นโยบายและแนวปฏิบัติ
ในการรักษาความปลอดภัยด้านสารสนเทศ

วิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์

สำนักงานคณะกรรมการการอาชีวศึกษา

นโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ

วิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์

วัตถุประสงค์

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์เหมาะสมมีประสิทธิภาพมีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ วิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์จึงเห็นสมควรกำหนดนโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยกำหนดให้มีมาตรการแนวปฏิบัติ ขั้นตอนปฏิบัติ โดยมีวัตถุประสงค์ดังต่อไปนี้

1. จัดทำนโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์

2. กำหนดขอบเขตของการบริหารจัดการความปลอดภัยระบบเทคโนโลยีสารสนเทศ และมีการปรับปรุงอย่างต่อเนื่อง

3. ทำการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศให้ครู เจ้าหน้าที่ทุกระดับ ในวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์ รับทราบและถือปฏิบัติอย่างเคร่งครัด

4. เพื่อกำหนดมาตรการ แนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร ครู เจ้าหน้าที่ผู้ดูแลระบบ ตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์อย่างเคร่งครัด

5. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี

องค์ประกอบของนโยบาย

ส่วนที่ 1 การควบคุมการเขาออกห้องแม่ข่ายคอมพิวเตอร์

ส่วนที่ 2 การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ 4 การจัดทำระบบสำรองข้อมูล

ส่วนที่ 1

การควบคุมการเข้าออกห้องแม่ข่ายระบบคอมพิวเตอร์

กำหนดสิทธิ์ ให้กับเจ้าหน้าที่ให้มีสิทธิ์ในการเข้าพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย ซึ่งประกอบด้วย

1. จัดทำทะเบียนผู้มีสิทธิ์ เข้าออกพื้นที่เพื่อปฏิบัติหน้าที่ตามสิทธิ และหน้าที่ที่ได้รับมอบหมาย
2. กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออก โดยจัดทำเป็นเอกสาร บันทึกการเข้าออกพื้นที่
3. จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติ การเข้าออก พื้นที่ และ มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ ปีละ 1 ครั้ง เป็นอย่างน้อย
4. บุคคลภายนอกเข้ามาติดต่อจะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้า-ออกให้ถูกต้องและจะต้องอยู่ กับบุคคลที่มาติดตอตลอดเวลา
5. บุคคลอื่นที่ไม่มี หน้าที่เกี่ยวข้อง ขอเข้าพื้นที่ หน่วยงานเจ้าของ พื้นที่ต้องตรวจสอบเหตุ ผลและความจำเป็นก่อนที่จะอนุญาต

ส่วนที่ 2

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวน สิทธิ์ การเขาถึงอย่างสม่ำเสมอทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ ดูแลระบบตามความจำเป็นในการใช้งาน
2. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูล และระบบขอมูลได้

ส่วนที่ 3

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

การใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

1. ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

2. ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

3. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

4. ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

5. ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 123 , abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น 111 , aaa เป็นต้น

6. ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ ใช้ งานทั่วไป เช่น ทุก ๆ 3 เดือน สำหรับผู้ดูแล และ 6 เดือน สำหรับผู้ใช้งานระบบ

7. ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล๊อคอินเข้าสู่ระบบงาน

8. ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

9. ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ใช้งาน

ส่วนที่ 4

การจัดทำระบบสำรองข้อมูล

แนวปฏิบัติงานการสำรองข้อมูลและระบบคอมพิวเตอร์

1. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ

2. จัดทำบันทึกการสำรองข้อมูล ผู้ดูแลระบบคอมพิวเตอร์ ต้องทำบันทึก รายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้ สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

3. การรายงานข้อผิดพลาด ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

4. ผู้ดูแลระบบคอมพิวเตอร์ มอบ หมายหน้าที่การสำรองข้อมูล แก่เจ้าห น้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

การปฏิบัติเกี่ยวกับการสำรองข้อมูล

1. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการ ตามความถี่ดังนี้

ลำดับ	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
1	Web Servers	ค่า configure ก่อนและหลังการเปลี่ยนแปลง	ข้อมูลเผยแพร่บนเว็บไซต์และฐานข้อมูล 1 ครั้งต่อสัปดาห์
2	ระบบ RMS	ค่า configure ก่อนและหลังการเปลี่ยนแปลง	ข้อมูลและฐานข้อมูล 1 ครั้งต่อสัปดาห์
3	Server ระบบ RNET ทุกตัว	ค่า configure ก่อนและหลังการเปลี่ยนแปลง	ข้อมูลและฐานข้อมูล 1 ครั้งต่อสัปดาห์
4	Server อื่น ๆ	ค่า configure ก่อนและหลังการเปลี่ยนแปลง	ก่อนและหลังการเปลี่ยนแปลง1 ครั้งต่อเดือน

การกู้คืนระบบ

1. ในกรณีที่พบปัญหาที่ อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์ และ/หรือระบบเครือ ข่ายจนเป็นเหตุทำให้ ต้องดำ เนินการกู้ คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์ และ/หรือผู้ดูแลระบบเครือข่าย ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อม ทั้งบันทึกและให้ รายงานสรุปผล การปฏิบัติงาน

2. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้ หรือตามความเหมาะสมเพื่อกู้คืนระบบ

3. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้ บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้ งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้ คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์