เอกสารแนบท้ายประกาศ

แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของมหาวิทยาลัยเกษตรศาสตร์ พ.ศ. ๒๕๕๗

จัดทำโดย
สำนักบริการคอมพิวเตอร์
มหาวิทยาลัยเกษตรศาสตร์

สารบัญ

หมวดที่ ๑

ความหมายและคำจำกัดความ

๑. **มหาวิทยาลัย** หมายความว่า มหาวิทยาลัยเกษตรศาสตร์

๒. **วิทยาเขต** หมายความว่า เขตการศึกษาซึ่งประกอบด้วยส่วนงานของมหาวิทยาลัยที่ตั้งอยู่ในเขตท้องที่ตามที่สภามหาวิทยาลัยกำหนด

๓. **หน่วยงาน** หมายความว่า คณะ/สำนัก/สถาบัน/ศูนย์ ที่เป็นส่วนราชการตามโครงสร้างของมหาวิทยาลัยเกษตรศาสตร์

๔. **หน่วยงานภายนอก** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของมหาวิทยาลัย โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

๕. **ห้องควบคุมระบบ** หมายถึง ห้องที่ติดตั้งและจัดวางระบบเซิร์ฟเวอร์ อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่ายของมหาวิทยาลัย ภายใต้การดูแลของสำนักบริการคอมพิวเตอร์ และ/หรือ หน่วยงานที่ให้บริการสารสนเทศ

๖. **ระบบอินเทอร์เน็ต** (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของมหาวิทยาลัยเข้ากับเครือข่ายอินเทอร์เน็ต

๗. **ระบบสารสนเทศ** หมายความว่า ระบบงานของมหาวิทยาลัยที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่มหาวิทยาลัยสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ ฯลฯ

๘. ระบบเครือข่ายคอมพิวเตอร์ (Computer Network System) หมายความว่า ระบบที่เชื่อมต่อคอมพิวเตอร์ เซิร์ฟเวอร์ อุปกรณ์เครือข่ายต่าง ๆ ของมหาวิทยาลัย

๙. **สินทรัพย์คอมพิวเตอร์** หมายความว่า ข้อมูล คอมพิวเตอร์ เซิร์ฟเวอร์ ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์เครือข่าย รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์

๑๐. **ผู้บริหารสำนักบริการคอมพิวเตอร์** หมายถึง ผู้อำนวยการ รองผู้อำนวยการ และผู้ช่วยผู้อำนวยการ

๑๑. **ผู้ดูแลระบบ**

"ผู้ดูแลระบบ" หมายความว่า ผู้ซึ่งได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่ดูแลเซิร์ฟเวอร์ ระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ให้บริการได้อย่างมีเสถียรภาพ ทั้งนี้ผู้ดูแลระบบมีสิทธิ์ในการดำเนินการดังต่อไปนี้

๑๑.๑. ผู้ดูแลระบบมีสิทธิ์ปรับตั้งระบบให้ทำงานได้อย่างมีประสิทธิภาพ และเสถียรภาพ

๑๑.๒. ผู้ดูแลระบบมีสิทธิ์ยุติการทำงานของกระบวนการที่สร้างภาระให้ระบบ หรืออาจทำให้เกิดปัญหากับการใช้งานต่อผู้ใช้ส่วนรวม

๑๑.๓. ผู้ดูและระบบมีสิทธิ์บีบอัดเพื่อลดขนาดแฟ้มข้อมูลของผู้ใช้ เพื่อบรรเทาปัญหาที่อาจเกิดจากเนื้อที่เก็บข้อมูลไม่พอเพียง

๑๑.๔. ผู้ดูแลระบบมีสิทธิ์กลั่นกรอง บริหารการใช้ช่องสัญญาณเครือข่าย จำกัดการเข้าถึงข้อมูล ทั้งข้อมูลที่อยู่ภายในเครือข่ายและภายนอกเครือข่าย เพื่อคงไว้ซึ่งประสิทธิภาพการใช้เครือข่ายและการใช้งานตามพันธกิจมหาวิทยาลัย

๑๒.ผู้ใช้งาน (user) หมายความว่า นิสิต บุคลากร ของมหาวิทยาลัยเกษตรศาสตร์ หรือบุคคลภายนอกที่มีบัญชีรายชื่อที่ออกโดยสำนักบริการคอมพิวเตอร์ และ/หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้สินทรัพย์คอมพิวเตอร์ของมหาวิทยาลัยเกษตรศาสตร์

๑๓.สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย

๑๔.จดหมายอิเล็กทรอนิกส์ (e-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับผ่านโพรโทคอล ต่างๆ เช่น SMTP, POP3, IMAP ฯลฯ

๑๕.สื่อบันทึกพกพา (portable media) หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD , DVD , flash drive, external hard disk ฯลฯ

๑๖.ชื่อผู้ใช้ (username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่กำหนดสิทธิ์การใช้งานไว้

๑๗.รหัสผ่าน (password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๑๘.การเข้ารหัสลับ (encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๑๙.การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย

๒๐.ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า การรักษาไว้ซึ่งความลับ (confidentiality) ความครบถ้วนถูกต้อง (integrity) และความพร้อมใช้ (availability) ของสารสนเทศ

๒๑.เหตุการณ์ด้านความปลอดภัย หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่งคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๒๒.สถานการณ์ด้านความปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของมหาวิทยาลัยถูกบุกรุกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๒๓.การพิสูจน์ยืนยันตัวตน (authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ และรหัสผ่าน

๒๔.SSID (service set identifier) หมายความว่า ชื่อระบุเครือข่ายไร้สาย

๒๕.MAC Address (media access control address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๒๖. VPN (virtual private network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๒๗. แผนผังระบบเครือข่าย (network diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของมหาวิทยาลัย

หมวดที่ ๒

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางการดำเนินงานการใช้ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของมหาวิทยาลัยเกษตรศาสตร์ สำหรับการควบคุมการเข้าถึงข้อมูล สำหรับลดปัญหาในเรื่องความเสี่ยงต่างๆ ในการใช้ระบบสารสนเทศ

๒. เพื่อให้บุคลากรในมหาวิทยาลัยเกษตรศาสตร์ ใช้เป็นแนวทางในการปฏิบัติงานให้เป็นไปอย่างมีประสิทธิภาพ

ผู้รับผิดชอบ

๑. สำนักบริการคอมพิวเตอร์
๒. หน่วยงานที่ให้บริการเครื่องคอมพิวเตอร์แม่ข่าย
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย
๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. ความมั่นคงทางกายภาพห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

ความมั่นคงทางกายภาพถือเป็นส่วนสำคัญอันหนึ่งของระบบรักษาความปลอดภัย ความมั่นคงทางกายภาพรวมถึงการป้องกันสถานที่และอุปกรณ์ ให้ปลอดภัยจากการปล้น การโจรกรรม อุบัติภัยทางธรรมชาติ เช่น แผ่นดินไหว น้ำท่วมเป็นต้น การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจร อุณหภูมิหรือความชื้น ในห้องควบคุมที่สูงเกินขีดจำกัด หรือการทำกระทำโดยประมาท เช่น การทำน้ำหกรดโดนเครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ ดังนั้นจึงมีความจำเป็นในการป้องกันอาคารและอุปกรณ์โดยกำหนดเป็นนโยบายเพื่อถือปฏิบัติ ในเรื่องการสร้างห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายรวมถึงมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๑.๑. จำแนกและกำหนดพื้นที่ห้องควบคุมระบบ เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้ โดยมีการจัดแบ่งพื้นที่ดังนี้

๑.๑.๑. ห้องควบคุมระบบแบ่งเป็นสองพื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

๑.๑.๒. พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึงเป็นห้องที่มีเซิร์ฟเวอร์ ระบบเครือข่ายคอมพิวเตอร์ติดตั้งอยู่

๑.๒. การเข้าไปในพื้นที่ควบคุม

๑.๒.๑. ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ ผู้บริหารหน่วยงานหรือบุคคลที่ผู้บริหารหน่วยงานนำเข้าเยี่ยมชม

๑.๒.๒. ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

๑.๒.๓. ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่ควบคุมเว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๒.๔. ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๒.๕. บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุมต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมายและต้องมีเจ้าหน้าที่อยู่ด้วยตลอดเวลา

๑.๓. การเข้าไปในพื้นที่จำกัดการเข้าถึง

๑.๓.๑. ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบหรือในกรณีที่บุคคลอื่นที่มีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย และต้องมีผู้ดูแลระบบที่ได้รับมอบหมายอย่างน้อย ๑ คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

๑.๓.๒. ไม่อนุญาตให้บุคคลที่มีอายุต่ำกว่า ๑๕ ปี เข้าไปในพื้นที่จำกัดการเข้าถึง

๑.๓.๓. ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง

๑.๓.๔. ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่จำกัดการเข้าถึงเว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๓.๕. ไม่อนุญาตให้เข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง

๑.๓.๖. ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อ ทรัพย์สินจะอนุญาตให้เข้าไปในพื้นที่จำกัดการเข้าถึงได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๔. ด้านกายภาพของห้องควบคุมระบบ

๑.๔.๑. แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้เช่น router, switch, server, UPS เป็นต้น

๑.๔.๒. มี rack ในการจัดเก็บอุปกรณ์ต่างๆที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา

๑.๔.๓. ตำแหน่งของการวางอุปกรณ์ต่างๆ ไม่ควรวางใกล้ประตู หน้าต่างเพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น

๑.๔.๔. การจัดวางสาย cable network สายไฟฟ้าควรมีการติดป้ายชื่อสายต้นทางปลายทาง และเก็บสายให้เรียบร้อยเพื่อป้องการการเดินสะดุด

๑.๔.๕. ติดประกาศบันทึกการบำรุงรักษา ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

๑.๔.๖. มีระบบรักษาความปลอดภัยในห้องเช่น กล้อง CCTV ระบบการเข้าออกห้องโดยระบบ fingerprint scan หรือ RFID เป็นต้น

๑.๔.๗. มีระบบสังเกตการณ์อุณหภูมิภายใน rack ระบบแจ้งเตือนและป้องกันอัคคีภัย

๑.๔.๘. มีระบบสำรองไฟฟ้าเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบสำรองไฟฟ้าอัตโนมัติ เป็นต้น

๑.๔.๙. มีระบบป้องกันกระแสไฟฟ้าจากฟ้าผ่า

๑.๔.๑๐. ระบบปรับอากาศแบบควบคุมอุณหภูมิ (๕๐-๘๐°F) และความชื้น (๒๐- ๘๐%)

๑.๔.๑๑. ติดตั้งฉนวนกันไฟไหม้ ที่ฝ้าเพดานและกำแพง

๑.๕. การบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

๑.๕.๑. กรณีติดตั้งเซิร์ฟเวอร์หรืออุปกรณ์ต่างๆ ให้แกะหีบห่อและประกอบให้แล้วเสร็จจากภายนอกพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงก่อนนำไปติดตั้งเว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๕.๒. กรณีที่จำเป็นต้องทำงานก่อสร้าง แก้ไข และติดตั้ง ในพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงต้องมีอุปกรณ์ควบคุม ฝุ่น ความร้อน เพื่อป้องกันความเสียหาย โดยผ่านความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมายก่อนการปฏิบัติงาน

๑.๕.๓. ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยทุก ๓ เดือน

๑.๕.๔. ร่างขั้นตอนแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟฟ้าลัดวงจร ไฟไหม้ แผ่นดินไหว น้ำท่วม หรือมีผู้บุกรุก เป็นต้น

๑.๕.๕. ซ้อมการปฏิบัติงานตามแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน ทุก ๖ เดือน

๑.๕.๖. มีตารางการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

๒. การควบคุมการเข้าถึง (Access control)

สำหรับการควบคุมการเข้าถึงระบบสารสนเทศ หมายถึง การเข้าถึงระบบของผู้ใช้ และรวมความถึงการกำหนดหน้าที่ของผู้ใช้ การเข้าถึงเครือข่าย การใช้งานระบบที่ให้บริการและระบบสารสนเทศ การเฝ้าดูการใช้งานระบบ คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถานที่ เป็นต้น

๒.๑. ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ ในการขออนุญาตเข้าระบบงานนั้นจะต้องทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบ และกำหนดให้ลงนามอนุมัติเอกสารดังกล่าวต้องจัดเก็บไว้เป็นหลักฐาน

๒.๒. เจ้าของข้อมูลและเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในหมวดที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๒.๓. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

๒.๔. ผู้ใช้งานต้องไม่ดาวน์โหลดหรือติดตั้งโปรแกรม หรือให้ผู้อื่นผู้ใดติดตั้งโปรแกรม ที่ไม่ถูกต้องตามลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของหน่วยงาน หากฝ่าฝืนมหาวิทยาลัย และสำนักบริการคอมพิวเตอร์จะถือเป็นความรับผิดชอบของผู้ใช้งานเครื่องคอมพิวเตอร์เครื่องนั้น

๒.๕. ผู้ใช้งาน ต้องไม่นำทรัพย์สินของทางราชการไปใช้ในทางเสื่อมเสีย ผิดกฎหมาย หรือทำให้ผู้อื่นได้รับความเดือดร้อน

๒.๖. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์ชนิดพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราเซอร์

๒.๗. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านระบบเครือข่ายคอมพิวเตอร์จะต้องตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๒.๘. ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์อย่างเคร่งครัด

๓. การควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ (network access control)

เพื่อควบคุมการใช้บริการบนระบบเครือข่ายคอมพิวเตอร์

๓.๑. ผู้ดูแลระบบต้องจัดทำนโยบายเพื่อควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่าย โดยเฉพาะเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

๓.๒. ผู้ดูแลระบบต้องจัดแบ่งเครือข่ายระหว่างการใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับมหาวิทยาลัยเกษตรศาสตร์ โดยพิจารณาจากบริการเครือข่าย ระบบสารสนเทศ กลุ่มของผู้ใช้งานของทั้งสองฝ่าย

๓.๓. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกมหาวิทยาลัยเกษตรศาสตร์ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตน ก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกมหาวิทยาลัยเกษตรศาสตร์สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยเกษตรศาสตร์ได้

๓.๔. การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต ผู้ดูแลระบบต้องจัดทำกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายของมหาวิทยาลัยเกษตรศาสตร์และเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น

๓.๕. ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย ผู้ดูแลระบบต้องจัดทำข้อกำหนดหรือข้อตกลงสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่างมหาวิทยาลัยเกษตรศาสตร์กับหน่วยงานภายนอก

๓.๖. การควบคุมผู้ใช้ในการใช้งานเครือข่าย ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๓.๗. การจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน ผู้ดูแลระบบต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน

๓.๘. การจำกัดเส้นทางบนเครือข่าย ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

๔. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๔.๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องลงทะเบียน MAC Address ผ่านระบบลงทะเบียนเครื่องคอมพิวเตอร์ โดยใช้รหัสบัญชีผู้ใช้ที่ออกโดยสำนักบริการคอมพิวเตอร์

๔.๒. ผู้ใช้งานต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๔.๓. ผู้ดูแลระบบต้องดำเนินการดังต่อไปนี้

๔.๓.๑. ต้องลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๔.๓.๒. ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๔.๓.๓. ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๔.๓.๔. เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

๔.๓.๕. เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๔.๓.๖. ต้องกำหนดค่าใช้ WPA (Wi-Fi protected access) หรือดีกว่าในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณ (access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

๔.๓.๗. เลือกใช้วิธีการควบคุม MAC Address ชื่อผู้ใช้และรหัสผ่านของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้และรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๔.๓.๘. ติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๔.๓.๙. ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการสำนักบริการคอมพิวเตอร์ทราบโดยทันที

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

เพื่อป้องกันการใช้งานเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต

๕.๑. การจำกัดระยะเวลาการใช้งาน ผู้ดูแลระบบต้องจำกัดระยะเวลา การใช้งานสำหรับระบบสารสนเทศ ที่มีความสำคัญสูงหรือมีความเสี่ยงสูง

๕.๒. การพิสูจน์ตัวตนสำหรับผู้ใช้ ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้เป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

๕.๓. การบริหารจัดการรหัสผ่าน ผู้ดูแลระบบต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

๕.๔. กระบวนการในการเข้าสู่ระบบให้บริการอย่างมั่นคงปลอดภัย ผู้ดูแลระบบต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการเพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการปฏิเสธการใช้งาน หากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง เป็นต้น

๕.๕. การพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบเครือข่ายคอมพิวเตอร์

๕.๖. การตัดเวลาการใช้งานเครื่องเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ เมื่อเครื่องเครื่องคอมพิวเตอร์ นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ เป็นต้น

๕.๗. การควบคุมการใช้งานโปรแกรมยูทิลิตี้ ผู้ดูแลระบบต้องกำหนดให้ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

๕.๗.๑. ก่อนใช้ต้องพิสูจน์ตัวตนก่อน

๕.๗.๒. ให้แยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน

๕.๗.๓. จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

๕.๗.๔. ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ใครเป็นผู้ใช้งาน

๕.๗.๕. การติดตั้งระบบเตือนภัยสำหรับระบบที่มีความสำคัญสูง ผู้อำนวยการสำนักบริการคอมพิวเตอร์ ต้องจัดให้ติดตั้งระบบเตือนภัยให้กับผู้ใช้ที่ปฏิบัติงานกับระบบที่มีความสำคัญสูง

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (application and information access control)

เพื่อป้องกันการใช้งานระบบสารสนเทศ โดยไม่ได้รับอนุญาต

๖.๑.๑. ต้องจัดให้มีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๖.๑.๒. ต้องแยกระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในมหาวิทยาลัยเกษตรศาสตร์ เป็นต้น

๖.๑.๓. ควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกมหาวิทยาลัยเกษตรศาสตร์

๖.๑.๔. ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศของมหาวิทยาลัยเกษตรศาสตร์

๖.๑.๕. ผู้ดูแลระบบสารสนเทศ ต้องตัดเวลาการใช้งานระบบสารสนเทศ เมื่อผู้ใช้งานระบบสารสนเทศไม่ได้มีการใช้งานเป็นระยะเวลา ๓๐ นาที

๗. ความมั่นคงปลอดภัยการใช้ระบบสารสนเทศและเครือข่าย

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๗.๑. ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้นเช่น Proxy, Firewall, IPS-IDS เป็นต้น และห้ามผู้ใช้เชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและขออนุญาตจากสำนักบริการคอมพิวเตอร์ เป็นลายลักษณ์อักษร

๗.๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราเซอร์

๗.๓. ผู้ใช้ต้องปรับปรุง Patch และ HotFix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลด Patch และ HotFix ต่างๆ จากเว็บไซต์เจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่ เป็นต้น

๗.๔. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๗.๕. ผู้ใช้ต้องไม่ใช้เครือข่ายของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมเป็นต้น

๗.๖. ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่าย และความปลอดภัยทางข้อมูลของมหาวิทยาลัย

๗.๗. ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย

๗.๘. ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยที่ยังไม่ได้ประกาศอย่างเป็นทางการ ผ่านอินเทอร์เน็ต

๗.๙. ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อแก้ไขหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

๗.๑๐.หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๘. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

๘.๑. การลงทะเบียนผู้ใช้งานใหม่ ผู้ดูแลระบบต้องร่วมกันจัดทำระเบียบปฏิบัติในการลงทะเบียนผู้ใช้งานใหม่เข้าเป็นสมาชิกของมหาวิทยาลัยเกษตรศาสตร์ เพื่อให้สามารถใช้งานระบบสารสนเทศ หรือโครงสร้างสนับสนุนระบบสารสนเทศอื่น ๆ ทั้งหมดได้ นอกจากนี้ต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้งานทันทีในกรณีที่มีการลาออกจากงาน

๘.๒. การบริหารจัดการรหัสผ่านของผู้ใช้งาน ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย

๘.๓. วิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่าน ส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ครอบครองอยู่ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น) ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้ต้องเป็นไปอย่างปลอดภัย

๘.๔. การบริหารสิทธิ์การเข้าถึงระบบของผู้ใช้งาน ผู้ดูแลระบบ ต้องกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วย

๘.๕. การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน ผู้ดูแลระบบต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ อย่างน้อย ๑ ครั้งในรอบ ๖ เดือน

๙. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ สามารถเข้าถึงระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้

๙.๑. การใช้งานรหัสผ่าน ผู้ดูแลระบบต้องกำหนดวิธีปฏิบัติที่ดีในการเลือกใช้งานรหัสผ่าน การยกเลิกและการเปลี่ยนแปลงรหัสผ่าน

๙.๑.๑. ผู้ดูแลระบบทำหน้าที่เฝ้าระวังการใช้งานผิดวัตถุประสงค์

๙.๑.๒. ผู้ดูแลระบบมีหน้าที่รายงานเหตุการณ์ผิดปกติให้กับผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

๙.๑.๓. ผู้ใช้งานต้องปฏิบัติตามคำแนะนำเมื่อผู้ดูแลระบบแจ้งให้เปลี่ยนรหัสผ่าน

๙.๑.๔. ผู้ดูแลระบบจะมีรหัสผ่านสองชุดเพื่อจัดการระบบ ชุดแรกเป็นรหัสผ่านที่ใช้ปกติ ชุดที่สองเป็นรหัสผ่านสำรองสำหรับการใช้งานในกรณีฉุกเฉิน

๙.๑.๕. ผู้ใช้งานต้องเขียนรหัสผ่านไว้ในรูปของเอกสารลับและส่งมอบให้ผู้ดูแลระบบเก็บรักษาไว้ หากมีการเปลี่ยนแปลงรหัสผ่านจะต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๙.๑.๖. เลือกรหัสผ่านที่ปลอดภัยและรักษารหัสนั้นให้เป็นความลับอยู่ตลอดเวลา การเปลี่ยนแปลงรหัสบัญชีควรเปลี่ยนทุก ๖ เดือน

๙.๑.๗. ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชีเช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ

๙.๑.๘. ไม่ปลอมแปลงชื่อภายใต้ระบบบัญชี หรือสร้างความเข้าใจให้ดูว่าเป็นบุคคลอื่น

๙.๑.๙. ไม่ลักลอบใช้รหัสผ่าน หรือแกะรหัสผ่านของผู้ใช้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

๙.๑.๑๐. รายงานการล่วงละเมิดความปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที

๙.๒. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล ผู้ใช้งานต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ใช้ดูแล

๙.๒.๑. ผู้ดูแลระบบมีอำนาจที่จะยุติหรือเพิกถอนสิทธิ์การใช้คอมพิวเตอร์และเครือข่ายโดยทันทีหากตรวจพบผู้ใช้ที่ฝ่าฝืนระเบียบหรือกระทำการใดที่อาจสร้างความเสียหายให้กับระบบ

๙.๒.๒. เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องควรติดตั้งระบบ screen saver โดยกำหนดรหัสในการเข้าใช้

๙.๒.๓. การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์จะเป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์นั้น

๙.๓. การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

๙.๓.๑. เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

๙.๓.๒. ผู้ใช้งานควรล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๙.๓.๓. การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา, smart mobile device เช่น เมื่อปฏิบัติงานอยู่นอกสถานที่

- ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง
- ต้องใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพา
- ต้องเข้ารหัสข้อมูลที่สำคัญไว้เป็นต้น

๙.๔. ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๙.๔.๑. ต้องแสดงหลักฐานเกณฑ์ในการกำหนดเครื่องข้อมูลลับ หรือข้อมูลที่สำคัญ

๙.๔.๒. ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ

๑๐. ข้อกำหนดการใช้งานเครือข่าย

๑๐.๑.สิทธิ์การใช้เครือข่าย

๑๐.๑.๑. สิทธิ์การใช้เครือข่ายเป็นสิทธิพิเศษเฉพาะ (privilege) ที่มหาวิทยาลัยเกษตรศาสตร์ มอบให้บุคคลหรือหน่วยงานที่ได้รับสิทธิ์ไม่สามารถโอนสิทธิ์ให้แก่บุคคลอื่นหรือหน่วยงานอื่นได้

๑๐.๑.๒. ผู้ใช้ต้องเคารพในสิทธิส่วนบุคคลและไม่ละเมิดความเป็นส่วนตัวของผู้ใช้รายอื่น

๑๐.๑.๓. ผู้ใช้ต้องใช้ระบบเครือข่ายคอมพิวเตอร์ตามมารยาทและจรรยาบรรณของการใช้เครือข่ายตามที่มหาวิทยาลัยเกษตรศาสตร์กำหนดและตามวิถีสากล

๑๐.๒.การใช้งานที่ไม่อนุญาตให้ปฏิบัติ

๑๐.๒.๑. การใช้ระบบเครือข่ายคอมพิวเตอร์เพื่อกระทำสิ่งที่ผิดกฎหมาย

๑๐.๒.๒. การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ด้วยบัญชีของผู้อื่นทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี

๑๐.๒.๓. การเข้าถึงข้อมูลของผู้อื่นเพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม โดยไม่ได้รับอนุญาต

๑๐.๒.๔. การเผยแพร่ข้อมูลของผู้ใช้หรือของหน่วยงานโดยไม่ได้รับอนุญาต

๑๐.๒.๕. การใช้งานที่เป็นสาเหตุให้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เสียหายหรือมีผลต่อประสิทธิภาพการทางานของระบบ

๑๐.๒.๖. การพยายามทำลายหรือทำลายระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

๑๐.๒.๗. การใช้หรือเผยแพร่ซอฟต์แวร์โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

๑๐.๒.๘. การลักลอบดักจับข้อมูลในระบบเครือข่ายคอมพิวเตอร์

๑๐.๒.๙. การปลอมแปลงเป็นบุคคลอื่นเพื่อสร้างความเข้าใจผิดให้แก่ระบบคอมพิวเตอร์และผู้ใช้อื่น

๑๐.๒.๑๐. การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์หรือเครือข่ายอื่น

๑๐.๒.๑๑. การเผยแพร่และ/หรือการเข้าถึงสื่อลามกอนาจาร

๑๐.๒.๑๒. การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อเปิดให้บริการใด ๆ โดยไม่ได้รับอนุญาต

๑๐.๒.๑๓. การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อประกอบธุรกิจ

๑๐.๒.๑๔. การนำไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์ไปจดทะเบียนชื่อโดเมนอื่นนอกเหนือจากชื่อโดเมน ku.ac.th, ku.th, kasetsart.org โดยไม่ได้รับอนุญาต

๑๐.๒.๑๕. การใช้ระบบเครือข่ายคอมพิวเตอร์อื่นใดที่ขัดต่อนโยบายและระเบียบของมหาวิทยาลัยเกษตรศาสตร์

๑๐.๓.การฝ่าฝืนระเบียบและการพิจารณาโทษ

๑๐.๓.๑. มหาวิทยาลัยเกษตรศาสตร์ จะไม่รับผิดชอบต่อผลของการกระทำที่เกิดขึ้นจากผู้ใช้และ/หรือบัญชีผู้ใช้

๑๐.๓.๒. ผู้ใช้ที่ฝ่าฝืนระเบียบการใช้งานระบบเครือข่ายคอมพิวเตอร์จะถูกพิจารณาระงับและ/หรือยกเลิกบัญชีผู้ใช้

๑๐.๓.๓. สำนักบริการคอมพิวเตอร์จะแจ้งหน่วยงานต้นสังกัดเพื่อพิจารณาโทษแก่ผู้ใช้ที่ฝ่าฝืนระเบียบ

๑๑. การใช้ไอพีแอดเดรสและชื่อโดเมนของระบบเครือข่ายคอมพิวเตอร์

๑๑.๑.การจัดสรรไอพีแอดเดรส

๑๑.๑.๑. ไอพีแอดเดรส 158.108.0.0/16, 2001:3c8:1303::/48, 2406:3100::/32 ของระบบเครือข่ายคอมพิวเตอร์เป็นทรัพย์สินของมหาวิทยาลัยเกษตรศาสตร์ โดยมหาวิทยาลัยเกษตรศาสตร์มอบอำนาจให้สำนักบริการคอมพิวเตอร์ทำหน้าที่บริหารจัดการ

๑๑.๑.๒. ให้สำนักบริการคอมพิวเตอร์ทำหน้าที่จัดสรรไอพีแอดเดรสให้กับหน่วยงานตามที่ร้องขอเพื่อให้ใช้งานได้อย่างเพียงพอและมีประสิทธิภาพ โดยสำนักบริการคอมพิวเตอร์สามารถปรับเปลี่ยนไอพีแอดเดรสที่ได้จัดสรรให้กับหน่วยงานจากหมายเลขเดิมเป็นหมายเลขใหม่ได้ตามหลักวิชาการ เพื่อให้สามารถบริหารและจัดการได้อย่างมีประสิทธิภาพ

๑๑.๒.การจัดการชื่อโดเมน

๑๑.๒.๑. มหาวิทยาลัยเกษตรศาสตร์ ได้ขึ้นทะเบียนชื่อโดเมนของมหาวิทยาลัยเกษตรศาสตร์ภายใต้ชื่อ “ku.ac.th , ku.th และ kasetsart.org” โดยสำนักบริการคอมพิวเตอร์รับภาระชำระค่าธรรมเนียมการขึ้นทะเบียนและค่าบำรุงรักษาชื่อโดเมน

๑๑.๒.๒. ให้สำนักบริการคอมพิวเตอร์ทำหน้าที่ให้บริการจดทะเบียนชื่อโดเมนประจำหน่วยงานและชื่อเครื่องภายใต้ชื่อโดเมนของมหาวิทยาลัยเกษตรศาสตร์

๑๑.๒.๓. หน่วยงานมีสิทธิ์ในการใช้ชื่อโดเมน ku.ac.th, ku.th และ kasetsart.org โดยยื่นเรื่องขออนุมัติต่อผู้อำนวยการสำนักบริการคอมพิวเตอร์ คำขออนุมัติจะต้องลงนามรับรองโดยคณบดี หรือผู้อำนวยการหรือหัวหน้าหน่วยงานเทียบเท่า

๑๑.๒.๔. โครงการพิเศษหรือโครงการใด ๆ ที่ได้รับอนุมัติจากมหาวิทยาลัยเกษตรศาสตร์สามารถขอจดชื่อโดเมนประจำโครงการได้ โดยหากเป็นโครงการระดับหน่วยงานให้จดทะเบียนภายใต้ชื่อโดเมนย่อยประจำหน่วยงานนั้น หรือในกรณีที่เป็นโครงการระดับมหาวิทยาลัยจะสามารถยื่นขอจดชื่อโดเมนภายใต้ชื่อโดเมนของมหาวิทยาลัยเกษตรศาสตร์ได้

๑๑.๒.๕. กลุ่มกิจกรรมมีสิทธิ์ในการขอใช้ชื่อโดเมนประจำกลุ่มกิจกรรมได้ โดยต้องมีหัวหน้ากลุ่มกิจกรรมและหัวหน้าหน่วยงานระดับภาควิชาหรือเทียบเท่าที่หัวหน้ากลุ่มกิจกรรมนั้นสังกัดอยู่ลงนามเห็นชอบ และยื่นเรื่องขออนุมัติต่อผู้อำนวยการสำนักบริการคอมพิวเตอร์

๑๑.๒.๖. การใช้ไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์ เพื่อจดทะเบียนชื่อโดเมนนอกสาระบบชื่อโดเมนของมหาวิทยาลัยเกษตรศาสตร์ โดยมิได้รับอนุญาตเป็นสิ่งต้องห้าม ยกเว้นกรณีมีเหตุผลความจำเป็นอย่างยิ่ง ทั้งนี้ให้หัวหน้าหน่วยงานที่ดำรงตำแหน่งคณบดีหรือผู้อำนวยการ หรือหัวหน้าหน่วยงานเทียบเท่า

ดำเนินการยื่นคำร้องต่อผู้อำนวยการสำนักบริการคอมพิวเตอร์ โดยชี้แจงเหตุผลและความจำเป็นที่ต้องขอจดทะเบียนชื่อโดเมนนอกสาระบบ การอนุมัติจดทะเบียนให้อยู่ในดุลยพินิจของผู้อำนวยการสำนักบริการคอมพิวเตอร์

๑๒. การใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail)

จดหมายอิเล็กทรอนิกส์ (e-mail) เป็นบริการที่มหาวิทยาลัยเกษตรศาสตร์จัดให้มีเพิ่มสนับสนุนการศึกษา การวิจัย การบริการ วิชาการ และการบำรุงศิลปวัฒนธรรม ตลอดจนการบริหารจัดการตามภารกิจของหน่วยงาน ผู้ใช้จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยเกษตรศาสตร์ภายใต้ชื่อโดเมน (Domain) ที่จดทะเบียนโดยมหาวิทยาลัยเกษตรศาสตร์ มีหน้าที่พึงปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ โดยไม่ขัดกับนโยบายการใช้คอมพิวเตอร์ของมหาวิทยาลัยเกษตรศาสตร์

๑๒.๑.ข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)

๑๒.๑.๑. ผู้ใช้มีหน้าที่และความรับผิดชอบโดยพึงระวังไม่ให้ผู้อื่นเข้าถึงรหัสผ่านเพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบ ผู้ใช้ต้องรักษารหัสผ่านเป็นความลับเฉพาะตัวและไม่อนุญาตให้ผู้อื่นเข้าใช้จดหมายอิเล็กทรอนิกส์ในนามของตนเองในทุกกรณี ผู้ใช้เป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้จดหมายอิเล็กทรอนิกส์ และการอนุญาตให้ผู้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ในนามของตนเอง

๑๒.๑.๒. ผู้ใช้พึงทราบว่าผู้ดูแลระบบไม่มีสิทธิ์ที่จะถามหรือร้องขอให้ผู้ใช้เปิดเผยรหัสผ่านประจำตัวเพื่อเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์

๑๒.๑.๓. ผู้ใช้ต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

๑๒.๑.๔. การใช้จดหมายอิเล็กทรอนิกส์ ในลักษณะต่อไปนี้เป็นสิ่งต้องห้าม

(๑) การใช้จดหมายอิเล็กทรอนิกส์ เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น

(๒) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่จดหมายลูกโซ่

(๓) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลชั้นความลับของมหาวิทยลัย

(๔) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลการประชุมของที่ประชุมผู้บริหารมหาวิทยาลัยหรือในการประชุมอื่นๆ โดยที่มิได้มีหน้าที่ หรือมิได้รับมอบหมายจากประธานในที่ประชุม

(๕) การปลอมแปลงหรือดับแปลงชื่อผู้ส่งให้เข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้นๆ ส่งมาจากบุคคลอื่น

(๖) การปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

(๗) การปลอมแปลงหรือดับแปลงส่วนหัวจดหมาย เช่น เส้นทาง วันเวลาการส่ง

(๘) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่กล่าวร้ายต่อบุคคลหรือกลุ่มบุคคล

(๙) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดีโด เสียง ที่ดูหมิ่น เหยียดหยาม หรือแบ่งแยกทาง ศาสนา เชื้อชาติ หรือเพศ

(๑๐) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่มีลักษณะหยาบคาย หรือลามกอนาจาร

(๑๑) การส่งจดหมายอิเล็กทรอนิกส์ เพื่อเผยแพร่โปรแกรมหรืองาน หรือเผยแพร่รหัสสำหรับใช้เข้าถึงโปรแกรมหรืองาน ในลักษณะที่ละเมิดลิขสิทธิ์

(๑๒) การส่งจดหมายอิเล็กทรอนิกส์ กระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

(๑๓) การส่งจดหมายอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบให้ระบบจดหมายอิเล็กทรอนิกส์หรือเครือข่ายลดทอนประสิทธิภาพลง

(๑๔) การส่งจดหมายอิเล็กทรอนิกส์ กระจายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบความมั่นคงปลอดภัย

๑๒.๒.การจัดการรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (Mailing List)

สำนักบริการคอมพิวเตอร์จัดให้มีระบบรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ เพื่อสร้างช่องทางการส่งจดหมายอิเล็กทรอนิกส์แบบกลุ่ม รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ที่บรรจุรายชื่อบัญชีผู้ใช้ที่ขึ้นทะเบียนในเครือข่ายของมหาวิทยาลัยเกษตรศาสตร์ หรือรายชื่อแยกตามกลุ่มของมหาวิทยาลัยเกษตรศาสตร์ เป็นข้อมูลปกปิดที่ไม่เผยแพร่ให้ผู้ใช้หรือหน่วยงานใดๆ การใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ดังกล่าวมีข้อกำหนดเฉพาะดังนี้

๑๒.๒.๑. หน่วยงานที่ได้รับมอบหมายจากอธิการบดี ใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่ข่าวสารและประชาสัมพันธ์ภารกิจของมหาวิทยาลัยเกษตรศาสตร์

๑๒.๒.๒. สำนักบริการคอมพิวเตอร์ใช้เพื่อแจ้งเตือน หรือแจ้งข่าวที่เกี่ยวข้องกับความมั่นคงปลอดภัย หรือการรักษาประสิทธิภาพของระบบคอมพิวเตอร์และเครือข่าย

๑๒.๒.๓. สำนักบริการคอมพิวเตอร์จัดให้มีระบบรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์กลุ่มย่อยตามคำร้องขอของหน่วยงาน ซึ่งต้องให้ผู้ใช้สมัครใจเข้าเป็นสมาชิกกลุ่มเพื่อรับข่าวสารเอง และผู้ใช้สามารถถอนการเป็นสมาชิกเพื่องดรับข่าวสารนั้นได้ตลอดเวลา ทั้งนี้ มหาวิทยาลัยเกษตรศาสตร์ไม่อนุญาตให้สร้างบริการรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์อื่นใดเอง เพื่อป้องกันการใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ที่บรรจุรายชื่อบัญชีจดหมายอิเล็กทรอนิกส์ โดยผู้ใช้ไม่สมัครใจบอกรับ ทั้งนี้ สำนักบริการคอมพิวเตอร์สงวนสิทธิ์ในการอนุมัติการขอจดทะเบียนชื่อกลุ่ม ตลอดจนการตั้งชื่อกลุ่ม ตามความเหมาะสม

๑๒.๓.โควตาบัญชีจดหมายอิเล็กทรอนิกส์ บัญชีจดหมายอิเล็กทรอนิกส์ ของผู้ใช้แต่ละรายจะมีโควตากำหนดการใช้งานดังนี้

๑๒.๓.๑. ขนาดข้อมูลรวมที่เก็บในเซิร์ฟเวอร์

๑๒.๓.๒. ขนาดของไฟล์แนบต่อการส่งจดหมายอิเล็กทรอนิกส์ หนึ่งฉบับ

๑๒.๓.๓. จำนวนบัญชีผู้รับต่อการส่งจดหมายอิเล็กทรอนิกส์ หนึ่งฉบับ

๑๒.๓.๔. อัตราส่งจดหมายอิเล็กทรอนิกส์ ต่อวันเวลาที่กำหนด

๑๒.๓.๕. จำนวนจดหมายอิเล็กทรอนิกส์ ต่อวันเวลาที่กำหนด

๑๒.๓.๖. โควตาเหล่านี้อาจแตกต่างกันตามประเภทและภารกิจของผู้ใช้ การกำหนดโควตาให้อยู่ในดุลยพินิจของสำนักบริการคอมพิวเตอร์ โดยสามารถเพิ่มหรือลดค่าแต่ละบัญชีจดหมายอิเล็กทรอนิกส์ตามความเหมาะสมเพื่อให้การใช้งาน และการบริหารจัดการเป็นไปอย่างมีประสิทธิภาพ

๑๒.๔.การตรวจระวังระบบ

มหาวิทยาลัยเกษตรศาสตร์มีนโยบายปกป้องข้อมูลส่วนบุคคลและให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อสนับสนุนภารกิจของมหาวิทยาลัยเกษตรศาสตร์ โดยไม่ตรวจดูจดหมายอิเล็กทรอนิกส์ที่รับส่งตามปกติ แต่มหาวิทยาลัยเกษตรศาสตร์มีภาระผูกพันตามกฎหมายที่ต้องติดตั้งระบบบันทึกข้อมูลจราจรและการเฝ้าระวังเพื่อคงไว้ซึ่งบริการที่มั่นคงปลอดภัยและมีประสิทธิภาพ มหาวิทยาลัยเกษตรศาสตร์สงวนสิทธิ์ในการใช้ระบบเฝ้าระวังเพื่อตรวจเนื้อหาจดหมายอิเล็กทรอนิกส์ที่เป็นภัยต่อระบบคอมพิวเตอร์ และกลั่นกรองหรือระงับการเผยแพร่นั้นโดยอัตโนมัติ ตลอดจนสงวนสิทธิ์การเข้าถึงจดหมายอิเล็กทรอนิกส์ เพื่อสืบสวน สอบสวน เมื่อระบบเฝ้าระวังแจ้งเตือนถึงปัญหาด้านความมั่นคงปลอดภัยจากการใช้จดหมายอิเล็กทรอนิกส์ใดๆ หรือการร้องขอจากเจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๒.๕. การระงับบัญชีจดหมายอิเล็กทรอนิกส์

บัญชีจดหมายอิเล็กทรอนิกส์เป็นสิทธิพิเศษเฉพาะ (Privilege) ที่มหาวิทยาลัยเกษตรศาสตร์เอื้ออำนวยให้ผู้ใช้ ซึ่งผู้ใช้ไม่สามารถโอนสิทธิ์ให้แก่ผู้อื่นใช้ได้ มหาวิทยาลัยเกษตรศาสตร์คงไว้ซึ่งอำนาจในการจำกัดระงับ หรือเพิกถอนสิทธิ์ให้แก่ผู้ใช้โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบายหรืออาจก่อให้เกิดปัญหา ความมั่นคงปลอดภัยหรือเสถียรภาพของระบบ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ การระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์ มีแนวปฏิบัติ ดังนี้

๑๒.๖. เมื่อผู้ใช้พ้นสภาพการอยู่ในสังกัดของมหาวิทยาลัยเกษตรศาสตร์ สำนักบริการคอมพิวเตอร์สามารถระงับบัญชีผู้ใช้ ซึ่งส่งผลให้การเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ผ่านบัญชีนั้นถูกระงับไปด้วย หากแต่ผู้ใช้ยังสามารถมีชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์สำหรับใช้ติดต่อได้ผ่านระบบจดหมายอิเล็กทรอนิกส์อีกระบบหนึ่งที่สำนักบริการคอมพิวเตอร์จัดบริการไว้ให้ (e-Mail for Life)

๑๒.๗. ผู้ใช้สามารถร้องขอการขยายสิทธิ์การใช้บัญชีผู้ใช้เพื่อคงสิทธิ์การใช้บัญชีจดหมายอิเล็กทรอนิกส์เดิมไว้ เมื่อต้องพ้นสภาพการอยู่ในสังกัดของมหาวิทยาลัยเกษตรศาสตร์ โดยยื่นคำร้องผ่านผู้บริหารต้นสังกัดพร้อมแนบเหตุผลความจำเป็นส่งถึงสำนักบริการคอมพิวเตอร์ การอนุญาตและระยะเวลาการขยายสิทธิ์ให้เป็นอำนาจของผู้อำนวยการสำนักบริการคอมพิวเตอร์หรือผู้ที่อธิการบดีมอบหมาย

๑๒.๘. บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งาน โดยคำร้องขอจากภาควิชาหรือคณบดี หรือผู้บริหารเทียบเท่าหัวหน้าภาควิชาหรือคณบดี หากพบว่ามีการใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ในสังกัดของหน่วยงานที่ขัดกับนโยบายฉบับนี้

๑๒.๙. บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งานโดยทันทีโดยผู้ดูแลระบบหากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบให้ประสิทธิภาพระบบเครือข่ายด้อยลง หรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้โดยผู้ใช้หรือการลักลอบเข้าใช้โดยผู้อื่น ทั้งนี้ สำนักบริการคอมพิวเตอร์มีสิทธิ์ระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้น ๆ โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

๑๓. การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

การใช้บริการด้านไอซีทีจากหน่วยงานภายนอก บางครั้งหน่วยงานภายนอกอาจเข้าถึงระบบสารสนเทศ แก้ไข เปลี่ยนแปลง และประมวลผลระบบงานโดยไม่ได้รับอนุญาต ดังนั้น จึงต้องกำหนดแนวทางในการปฏิบัติงานของหน่วยงานภายนอกเพื่อความมั่นคง ปลอดภัย ของระบบสารสนเทศของมหาวิทยาลัยเกษตรศาสตร์ โดยนโยบายและแนวปฏิบัตินี้ต้องตรวจสอบ และประเมินตามระยะเวลา 1 ครั้งต่อปี

๑๓.๑.บุคคลภายนอก ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศและการสื่อสารของมหาวิทยาลัยเกษตรศาสตร์ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้อำนวยการสำนักบริการคอมพิวเตอร์ หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย

๑๓.๒.สำนักบริการคอมพิวเตอร์ หรือหน่วยงานที่เกี่ยวข้องต้องจัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

๑๓.๒.๑. เหตุผลในการขอใช้งาน

๑๓.๒.๒. ระยะเวลาในการใช้งาน

๑๓.๒.๓. การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๑๓.๒.๔. การตรวจสอบ Mac Address ของอุปกรณ์ที่เชื่อมต่อ

๑๓.๒.๕. การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๑๓.๓.หน่วยงานภายนอกที่ทำงานให้กับมหาวิทยาลัยเกษตรศาสตร์ทุกหน่วยงาน จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของมหาวิทยาลัยเกษตรศาสตร์ โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบสารสนเทศ

๑๓.๔.ผู้ให้บริการจากหน่วยงานภายนอก ต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

๑๓.๕.เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๑๓.๖.มหาวิทยาลัยเกษตรศาสตร์มีสิทธิ์ในการตรวจสอบตามสัญญาการใช้บริการด้านไอซีทีเพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

๑๔. การดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ก่อให้เกิดความเชื่อมั่นต่อระบบ ส่งผลถึงความเชื่อมั่นต่อองค์กร หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย จำเป็นต้องมีการตอบสนองต่อเหตุการณ์อย่างทันท่วงที ดังนั้น จึงต้องมีแนวปฏิบัติเมื่อเกิดเหตุการณ์ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๑๔.๑.ระบบไฟร์วอลล์

๑๔.๑.๑. ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละครั้ง

๑๔.๑.๒. ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟล์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๑๔.๑.๒.๑. กลุ่มข้อมูล (Packet) ที่ไฟล์วอลล์ได้ปิดกั้น

๑๔.๑.๒.๒. ลักษณะของกลุ่มข้อมูล (Packet) ที่ถูกปิดกั้น

๑๔.๑.๒.๓. หมายเลขไอพี ของเครือข่ายใดที่ถูกปิดกั้น เป็นจำนวนมาก

๑๔.๑.๓. หากตรวจสอบพบการโจมตี หรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศ ให้แจ้งผู้อำนวยการสำนักบริการคอมพิวเตอร์ หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

๑๔.๑.๔. กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

๑๔.๒.เครื่องคอมพิวเตอร์แม่ข่าย

๑๔.๒.๑. ต้องตรวจสอบความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่ายก่อนให้บริการ โดยอย่างน้อยต้องดำเนินการดังต่อไปนี้

๑๔.๒.๑.๑. ติดตั้งไฟล์วอลล์ที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เปิดเฉพาะ port ที่ใช้งาน

๑๔.๒.๑.๒. ปิด Service ที่ไม่ได้ใช้งาน

๑๔.๒.๑.๓. ติดตั้ง NTP เพื่อเทียบเวลาให้ถูกต้อง

๑๔.๒.๑.๔. จำกัดการเข้าถึงจาก root หรือ Administrator โดยตรง

๑๔.๒.๒. หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแลและกำหนดผู้ดูแลรับผิดชอบหลัก และผู้รับผิดชอบสำรอง

๑๔.๒.๓. หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องตรวจสอบความมั่นคงปลอดภัย ต้องจดบันทึก ตรวจสอบ แก้ไข และรายงาน เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยต่อผู้บังคับบัญชา หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย

๑๔.๒.๔. หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องตรวจสอบ แก้ไข และรายงานช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายต่อ หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย

๑๔.๒.๕. กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ต้องดำเนินการแจ้งไปยังผู้รับผิดชอบหน่วยงาน หรือผู้มีอำนาจที่ได้รับมอบหมาย ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

๑๔.๓.ภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ต ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

๑๔.๓.๑. มหาวิทยาลัยเกษตรศาสตร์ต้องดำเนินการจัดหาซอฟต์แวร์เพื่อป้องกัน

๑๔.๓.๒. หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่ออินเทอร์เน็ต ต้องดำเนินการติดตั้งโปรแกรมป้องกันภัยคุกคามทางอินเทอร์เน็ต และต้องตั้งให้มีการ Update อย่างน้อยสัปดาห์ละครั้ง

๑๔.๓.๓. ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของของอุปกรณ์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๑๔.๓.๓.๑. การคุกคามทางอินเทอร์เน็ตใดที่มีเป็นจำนวนมาก

๑๔.๓.๓.๒. ถูกส่งมาจากที่ใด และถูกส่งไปยังที่ใด

๑๔.๓.๔. ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่มีภัยคุกคามทางอินเทอร์เน็ต โดยเฉพาะที่ตรวจพบว่ามีการกระจายภายในเครือข่ายมหาวิทยาลัยเกษตรศาสตร์

๑๔.๓.๕. กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

ระดับความรุนแรงของเหตุการณ์

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
๐	ไม่มีผลกระทบ	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ
๑	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
๒	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
๓	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
๔	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
๕	ปิดหน่วยงาน	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

หมวดที่ ๓
นโยบายการสำรองและกู้คืนสารสนเทศ

วัตถุประสงค์

๑. เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและระบบคอมพิวเตอร์
๒. เพื่อให้มีการสำรองข้อมูลที่สำคัญให้ครบทุกหมวดหมู่
๓. เพื่อให้มีลักษณะการปฏิบัติการสำรองข้อมูลและกู้คืนข้อมูลที่เป็นมาตรฐาน
๔. เพื่อป้องกันและขจัดปัญหาข้อมูลสำคัญสูญหาย

ผู้รับผิดชอบ

๑. สำนักบริการคอมพิวเตอร์
๒. หน่วยงานที่ให้บริการเครื่องคอมพิวเตอร์แม่ขาย
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติการสำรองข้อมูล

๑. หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการต้องดำเนินการสำรองข้อมูล ดังนี้
   ๑.๑. ผู้ดูแลระบบต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และจัดระดับความสำคัญของข้อมูล
   ๑.๒. ผู้ดูแลระบบต้องจัดให้มีระบบการสำรองข้อมูล
   ๑.๓. ผู้ดูแลระบบต้องจัดทำผังหรือขั้นตอนการสำรองข้อมูล
   ๑.๔. ผู้ดูแลระบบต้องทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
   ๑.๕. ผู้ดูแลระบบต้องจัดทำบันทึกการสำรองข้อมูล และตรวจสอบว่าการสำรองข้อมูลสำเร็จหรือไม่ แก้ไข และรายงานต่อผู้บังคับบัญชา หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย
   ๑.๖. ผู้ดูแลระบบต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงาน
   ๑.๗. ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลที่มีระดับความสำคัญสูง (Encrypted backup) โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย
   ๑.๘. ผู้ดูแลระบบต้องดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชา หรือ ผู้มีอำนาจตามที่ได้รับมอบหมายในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้
   ๑.๙. ผู้ดูแลระบบเป็นผู้กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
   ๑.๑๐.ผู้ดูแลระบบทดสอบข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง
   ๑.๑๑.ผู้ดูแลระบบสำรวจข้อมูล และ จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรอง และความถี่ในการสำรองข้อมูล ดังนี้

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
๐	ไม่มีผลกระทบ	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ
๑	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
๒	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
๓	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
๔	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
๕	ปิดหน่วยงาน	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

๑.๑๒.ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยว่าการสำรองข้อมูลตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

ที่	รายการ	ระดับความสำคัญ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล	ระยะเวลาสำรองข้อมูล	ระยะเวลาการกู้คืนข้อมูล
๑	Mail servers	๔	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง	๑ เดือน	๔ ชม.
			ข้อมูลในเมล์บ็อกซ์	การสำรองข้อมูลแบบเต็ม (Full Backup) ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่	๑ เดือน	๔ ชม.
๒	Web servers	๒	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง	๑ เดือน	๔ ชม.
			ข้อมูลเผยแพร่บนเว็บไซต์	การสำรองข้อมูลแบบเต็ม ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่	๑ เดือน	๔ ชม.
๓	Database servers	๔	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง	๑ เดือน	๔ ชม.
			ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	การสำรองข้อมูลแบบเต็ม ทุกวัน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่	๑ เดือน	๔ ชม.
๔	Firewall server	๓	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง	๑ เดือน	๔ ชม.
			ข้อมูล Rule ของ Firewall	การสำรองข้อมูลแบบเต็ม ๑ ครั้งต่อเดือน และนำสื่อบันทึก	๑ เดือน	๔ ชม.

ที่	รายการ	ระดับความสำคัญ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล	ระยะเวลาสำรองข้อมูล	ระยะเวลาการกู้คืนข้อมูล
				ข้อมูลนั้นไปไว้นอกสถานที่		
๕	เซิร์ฟเวอร์อื่น ๆ เช่น ... (ต้องกำหนดเองว่าเซิร์ฟเวอร์อื่น ๆ ได้แก่อะไรบ้าง	...	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง	๑ เดือน	๔ ชม.
			ข้อมูลบนเซิร์ฟเวอร์อื่น ๆ	การสำรองข้อมูลแบบเต็ม ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่	๑ เดือน	๔ ชม.

๒. แนวปฏิบัติการกู้คืนข้อมูล

๒.๑. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย ดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงาน ต่อผู้บังคับบัญชา หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย

๒.๒. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๒.๓. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๒.๔. แผนการกู้คืน

สาเหตุ	วิธีการ
กรณีที่ ๑ เกิดความเสียหายขึ้นกับโปรแกรมต้นฉบับ (Source code)	ดำเนินการติดตั้งโปรแกรมต้นฉบับ (Source code) ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด
กรณีที่ ๒ เกิดความเสียหายขึ้นกับฐานข้อมูล (Database)	ดำเนินการกู้คืนฐานข้อมูลที่เก็บไว้ล่าสุด เพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด
กรณีที่ ๓ เกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ฮาร์ดแวร์ยังคงทำงานปกติ	ดำเนินการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจากโปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมถึงกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

สาเหตุ	วิธีการ
กรณีที่ ๔ เกิดความเสียหายขึ้นกับฮาร์ดแวร์	ให้บริษัทผู้ดูแลแก้ไขเบื้องต้นให้ฮาร์ดแวร์สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับระบบปฏิบัติการและระบบงาน ให้บริษัทหรือผู้ได้รับมอบหมายดำเนินการติดตั้งระบบปฏิบัติการและระบบงานนั้นใหม่ โดยใช้โปรแกรมต้นฉบับ ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

๓. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

๓.๑. ผู้ดูแลระบบต้องจัดทำแผนความพร้อมกรณีฉุกเฉิน โดยแผนความพร้อมกรณีฉุกเฉินต้องได้รับการเห็นชอบจากผู้บริหารด้านไอทีระดับหน่วยงาน ประกอบด้วย

ก. การกำหนดชนิดของภัยพิบัติ

ข. ประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีระดับความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้

ค. กำหนดขั้นตอนรับมือภัยพิบัติ

๓.๒. ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๓.๓. ทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๔
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

๑. สำนักบริการคอมพิวเตอร์

๒. หน่วยงานที่ให้บริการเครื่องคอมพิวเตอร์แม่ข่าย

๓. สำนักตรวจสอบภายใน

๔. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

๑.๑. ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๑.๒. ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๑.๓. ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๑.๔. ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๒. การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๒.๑. ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๒.๒. ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๒.๓. จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๓. ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ ปีละ ๑ ครั้ง

๔. ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของสำนักตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor)

๕. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๖. มาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

๖.๑. ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๖.๒. ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น สำหรับให้ผู้ตรวจสอบใช้งาน และควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้แหล่งจัดเก็บข้อมูลอื่นที่มีข้อกำหนดการเข้าถึงข้อมูล

๖.๓. กำหนดให้ระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๖.๔. กำหนดให้เฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อก แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

๖.๕. ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาตโดยมีการป้องกันเป็นอย่างดี

๗. ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูง ซึ่งประกอบด้วย อธิการบดี รองอธิการบดีฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการสำนักบริการคอมพิวเตอร์ ซึ่งมีหน้าที่กำกับดูแลด้านสารสนเทศของมหาวิทยาลัย เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นโดยตรง รวมถึงในกรณีที่มีการร้องเรียน และฟ้องร้องภายใต้กฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๘. ต้องสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันที่เหมาะสม

๙. รายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศปีละ ๑ ครั้ง เสนอต่อคณะกรรมการยุทธศาสตร์เทคโนโลยีสารสนเทศ และแจ้งคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยเพื่อดำเนินการต่อไป

๑๐.แสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศผ่านเว็บไซต์ ให้ประชาคมของมหาวิทยาลัยเกษตรศาสตร์ทราบ ตามนโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

หมวดที่ ๕
นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อให้บุคลากรในสังกัดมหาวิทยาลัยเกษตรศาสตร์ ตลอดจนบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึงสารสนเทศ ทราบและเข้าใจถึงความรับผิดชอบถึงการใช้งานนั้นอย่างถูกต้องตามหลักจริยธรรมและหลักกฎหมาย

๒. สร้างความมั่นใจว่าการใช้และการรักษาความมั่นคงปลอดภัยสารสนเทศภายในมหาวิทยาลัยเกษตรศาสตร์เป็นไปอย่างถูกต้องตามกฎหมายและข้อบังคับที่เกี่ยวข้อง

๓. เพื่อป้องกันการใช้งานระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ผิดวัตถุประสงค์

ผู้รับผิดชอบ

๑. สำนักบริการคอมพิวเตอร์

๒. กองการเจ้าหน้าที่ สำนักอธิการบดี

๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยจัดสัมมนาอย่างน้อยปีละ ๑ ครั้ง

๒. ผู้ดูแลระบบต้องจัดให้มีหลักสูตรที่สอดคล้องกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศเพื่อป้องกันการเข้าถึงจากผู้ใช้ซึ่งไม่ได้รับอนุญาต

๓. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ หรือเผยแพร่เกร็ดความรู้ในการใช้งานอย่างสม่ำเสมอ

๔. จัดทำคู่มือการใช้งานสารสนเทศ และเผยแพร่ทางเว็บไซต์ของมหาวิทยาลัย