แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับผู้ให้บริการภายนอก

ข้อกำหนดการควบคุมความมั่นคงปลอดภัยจากผู้ให้บริการภายนอก

- ผู้ให้บริการภายนอกต้องปฏิบัติตามกฎระเบียบ, นโยบาย, ขั้นตอนการปฏิบัติงาน และวิธีการปฏิบัติงานต่าง ๆ ของคณะ อย่างเคร่งครัด โดยกรณีที่มีข้อสงสัยให้สอบถามจากเจ้าหน้าที่ของหน่วยงานที่เป็นผู้ติดต่อประสานงาน
- ผู้ให้บริการภายนอกต้องมีการระบุจัดทำข้อตกลงหรือสัญญาการให้บริการ (Service Level Agreement) ให้ชัดเจนครบถ้วน
- กรณีมีการว่าจ้างช่วง (Sub contract) ในการทำงาน ผู้ให้บริการภายนอกจะต้องควบคุมดูแลให้ผู้รับจ้างช่วงปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ คำสั่งและวิธีปฏิบัติที่เกี่ยวข้องกับคณะ
- ผู้ให้บริการภายนอกต้องติดบัตรผู้มาติดต่อตลอดเวลาที่ปฏิบัติงานในพื้นที่
- ผู้ให้บริการภายนอกทุกคนต้องรักษาข้อมูลต่าง ๆ ที่ได้รับทราบระหว่างการปฏิบัติงานให้แก่คณะ ไว้เป็นความลับและอนุญาตให้ใช้ข้อมูลเพื่อการปฏิบัติงานให้กับทางคณะ เท่านั้น ห้ามมิให้ทำการเปิดเผยต่อบุคคลอื่นก่อนได้รับอนุญาตจากทางคณะอย่างเด็ดขาด
- กรณีที่ผู้ให้บริการภายนอกมีความจำเป็นต้องขอใช้งานข้อมูลภายในคณะ ให้ทำการแจ้งต่อเจ้าหน้าที่ที่เป็นผู้ติดต่อประสานงานเพื่อขออนุญาตใช้งานข้อมูลจากเจ้าของข้อมูลหรือผู้มีอำนาจ โดยผู้ให้บริการภายนอกได้รับอนุญาตให้ใช้งานข้อมูลเท่าที่จำเป็นต้องรับรู้หรือใช้เพื่อการปฏิบัติงานเท่านั้น
- คณะขอสงวนสิทธิ์ในการเข้าตรวจสอบทุกพื้นที่ที่มีการนำข้อมูลของคณะไปใช้งาน ส่งผ่าน หรือประมวลผล ซึ่งการตรวจสอบอาจทำโดยผู้ตรวจสอบจากภายนอกที่ได้รับการว่าจ้างจากคณะหรือผู้ตรวจสอบภายในคณะ ก็ได้
- ผู้ให้บริการภายนอกต้องแจ้งรายชื่อของเจ้าหน้าที่ที่จะเข้าปฏิบัติงานต่อคณะก่อนเริ่มปฏิบัติงาน และหากมีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงาน ต้องแจ้งให้ทางคณะทราบล่วงหน้าทุกครั้ง
- ห้ามผู้ให้บริการภายนอกนำสื่อบันทึกข้อมูลใด ๆ มาเชื่อมต่อกับอุปกรณ์สารสนเทศ ภายในพื้นที่สำนักงานของคณะด้วยตนเอง หากมีความจำเป็นต้องถ่ายโอนข้อมูล ให้ดำเนินการโดยเจ้าหน้าที่ของคณะเท่านั้น
- หากผู้ให้บริการภายนอกที่มีความจำเป็นต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ เข้าปฏิบัติงาน ต้องแจ้งความจำนงต่อเจ้าหน้าที่ที่เป็นผู้ติดต่อประสานงาน เพื่อดำเนินการขออนุมัติตามความเหมาะสม
- ผู้ให้บริการภายนอกต้องไม่นำเอกสารหรือซอฟต์แวร์ที่มีลิขสิทธิ์ของคณะ ไปใช้งานส่วนตัวหรือใช้งานในทางที่ผิด และห้ามมิให้นำเอกสารหรือซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ มาใช้งานในคณะ
- ในการปฏิบัติงาน ผู้ให้บริการภายนอกต้องการติดตั้งโปรแกรม, ปรับแต่งระบบเครือข่าย, เครื่อง Server หรือกระทำการใด ๆ ที่ก่อให้เกิดความเปลี่ยนแปลง (Change) ต่อระบบเทคโนโลยีสารสนเทศของคณะ ต้องแจ้งต่อเจ้าหน้าที่ผู้ติดต่อประสานงานเพื่อดำเนินการขออนุมัติก่อนดำเนินการทุกครั้ง

- ผู้ให้บริการภายนอกต้องไม่นำบุคคลอื่นที่ไม่เกี่ยวข้อง เข้ามาในพื้นที่คณะโดยไม่ได้รับอนุญาต
- ห้ามผู้ให้บริการภายนอกทำการถ่ายรูป หรือ บันทึกเสียง ภายในพื้นที่คณะ ก่อนได้รับอนุญาต
- ผู้ให้บริการภายนอกต้องรายงานจุดอ่อน ช่องโหว่ และเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบเห็นให้เจ้าของระบบหรือผู้ที่เกี่ยวข้องทราบ พร้อมทั้งดำเนินการแก้ไขข้อตรวจพบทันที
- ผู้ให้บริการภายนอกต้องปฏิบัติงานตามขอบเขตและหน้าที่ความรับผิดชอบที่ได้รับมอบหมายหรือที่ระบุไว้ในสัญญาเท่านั้น
- ผู้ให้บริการภายนอกต้องปฏิบัติงานด้วยความระมัดระวัง เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อคณะ
- การกระทำใด ๆ ของเจ้าหน้าที่ของผู้ให้บริการภายนอกที่ก่อให้เกิดความเสียหาย, ละเมิดข้อตกลงหรือสัญญาต่าง ๆ ที่ได้ทำไว้กับผู้ให้บริการภายนอกที่เป็นต้นสังกัดของเจ้าหน้าที่ผู้นั้น ต้องรับผิดชอบต่อความเสียหายทั้งหมด
- ในวันสุดท้ายของการปฏิบัติงานตามข้อตกลงหรือสัญญาผู้ให้บริการภายนอกต้องทำการส่งคืนทรัพย์สินต่าง ๆ เช่น กุญแจ, อุปกรณ์ต่าง ๆ และ รหัสเข้าระบบ ให้แก่เจ้าหน้าที่ผู้ติดต่อประสานงานอย่างครบถ้วน
- กรณีที่ผู้ให้บริการภายนอกมีการดำเนินการเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อการให้บริการ ตามข้อตกลงหรือสัญญา ผู้ให้บริการภายนอกต้องแจ้งต่อทางคณะอย่างเป็นลายลักษณ์อักษร ล่วงหน้าอย่างน้อย ๑ เดือน เพื่อให้คณะทำการพิจารณา วิเคราะห์ผลกระทบ และหาวิธีในการแก้ไขควบคุมความเสี่ยงได้อย่างเหมาะสม

การเข้าถึงเครือข่าย (Network Access Control)

- มาตรการควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)
  - ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัยเพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วทำการบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”
  - ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ ให้ถูกต้องชัดเจน
- การขออนุญาตใช้งานพื้นที่ Web Server ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ
- ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

- ต้องมีการควบคุมการเข้าถึงระบบเครือข่ายระยะไกล โดยใช้งานผ่านระบบที่กำหนดไว้เท่านั้น
- ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น
- ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน
- ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล
- แนวปฏิบัติอื่น ๆ นอกเหนือจากนี้ให้เป็นไปตามประกาศ ระเบียบ ข้อบังคับ หรือแนวปฏิบัติของมหาวิทยาลัยมหิดล ที่เกี่ยวข้องกับการใช้งานระบบเครือข่ายจากภายนอกสำนักงาน (ถ้ามี)