ประกาศส่วนแผนงาน
มหาวิทยาลัยเทคโนโลยีสุรนารี
เรื่อง แนวปฏิบัติและข้อควรระวังในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่วนแผนงาน

.....

เพื่อให้บุคลากรส่วนแผนงานทุกคนได้พึงระวังและตระหนักถึงแนวปฏิบัติและข้อควรระวังในการรักษาความปลอดภัยด้านสารสนเทศ ส่วนแผนงาน มหาวิทยาลัยเทคโนโลยีสุรนารี ซึ่งจะทำให้เกิดความปลอดภัยของข้อมูล และให้การดำเนินการภายในส่วนแผนงานเป็นไปด้วยความเรียบร้อย มีประสิทธิภาพ จึงได้จัดทำเป็นแนวปฏิบัติและข้อควรระวังในเรื่องต่อไปนี้

๑. การควบคุมการเข้าถึง Server

๑.๑ บุคคลที่จะได้รับสิทธิ์การเข้าถึงข้อมูลระบบสารสนเทศใน Server ส่วนแผนงานได้ ต้องเป็นบุคลากรส่วนแผนงานเท่านั้น ผู้ดูแลระบบจะสร้างบัญชี (User-Password) โดยอนุญาตเฉพาะส่วนที่จำเป็นและคำนึงถึงประเภทข้อมูลและชั้นความลับเป็นหลัก

๑.๒ กำหนดให้การเข้าใช้ระบบ (Log in) มีการตรวจจับการเปิดระบบไว้ เมื่อไม่มีการใช้งานต้องทำการออกจากระบบ (Log out) อัตโนมัติตามระยะเวลาที่เหมาะสม

๑.๓ ห้ามเปิดเผยรหัสเข้าใช้งานและ Password ให้ผู้อื่นทราบและรวมถึงต้องเก็บรหัสของตัวเองให้มิดชิดในที่ปลอดภัย

๑.๔ บุคลากรส่วนแผนงานจะต้องร่วมกันกำหนดสิทธิ์การเข้าถึงข้อมูลใน Server ตามระดับชั้นความลับ ดังนี้

๑.๔.๑ ระดับหัวหน้าส่วน
๑.๔.๒ ระดับหัวหน้างาน
๑.๔.๓ ระดับบุคลากรส่วนแผนงาน

๒. การควบคุมทางกายภาพ

๒.๑ บุคลากรทุกคนต้องช่วยกันดูแลการเข้า-ออก โดยการปิดล็อคประตูทุกครั้งหลังเลิกงาน

๒.๒ หากมีบุคคลภายนอกขอใช้งานเครื่องคอมพิวเตอร์ บุคคลที่เป็นเจ้าของเครื่องจะต้องอยู่คอยควบคุมการใช้งานจนกระทั่งสิ้นภารกิจ

๒.๓ กำหนดบุคคลที่จะคอยควบคุมดูแลและตรวจสอบการใช้โปรแกรมที่จัดทำขึ้นโดยเฉพาะและการนำเข้า ข้อมูลเท็จ หรือลามก ส่งต่อสู่ระบบคอมพิวเตอร์

๒.๔ ให้ร่วมกันดูแล ตรวจสอบสายไฟฟ้า สายเครือข่ายอินเตอร์เน็ต อุปกรณ์คอมพิวเตอร์และ Hardware ให้อยู่ในสภาพร้อมใช้งาน อย่างน้อย เดือนละ ๑ ครั้ง เมื่อพบสิ่งผิดปกติให้รีบแจ้งศูนย์คอมพิวเตอร์อย่างเร่งด่วน

๒.๕ พึงระมัดระวัง ไม่ให้เกิดความเสี่ยงต่อการชำรุดเสียหายของเครื่องคอมพิวเตอร์ เช่น หลีกเลี่ยงการนำอาหารและเครื่องดื่มมารับประทานบริเวณคอมพิวเตอร์ เป็นต้น

๒.๖ กรณีมีการคืนเครื่องคอมพิวเตอร์ให้เจ้าของเครื่องลบข้อมูลออกทั้งหมด และมอบให้ผู้ดูแลระบบตัดสิทธิ์การเข้าถึง Server และตรวจเช็คการเข้าถึง ๖ เดือน/ครั้ง

๒.๗ ไม่ควรนำข้อมูลส่วนตัวเก็บไว้ใน Server

๓. การจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

๓.๑ ไม่เก็บไฟล์ข้อมูลที่มีความสำคัญไว้ที่ Server ที่เดียว เพื่อลดความเสี่ยงจากปัญหาข้อมูลสูญหายหรือระบบล้มเหลว

๓.๒ ให้มีการทบทวนสิทธิ์การเข้าถึงข้อมูลใน Server เป็นประจำ ปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

๓.๓ ตรวจสอบหรือทดสอบระบบ Server อย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๓.๔ เมื่อเกิดปัญหาในการใช้งานระบบ Server ให้รีบแจ้งผู้ดูแลระบบทราบทันที เพื่อบันทึกสถิติและเพื่อวิเคราะห์หาสาเหตุเพื่อไม่ให้เกิดขึ้นซ้ำ

๓.๕ เมื่ออุปกรณ์ UPS สำรองไฟเกิดการชำรุด ต้องรีบแจ้งศูนย์คอมพิวเตอร์โดยด่วน เพื่อป้องกันข้อมูลสูญหาย ในกรณีไฟดับ/ไฟตก/ไฟไม่สม่ำเสมอ

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยเคร่งครัด

ประกาศ ณ วันที่ ๒๓ กุมภาพันธ์ พ.ศ. ๒๕๖๔

(นายศราวุธ ป้อมสินทรัพย์)
หัวหน้าส่วนแผนงาน