้งานโปรแกรมประยุกต์หรือโปรแกรมอรรถประโยชน์ที่ละเมิดลิขสิทธิ์ หากพบถือเป็นความผิดส่วนบุคคล

๒.๘ ห้ามจัดเก็บข้อมูลที่ผิดกฎหมาย สิ่งที่ละเมิดลิขสิทธิ์ หรือข้อมูลที่ไม่เหมาะสมลงในคอมพิวเตอร์หรือระบบใดๆ ของวิทยาลัยเทคนิคปัว

๒.๙ ห้ามนำคอมพิวเตอร์ ข้อมูล หรือทรัพยากรของวิทยาลัยเทคนิคปัว ไปใช้เพื่อหาประโยชน์ส่วนตัวหรือทางการค้า

๒.๑๐ ห้ามเผยแพร่หรือเปิดเผยข้อมูลหรือข้อมูลลับของมหาวิทยาลัยต่อบุคคลภายนอก เว้นแต่จะมีการเผยแพร่เป็นการทั่วไป

๒.๑๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบปฏิบัติการต้องแสดงให้ผู้ใช้งานรับทราบ

๒.๑๒ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

๒.๑๒.๑ ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

๒.๑๒.๒ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้:

- ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์
- ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง
- จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน
- จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๒.๑๒.๓ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification ad Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้:

- ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

- หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านการศึกษาและงานที่ต้องทำ

- สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม

๒.๑๒.๔ การบริหารจัดการรหัสผ่าน (Password Management System) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยมีแนวปฏิบัติ ดังนี้:

- มีระบบบริหารจัดการรหัสผ่าน ผ่านระบบเครือข่ายสารสนเทศของวิทยาลัยฯ
- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านของตนเองในครั้งแรกที่มีการเข้าสู่ระบบ
- มีระบบแจ้งระดับความความปลอดภัยของรหัสผ่าน

## นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพ

**๑.วัตถุประสงค์**

เพื่อกำหนดมาตรฐานในการควบคุมและป้องกันการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาจากความสำคัญของอุปกรณ์ ระบบ และข้อมูล

**๒. แนวทางปฏิบัติ**

๒.๑ ศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการและพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจนและจัดทำแผนผังแสดงตำแหน่งและประกาศให้ทราบทั่วกัน

๒.๒ ศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ

๒.๓ ศูนย์ข้อมูลเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศ

๒.๔ หน่วยงานภายนอกที่นำอุปกรณ์เข้ามาเชื่อมต่อเพื่อใช้งานต้องลงบันทึกในแบบฟอร์มขออนุญาตและมีเจ้าหน้าที่ที่รับผิดชอบลงนามรับรอง

๒.๕ ศูนย์ข้อมูลเทคโนโลยีสารสนเทศกำหนดการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

- มีบัญชีควบคุมอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต
- อุปกรณ์ที่ไม่มีการใช้งานจะต้องนำมาเก็บไว้ในสถานที่ที่ปลอดภัย เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต
- สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน
- ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน
- ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้
- ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๒.๖ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

๒.๖.๑ มีมาตรการป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ได้แก่:

- พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในให้ติดตั้งสัญญาณเตือนภัย เพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น
- มีระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบว่ายังใช้งานได้ตามปกติ
- ให้มีการบันทึกวันและเวลาเข้า-ออก พื้นที่หรือบริเวณที่มีความสำคัญของผู้ที่มาเยือน
- ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับอนุญาต
- จัดเก็บบันทึกการเข้า-ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น
- ผู้มาเยือนต้องติดบัตรให้เห็นชัดตลอดระยะเวลาที่อยู่บริเวณพื้นที่ใช้งานระบบ

๒.๖.๒ การลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบ พัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของของวิทยาลัย จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ในห้องที่มีความสำคัญให้น้อยที่สุด การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้:

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ กฎหมาย ระเบียบ ข้อบังคับหรือข้อกำหนดอื่น ๆ วัฒนธรรมองค์กร
- มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน
- มีการกำหนดขอบเขตของการป้องกัน ดังนี้:

ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์ ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๒.๖.๓ กำหนดมาตรการทำลายสื่อบันทึกข้อมูล/ข้อมูลอิเล็กทรอนิกส์ ดังนี้:

ต้องทำลายข้อมูลสำคัญภายในอุปกรณ์บันทึกข้อมูลหรือสื่อที่ใช้สำหรับบันทึกข้อมูลก่อนที่จะกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

- สื่อบันทึกข้อมูลที่เป็นประเภทจานแม่เหล็กให้ทำการ Format อุปกรณ์ดังกล่าวโดยไม่สามารถเรียกคืนกลับมาได้ตามมาตรฐาน DOD ๕๒๒๐.๐๐ M หรือวิธีบดขยี้ตามมาตรฐาน ISO/IEC ๒๗๐๐๒: ๒๐๐๕
- สื่อบันทึกข้อมูลประเภท Optical Disk ทำลาย โดยวิธีบดขยี้ การหัก หรือเจาะรูโดยไม่สามารถเรียกข้อมูลกลับมาได้ตามมาตรฐาน ISO/IEC ๒๗๐๐๒ : ๒๐๐๕
- สื่อบันทึกข้อมูลขนาดเล็กแบบพกพา (flash drive) ให้ทำการ Format อุปกรณ์ดังกล่าวโดยไม่สามารถเรียกคืนกลับมาได้ตามมาตรฐาน DOD ๕๒๒๐.๐๐ M มีกระบวนการในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ตามมาตรฐาน NSA

๒.๗ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๒.๘ การควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

การใช้บริการเครือข่าย

กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น กำหนดบริการที่อนุญาตให้มีการใช้งานได้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น การใช้งานระบบสารสนเทศที่สำคัญ ไม่ว่าจะเป็นระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง การใช้งานระบบเครือข่ายไร้สายจะต้องมีการลงทะเบียนตาม ใช้งานชื่อผู้ใช้ รหัสผ่านและสิทธิ์ตามแนวปฏิบัติการเข้าถึงของผู้ใช้งาน

๒.๙ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง ต้องตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงจะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนสำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน อย่างน้อย ๑ วิธี

๒.๑๐ มีบัญชีอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ที่ใช้งาน และมีการยืนยันการเข้าถึงอุปกรณ์ดังกล่าว ดังนี้

การระบุอุปกรณ์และการจัดเก็บข้อมูล:

- ใช้หมายเลข IP Address ในการระบุอุปกรณ์ โดยกำหนดเป็นช่วงของหมายเลข IP แยกตามประเภทของอุปกรณ์
- จัดเก็บข้อมูล อุปกรณ์บนเครือข่ายโดยระบุชนิดของอุปกรณ์การใช้งาน และเก็บบันทึกในรูปแบบสื่ออิเล็กทรอนิกส์ และเอกสารแล้วนำไปเก็บไว้ในตู้นิรภัย

มีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ ดังนี้:

- กำหนดบัญชีผู้ใช้และสิทธิการเข้าถึงอุปกรณ์บนอุปกรณ์เครือข่าย
- ให้ใช้โปรแกรมประเภท terminal ในการเข้าถึงอุปกรณ์
- ตั้งค่าความเร็วของการเข้าถึงตามคุณลักษณะของอุปกรณ์นั้น (สามารถดูได้จากคู่มือของอุปกรณ์)
- เมื่อเข้าสู่อุปกรณ์แล้วระบบจะให้กรอกชื่อผู้ใช้และรหัสผ่าน
- เมื่อกรอกชื่อผู้ใช้และรหัสผ่านที่ถูกต้องระบบจะยอมให้ใช้งานอุปกรณ์ตามสิทธิ์ที่ได้กำหนดไว้
- เมื่อกรอกชื่อผู้ใช้และรหัสผ่านที่ไม่ถูกต้องระบบจะไม่ยอมให้เข้าใช้งานอุปกรณ์
- ระบบจะให้กรอกชื่อผู้ใช้และรหัสผ่านไม่เกิน ๓ ครั้ง มิฉะนั้นระบบจะล็อคการเข้าใช้งานอุปกรณ์เป็นเวลา ๓๐ นาที
- ควบคุมการใช้งานอย่างเหมาะสม
- จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๒.๑๑ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย การปรับเปลี่ยนหรือควบการเข้าถึงพอร์ตต้องการทำหนังสือขออนุญาตจากผู้อำนวยการวิทยาลัยเทคนิคปัวเป็นลายลักษณ์อักษร บันทึกและควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต

ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๒.๑๒ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก และมีการแบ่งแยกเครือข่ายตามแต่ละหน่วยงานและการใช้งาน (VLAN)

๒.๑๓ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

- มีการตรวจสอบการเชื่อมต่อเครือข่าย
- จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย
- ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย
- มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์
- ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๒.๑๔ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

- ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)
- กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย
- กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการใช้บริการเครือข่าย

๒.๑๕ การควบคุมการเข้าใช้งานระบบจากภายนอก

การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของหน่วยงานต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการวิทยาลัยเทคนิคปัวหรือบุคคลที่ได้รับมอบหมายจากวิทยาลัยเทคนิคปัวก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของกรมในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวให้ตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๒.๑๖ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out) การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที เป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๒.๑๗ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง มีการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยมีการกำหนดให้ใช้งานได้ไม่เกิน ๒ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลา

การทำงานของหน่วยงานตามปกติเท่านั้น การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย กำหนดให้ระบบสารสนเทศมีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

**การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)** โดยต้องมีการควบคุม อย่างน้อยดังนี้

๑. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

- ผู้ใช้งานสามารถใช้โปรแกรมประยุกต์หรือแอพพลิเคชั่นตามที่หน่วยงานรับผิดชอบเท่านั้น
- ผู้ใช้งานสามรถใช้งานโปรแกรมประยุกต์หรือแอพพลิเคชั่นตามสิทธิที่ได้รับเท่านั้น

๒. ระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

- ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน
- มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ
- มีการควบคุมอุปกรณ์คอมพิวเตอร์ ระบบสื่อสารและการปฏิบัติงานจากภายนอกหน่วยงานที่เกี่ยวข้องกับระบบดังกล่าว

๓. การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

ลงทะเบียนอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ มีแนวทางปฏิบัติในการใช้งานโดยแบ่งออกเป็น ๒ กลุ่ม ดังนี้:

๓.๑ อุปกรณ์คอมพิวเตอร์

เครื่องคอมพิวเตอร์ที่วิทยาลัยเทคนิคปัวอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของวิทยาลัยเทคนิคปัว ดังนั้นผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของวิทยาลัยเทคนิคปัว โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของวิทยาลัยเทคนิคปัว ต้องเป็นโปรแกรมที่วิทยาลัยเทคนิคปัวได้ซื้อลิขสิทธิ์มาอย่างถูกกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของวิทยาลัยเทคนิคปัว

๓.๒ อุปกรณ์สื่อสารเคลื่อนที่

การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยงานศูนย์ข้อมูลสารสนเทศวิทยาลัยเทคนิคปัว หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับวิทยาลัยเทคนิคปัวเท่านั้น

๔. การใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

ผู้ใช้ มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง ทำการล็อกหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์ การนำเครื่องคอมพิวเตอร์มาใช้กับระบบเครือข่ายของวิทยาลัยเทคนิคปัว ต้องยืนยันตัวตนผ่านระบบก่อนเข้าใช้งานทุกครั้ง อุปกรณ์สื่อสารเคลื่อนที่: เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ จะต้องยืนยันตัวตนก่อนเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต อนุญาตให้เข้าใช้งานระบบได้ไม่เกิน ๒ ชั่วโมง หลังจากนั้นระบบจะบังคับให้ต้องมีการยืนยันตัวตนใหม่ ไม่อนุญาตให้เข้าใช้งานเว็บไซต์ที่ไม่เหมะสม หากผู้ดูแลระบบตรวจพบ

จะระงับสิทธิ์การเข้าถึงระบบ ไม่อนุญาตให้ผู้ใช้งานผ่านอุปกรณ์สื่อสารกระทำผิด พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายเทคโนโลยีสารสนเทศ

**การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)**

๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการวิทยาลัยเทคนิคปัวหรือผู้ดูแลระบบเครือข่ายสารสนเทศวิทยาลัยเทคนิคปัวได้รับมอบหมาย

๒. ผู้ดูแลระบบเครือข่ายวิทยาลัยเทคนิคปัว ต้องดำเนินการดังต่อไปนี้:

- กำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Access point) ให้เหมาะสม เพื่อป้องกันการเข้าใช้งานจากบุคคลที่ไม่ได้รับอนุญาตเข้าใช้ระบบ
- ทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน
- ต้องทำการเปลี่ยนค่าชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบ ให้เลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
- ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย
- ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
- เลือกใช้วิธีการควบคุมชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มีชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๓. มีการติดตั้งอุปกรณ์ป้องกันระบบบุกรุก (Firewall) ระหว่างเครือข่ายช่วยใช้กับภายใน หน่วยงาน

๔. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๔.๑ ผู้ดูแลระบบเครือข่ายวิทยาลัยเทคนิคปัว

- กำหนดท่าและตำแหน่งของพื้นที่ใช้งาน พื้นที่ควบคุมให้ชัดเจนและประกาศให้ทราบทั่วกัน
- กำหนดพื้นที่ควบคุม ได้แก่ พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ที่ใช้เครือข่ายไร้สาย (Wireless LAN Coverage Area)
- กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งาน แบ่งสิทธิในการใช้งาน ดังนี้ ผู้ดูแลระบบเครือข่าย ผู้ใช้งานทั่วไป และผู้ที่มาเยี่ยมผู้ติดต่อเครือข่ายหรือบุคคลภายนอก
- ตรวจสอบระบบรักษาความมั่นคงปลอดภัยทางกายภาพ ให้สามารถควบคุมดูแลและป้องกันได้ครอบคลุมระบบงาน รวมทั้งตรวจสอบความเสียหายที่อาจจะเกิดขึ้นในสถานการณ์ปัจจุบันนั้น ๆ อย่างน้อยปีละ

๒ ครั้ง และนำเสนอรายงานผู้อำนวยการวิทยาลัยเทคนิคปัว วิทยาลัยฯ ควรมีการเข้าออกอาคารสถานที่ โดยเฉพาะมีการจัดการและจัดทำเอกสารระบุสิทธิของบุคลากรและบุคคลภายนอกในการเข้าถึงอาคารสถานที่ที่แบ่งแยกได้ ดังนี้

- กำหนดสิทธิผู้ใช้ที่มีสิทธิผ่านเข้าออกและลงเวลาที่มีสิทธิในการผ่านเข้าออก ในแต่ละ "พื้นที่ใช้งาน" อย่างชัดเจน มีการอ้างอิงของวิทยาลัยเทคนิคปัวของบุคคลภายนอกหรือผู้มาติดต่อเข้าที่พักรักษาความปลอดภัย จะต้องให้มีการแลกบัตรประชาชนหรือบัตรบุคคลนั้นๆ ไม่ว่าจะเป็นบัตรประชาชน บัตรที่หน่วยงานให้มาหรือแม้แต่ใบขับขี่หรือหนังสือเดินทาง แล้วทำการบันทึกข้อมูลบัตรไว้ในฐานข้อมูลบุคคลนั้นๆ และบันทึกฟอร์มการเข้าออกเป็นลายลักษณ์อักษร บุคคลที่มาติดต่อต้องติดบัตรผู้มาเยือน (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในสถานที่นั้นๆ บุคคลที่มาบุคคลภายนอกจะต้องติดต่อเพื่อขออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้อง และจะต้องอยู่กับบุคคลที่ติดต่อตลอดเวลา บุคคลภายนอกหรือผู้ติดต่อต้องติดแบบฟอร์มการเข้าออกและบัตรผู้ติดต่อ (Visitor) พร้อมกับเจ้าหน้าที่รักษาความปลอดภัยเรียกออกจากเอกสารและเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบผู้ติดต่อและสิ้นสุดการพร้อมเวลาออก นอกจากนั้นให้ผู้ใช้รับสิทธิเข้าออก สถานที่ที่ได้เฉพาะในบริเวณที่ทำงานเท่านั้น หากมีบุคคลอื่นที่ไม่ใช่ผู้ใช้เข้าในพื้นที่ใดที่ได้รับการตรวจสอบดูแลและควบคุมแล้วนั้นจะต้องมีการแจ้งเจ้าหน้าที่รักษาความปลอดภัยตรวจสอบและดำเนินการทำความเข้าใจกับบุคคลที่อาจจะต้อง

## นโยบายในการรักษาความมั่นคงปลอดภัยของผู้ใช้งาน

**๑.วัตถุประสงค์**

เพื่อเป็นแนวทางให้ผู้ใช้งานรับทราบแนวปฏิบัติและกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบกำหนดไว้ เพื่อให้การใช้งานเทคโนโลยีสารสนเทศปลอดภัยและมีประสิทธิภาพ

**๒. การบริหารจัดการบัญชีผู้ใช้งาน**

๒.๑ นักศึกษา: ได้รับบัญชีผู้ใช้งานคอมพิวเตอร์ โดยชื่อผู้ใช้งานเป็นรหัสนักศึกษาและรหัสผ่านเป็นเลขประจำตัวประชาชน บัญชีจะถูกปิดการใช้งานเมื่อสำเร็จการศึกษา ลาออก พ้นสภาพ หรือเสียชีวิต

๒.๒ นักศึกษาแลกเปลี่ยน: ได้รับบัญชีผู้ใช้งานคอมพิวเตอร์ชั่วคราวที่มีกำหนดอายุการใช้งานหลังจากคณะต้นสังกัดมีหนังสือขออนุญาต

๒.๓ ศิษย์เก่า: บัญชีผู้ใช้งานจะถูกปิดการใช้งานเมื่อสำเร็จการศึกษา

๒.๔ บุคลากรใหม่: สามารถลงทะเบียนรับบัญชีได้หลังจากต้นสังกัดทำหนังสือรายงานตัว บัญชีจะถูกปิดเมื่อลาออก ไล่ออก เกษียณ หรือเสียชีวิต

๒.๕ บุคลากรเดิมเปลี่ยนตำแหน่ง: บัญชีจะถูกระงับการใช้งานและจะสามารถใช้งานได้หลังจากต้นสังกัดทำหนังสือรายงานตัว บัญชีจะถูกปิดเมื่อลาออก ไล่ออก เกษียณ หรือเสียชีวิต

๒.๖ บุคลากรจ้างพิเศษ: สายวิชาการ/ผู้บริหาร (เช่น อาจารย์พิเศษ): ได้รับบัญชีแบบพิเศษที่เข้าใช้งานเครือข่ายอินเทอร์เน็ตและระบบสารสนเทศของวิทยาลัยเทคนิคปัวได้ โดยต้องมีหนังสือขออนุญาตจากต้นสังกัด บัญชีจะถูกปิดเมื่อสิ้นสุดสัญญาจ้าง สายสนับสนุน: ได้รับบัญชีแบบชั่วคราวที่มีอายุการใช้งานกำหนดไว้ โดยต้องมีหนังสือขออนุญาตจากต้นสังกัด สามารถใช้งานเครือข่ายอินเทอร์เน็ตได้

๒.๗ บุคลากรเกษียณอายุราชการ: บัญชีจะถูกปิดการใช้งาน ยกเว้นผู้บริหารที่ต่ออายุราชการ จะเปิดใช้งานต่อจนสิ้นสุดวาระ

๒.๘ ผู้ใช้งานชั่วคราว: ใช้สำหรับบุคคลภายนอกที่ได้รับสิทธิ์ใช้งานเครือข่ายอินเทอร์เน็ตของวิทยาลัยเทคนิคปัว เช่น ผู้ที่มาติดต่องานหรือเข้าร่วมอบรม บัญชีจะมีอายุการใช้งานกำหนดไว้และต้องมีหนังสือขออนุญาตจากต้นสังกัด

**๓. แนวปฏิบัติของผู้ใช้งาน**

๓.๑ บุคลากรใหม่สามารถลงทะเบียนรับบัญชีได้หลังจากต้นสังกัดส่งหนังสือรายงานตัว

๓.๒ เมื่อบุคลากรเปลี่ยนตำแหน่งหรือย้ายหน่วยงาน บัญชีจะถูกระงับและจะใช้งานได้หลังจากต้นสังกัดทำหนังสือรายงานตัว

๓.๓ ควรตั้งรหัสผ่านที่มีความยาวอย่างน้อย ๘ ตัวอักษรขึ้นไป ประกอบด้วยตัวเลข ตัวอักษร และอักขระพิเศษ

๓.๔ ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน หรือเมื่อมีการแจ้งเตือน

๓.๕ ต้องเก็บชื่อผู้ใช้งานและรหัสผ่านเป็นความลับ

๓.๖ ต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้งผ่านซอฟต์แวร์ควบคุม

๓.๗ ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตน

๓.๘ ควรตั้งค่าโปรแกรมถนอมหน้าจอให้ล็อคหน้าจอเมื่อไม่มีการใช้งาน และต้องใส่รหัสผ่านเพื่อใช้งานต่อ

๓.๙ ควร Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓.๑๐ ต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูลก่อนทำลายหรือจำหน่ายอุปกรณ์

๓.๑๑ มีหน้าที่รับผิดชอบต่อสินทรัพย์ที่ส่วนงานมอบให้

๓.๑๒ เครื่องคอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัส ยกเว้นเครื่องเพื่อการศึกษาที่ได้รับอนุญาต

๓.๑๓ ข้อมูล, ไฟล์, ซอฟต์แวร์ที่ได้รับจากผู้อื่นต้องได้รับการตรวจสอบไวรัสและโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งาน

๓.๑๔ ในการใช้อีเมลของวิทยาลัยเทคนิคปัว ควรใช้เพื่อการติดต่องานเท่านั้น ไม่ควรระบุความสำคัญในหัวข้ออีเมล และควรลงชื่อออกจากระบบทุกครั้งเมื่อใช้งานเสร็จ

๓.๑๕ ต้องทำการอับเดต patch สำหรับระบบปฏิบัติการให้ใหม่เสมอ

๓.๑๖ เมื่อพบว่าเครื่องติดไวรัสต้องไม่เชื่อมต่อเข้าเครือข่ายและต้องแจ้งผู้ดูแลระบบ

**การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)**

การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) มีการกำหนดรายละเอียดที่เกี่ยวข้องกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดได้อย่างเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึงด้วย ต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน การมอบหมายสิทธิต้องสอดคล้องกับนโยบายควบคุมการเข้าถึงระบบสารสนเทศ ต้องทำการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

**การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)**

มีการจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

- กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรภาษาอังกฤษที่เป็นตัวพิมพ์ใหญ่และเล็ก ตัวเลข และสัญลักษณ์
- ไม่ควรกำหนดรหัสผ่านในส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิด หรือวัน เดือน ปีเกิด หรือเบอร์โทรศัพท์ หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- การตั้งรหัสผ่านชั่วคราวต้องยากต่อการคาดเดาและมีความแตกต่างกัน

- การส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งอีเมล หลังจากผู้ใช้งานได้รับรหัสผ่านแล้วให้ตอบกลับทันที
- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และต้องตั้งรหัสผ่านให้มีความปลอดภัยยากแก่การคาดเดา
- ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)
- ผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น
- ห้ามเผยแพร่ แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน
- ต้องมีการลงนามการรับรหัสผ่านเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน
- การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง รวมถึงมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

**การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)**

ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

**การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)**

- มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password User) เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ
- ต้องเปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก
- ตั้งรหัสผ่านที่ยากต่อการคาดเดา
- กำหนดรหัสผ่านให้มีตัวอักษรมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์
- ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน
- ไม่ตั้งรหัสผ่านเป็นวันเกิด ปีที่เกิด ซึ่งง่ายต่อการคาดเดา
- ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่าย
- ต้องเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์
- ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)
- ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก ๆ ๙๐ วัน หรือทุกครั้งที่ได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่านจากผู้ดูแลเครือข่ายสารสนเทศวิทยาลัยเทคนิคปัว
- หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน
- หลีกเลี่ยงการใช้รหัสผ่านเดิม

**การกำหนดชื่อผู้ใช้งาน (Username) และการลงทะเบียน:**

จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน การกำหนดชื่อผู้ใช้งาน (Username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรสามตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สี่ หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น ในกรณีที่เป็นนักศึกษา การกำหนดชื่อผู้ใช้งาน (Username) จะกำหนดเป็นรหัสนักศึกษา มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และความต้องการทางการศึกษา จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยสำนักหรือผู้ดูแลระบบที่ได้รับมอบหมาย มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น ผู้ดูแลระบบต้องเปลี่ยนรหัส ถี่กว่าผู้ใช้งานทั่วไป

**๔. ข้อห้ามสำหรับผู้ใช้งาน**

๔.๑ ห้ามใช้ทรัพย์สินของส่วนงานเพื่อการรบกวน ทำลาย หรือโจรกรรมข้อมูลที่ขัดต่อกฎหมายและศีลธรรม

๔.๒ ห้ามเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ที่ผู้อื่นทำขึ้นเป็นการเฉพาะเพื่อไปเปิดเผยโดยมิชอบ

๔.๓ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของส่วนงานหยุดชะงัก

๔.๔ ห้ามใช้ระบบสารสนเทศของวิทยาลัยเทคนิคปัวเพื่อควบคุมคอมพิวเตอร์หรือระบบภายนอกโดยไม่ได้รับอนุญาต

๔.๕ ห้ามลักลอบใช้งานหรือรับรู้รหัสผ่านส่วนบุคคลของผู้อื่น

๔.๖ ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของวิทยาลัยเทคนิคปัวโดยไม่ได้รับอนุญาต

๔.๗ ห้ามกระทำใดๆ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ

๔.๘ ห้ามส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์โดยปกปิดหรือปลอมแปลงที่มา

๔.๙ ห้ามกระทำใดๆ ที่อาจก่อให้เกิดความเสียหายต่อข้อมูลหรือระบบคอมพิวเตอร์ที่เกี่ยวกับความมั่นคงของชาติ ความปลอดภัยสาธารณะ หรือบริการสาธารณะ

๔.๑๐ ห้ามจำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นเพื่อใช้เป็นเครื่องมือในการกระทำความผิดตาม พ.ร.บ. คอมพิวเตอร์

๔.๑๑ ห้ามนำเข้าหรือเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของราชอาณาจักรหรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี

๔.๑๒ ห้ามนำเข้าหรือเผยแพร่ข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จที่อาจก่อให้เกิดความเสียหายแก่ผู้อื่น

๔.๑๓ ห้ามนำเข้าหรือเผยแพร่ข้อมูลอันเป็นเท็จที่อาจทำให้ประเทศเสียหายหรือประชาชนตื่นตระหนก

๔.๑๔ ห้ามนำเข้าหรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่เป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือการก่อการร้าย

๔.๑๕ ห้ามนำเข้าหรือเผยแพร่ข้อมูลที่มีลักษณะลามกและประชาชนทั่วไปเข้าถึงได้

๔.๑๖ ห้ามนำเข้าหรือเผยแพร่ภาพของผู้อื่นที่สร้างขึ้น ตัดต่อ หรือดัดแปลงด้วยวิธีทางอิเล็กทรอนิกส์ในลักษณะที่อาจทำให้ผู้นั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง

๔.๑๗ ห้ามคัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์ก่อนได้รับอนุญาต และห้ามใช้หรือลบแฟ้มข้อมูลของผู้อื่น

๔.๑๘ ห้ามติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หากพบเป็นความผิดส่วนบุคคล

๔.๑๙ ห้ามเข้าห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ที่เป็นเขตหวงห้าม เว้นแต่จะได้รับอนุญาต

๔.๒๐ ห้ามนำเครื่องมือหรืออุปกรณ์ใดๆ เชื่อมต่อเครือข่ายเพื่อประกอบธุรกิจส่วนบุคคล

บทลงโทษเมื่อกระทำผิด หากผู้ใช้งานฝ่าฝืนเงื่อนไข วิทยาลัยเทคนิคปัวขอสงวนสิทธิ์ในการระงับหรือยกเลิกการให้บริการทันที และผู้ใช้งานจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นแต่เพียงผู้เดียว

วิทยาลัยเทคนิคปัว จึงประกาศมาให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๙ กันยายน พ.ศ. ๒๕๖๘

(นายรชต ดิลกรัชตสกุล)
ผู้อำนวยการวิทยาลัยเทคนิคปัว