ข้อกำหนดการบริหารจัดการการป้องกันไวรัส และภัยคุกคามทางเครือข่าย
สำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์

---

1. เครื่องคอมพิวเตอร์ของบุคลากรต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) และโปรแกรมป้องกันภัยคุกคามทางเครือข่าย (Anti-Malware) ตามที่นโยบายของ สำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา และสนับสนุนการให้บริการของสำนักหอสมุด พัฒนา ระบบป้องกัน โดยจะต้องได้รับอนุญาตจากหัวหน้าฝ่าย
2. บุคลากรจะต้องทำการปรับปรุงอัปเดตข้อมูลสำหรับตรวจสอบโปรแกรมไวรัสและภัยคุกคามทางเครือข่าย (Virus and Malware Platform) ไวรัสคอมพิวเตอร์ (Virus signature) และปรับปรุงระบบปฏิบัติการ (Update patch) ให้เป็นปัจจุบันอยู่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้นได้
3. บุคลากรต้องพึงระวังไวรัสและภัยคุมคามทางเครือข่ายตลอดเวลา โดยไม่ทำการท่องเว็บเพจที่ผิดปกติ รวมทั้งเมื่อพบสิ่งผิดปกติหรือเป็นปัญหา ต้องแจ้งให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบ เพื่อทำการตรวจสอบ พิจารณาถึงปัญหาที่เกิดขึ้น และหาแนวทางแก้ไขปัญหาร่วมกัน
4. เมื่อบุคลากรพบว่าเครื่องคอมพิวเตอร์ติดไวรัส หรือเกิดภัยคุกคามจะต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์กับระบบเครือข่ายเด็ดขาด และแจ้งให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบ เพื่อดำเนินการแก้ไข
5. ในส่วนเอกสารข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากบุคคลอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และภัยคุกคามทางเครือข่ายก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง
6. ห้ามดำเนินการเผยแพร่ไวรัสคอมพิวเตอร์ ภัยคุกคาม (Malware) หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์และข้อมูลขององค์กร สิทธิ์ที่จะพัฒนาระบบหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการ ดังนี้

   6.1 พัฒนาและออกแบบระบบหรือมีการใช้ฮาร์ดแวร์ใด ๆ ที่จะเป็นการทำลายขั้นตอนการทำงานระบบรักษาความปลอดภัยขององค์กร รวมทั้ง การกระทำในลักษณะการแอบใช้รหัสผ่านบุคคลอื่น การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

   6.2 พัฒนาและออกแบบระบบใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์ เพื่อหาผลประโยชน์ให้แก่ตนเองในเชิงพาณิชย์

   6.3 พัฒนาและออกแบบระบบหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์โดยหาผลประโยชน์ให้แก่ตนเองในเชิงพาณิชย์

ข้อกำหนดการบริหารจัดการโปรแกรมป้องกันไวรัสคอมพิวเตอร์

สำหรับบุคลากรฝ่ายเทคโนโลยีสารสนเทศ

---

1. ผู้ดูแลระบบเข้าสู่ระบบป้องกันไวรัส Bitdefender Cloud ผ่านหน้าเว็บเพจโดยมีการเข้าใช้งานระบบด้วยการยืนยันตัวตน 2 ครั้ง ผ่าน Google Authenticator
2. ผู้ดูแลระบบดำเนินการกำหนดมาตรฐาน (Master Policy) การป้องกันภัยคุกคามต่าง ๆ ในเครื่องแม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย
3. ผู้ดูแลระบบเปิดฟังก์ชันการใช้งาน Scan ไวรัสคอมพิวเตอร์ และภัยคุมคามต่างๆ โดยมีการอัปเดตในทุกวัน
4. ผู้ดูแลระบบดำเนินการบริหารจัดการ และแชร์ไฟล์ข้อมูลการติดตั้งระบบแอนตี้ไวรัสให้แก่บุคลากรที่รับผิดชอบดูแลเครื่องแม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย
5. ผู้ดูแลระบบอาจมีการเปลี่ยนแปลงความถี่/ระยะเวลาในแต่ละข้อกำหนดตามความเหมาะสม โดยเป็นการบริหารจัดการผ่านหน้า Web Gravityzone Bitdefender Management ของระบบป้องกันไวรัสคอมพิวเตอร์
6. ระบบ Web Gravityzone Bitdefender Management จำเป็นต้องมีการรายงานผลภัยคุกคามต่าง ๆ (Security Audit Report) เป็นรายเดือน ให้แก่ผู้ดูแลระบบผ่านช่องทางจดหมายอิเล็กทรอนิกส์ (E-mail)
7. กรณีระบบ Web Gravityzone Bitdefender Management มีปัญหา และมีการอัปเดตระบบ ให้แจ้งแก่หัวหน้าฝ่ายรับทราบ
8. ผู้ดูแลระบบต้องตรวจสอบและแก้ไขความผิดพลาดของภัยคุกคามที่เกิดขึ้น ในกรณีมีรายงานแจ้งจากระบบหรือบุคลากรในสำนักหอสมุด
9. ผู้ดูแลระบบต้องตรวจสอบข้อมูลมาตรฐาน (Master Policy) ให้เป็นปัจจุบันอยู่เสมอ และลบข้อมูลการติดตั้งระบบป้องกันไวรัสออกในเครื่องที่ไม่มีการใช้งานนานเกิน 2 ปี