ประกาศมหาวิทยาลัยนวมินทราธิราช
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของมหาวิทยาลัยนวมินทราธิราช มีความมั่นคง ปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล อันจะเป็นการป้องกันปัญหาที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและภัยคุกคามต่าง ๆ จึงสมควรให้มีประกาศมหาวิทยาลัยนวมินทราธิราช เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

อาศัยอำนาจตามความในมาตรา ๓๑ แห่งพระราชบัญญัติมหาวิทยาลัยนวมินทราธิราช พ.ศ. ๒๕๕๓ และมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศไว้ ดังต่อไปนี้

๑. ประกาศนี้เรียกว่า "ประกาศมหาวิทยาลัยนวมินทราธิราช เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย"

๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

๓. ในประกาศนี้

"มหาวิทยาลัย" หมายความว่า มหาวิทยาลัยนวมินทราธิราช

"นโยบาย" หมายความว่า แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยนวมินทราธิราช

"แนวปฏิบัติ" หมายความว่า แนวทางปฏิบัติ ข้อปฏิบัติ และหรือวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยนวมินทราธิราช

คำนิยามที่มิได้กำหนดไว้ในประกาศนี้ให้นำคำนิยามในประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม มาใช้โดยอนุโลม

๔. บรรดาประกาศหรือคำสั่งอื่นใดที่ขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย มีวัตถุประสงค์ ดังนี้

๕.๑ เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยเกิดความมั่นคง ปลอดภัยและเชื่อถือได้

๕.๒ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติแก่ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้มหาวิทยาลัย และเผยแพร่ให้ผู้เกี่ยวข้องได้รับทราบ เข้าถึงและถือปฏิบัติตามนโยบายและแนวปฏิบัติอย่างเคร่งครัด โดยต้องมีการทบทวนนโยบายไม่น้อยกว่าปีละ ๑ ครั้ง

๖. นโยบายในการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย ประกอบด้วย

๖.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control)

๖.๑.๑ การควบคุมเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งาน ให้มีกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๖.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิเท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน รวมทั้งต้องมีการทบทวนสิทธิการใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๖.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องกำหนดสิทธิในการเข้าถึงเครือข่าย ผู้จะเข้าใช้งานต้องลงบันทึกการเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ตโดยผ่านระบบรักษาความปลอดภัยของมหาวิทยาลัย และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อให้สามารถควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๖.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องกำหนดให้ผู้เข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนเข้าใช้งาน ต้องมีการกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เกิดการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๖.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น ต้องกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอพพลิเคชั่นต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๖.๒ การจัดการระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องมีการจัดทำระบบสารสนเทศระบบสำรองข้องมูลที่เหมาะสมและอยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับจากมากไปหาน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูลและจัดทำแผนเตรียมความพร้อมฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๖.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้มีผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) ทำการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๗. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยนวมินทราธิราช แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๗ มิถุนายน พ.ศ. ๒๕๖๔

(รองศาสตราจารย์อนันต์ มโนมัยพิบูลย์)
อธิการบดีมหาวิทยาลัยนวมินทราธิราช

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของมหาวิทยาลัยนวมินทราธิราช
ประกาศ ณ วันที่

มาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

ตามประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.๒๕๕๕ และประกาศกระทรวงดิจิทัลเพื่อเศรษกิจและสังคม เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ และตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยพระราชบัญญัติและประกาศดังกล่าวเป็นการบังคับโดยกฎหมายให้มหาวิทยาลัยนวมินทราธิราชปฏิบัติตาม เพื่อให้เกิดมาตรฐานในการบริหารด้านเทคโนโลยีสารสนเทศจึงต้องกำหนดนโยบายให้สอดคล้องกับกฎหมายที่กล่าวมาข้างต้น ในหลาย ๆ ด้าน เพื่อป้องกันภัยคุกคามต่าง ๆ ที่จะส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ รวมไปถึงการปกป้องคุ้มครองข้อมูลส่วนบุคลให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยจะต้องกำหนดนโยบายด้านสารสนเทศให้ครอบคลุมถึงมาตรการป้องกันด้านบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) เพื่อให้เป็นไปตามมาตรฐาน ตามพระราชบัญญัติและประกาศที่กล่าวมาข้างต้น มหาวิทยาลัยนวมินทราธิราช จึงกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยในทุก ๆ ด้าน ดังนี้

คำนิยาม

คำนิยาม		คำอธิบาย
AES	Advanced Encryption Standard	มาตรฐานการเข้ารหัสลับขั้นสูงเป็นข้อกำหนดการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งกำหนดขึ้นในปี ๒๕๔๔ โดยสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (NIST) เทคโนโลยีนี้ได้มีการนำไปใช้โดยรัฐบาลสหรัฐอเมริกาและประเทศอื่น ๆ ทั่วโลก เพื่อปกป้องข้อมูลที่เป็นความลับ
DMZ	Demilitarized Zone	กลุ่มของ Server ต่าง ๆ ที่คอยให้บริการกับทั้ง Internal Zone และ External Zone คือทั้ง ๒ Zone นั้นสามารถใช้บริการจาก DMZ ได้ หรืออาจเรียกได้ว่า DMZ เป็น Public Zone ก็ได้ ตัวอย่างของ Server ใน DMZ เช่น Web Server, Mail Server เป็นต้น
IDS	Intrusion Detection System	Hardware หรือ Software ที่ติดตามตรวจสอบสัญญาณจราจร (Traffic) ที่ส่งผ่านบนเครือข่ายคอมพิวเตอร์ ด้วยการ วิเคราะห์รูปแบบพฤติกรรมในแพ็กเก็ตข้อมูล (Packet Data) เพื่อค้นหาสิ่งที่ผิดปกติ (Anomaly) แล้วนำเข้าสู่กระบวนการทำนาย (Prediction) เพื่อตัดสินว่าเป็นเหตุการณ์ บุกรุกจริง แล้วแจ้งเตือน (Alert) ให้ผู้ดูแลระบบทราบเพื่อดำเนินการป้องกันและแก้ไขต่อไป
IPS	Intrusion Prevention System	Software หรือ Hardware ที่ได้รับการออกแบบมาเพื่อให้ตรวจสอบการบุกรุกโดยจะทำงานคล้าย ๆ กับ IDS แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้องอาศัยโปรแกรมหรือ hardware ตัวอื่น ๆ
MAC Address	Media Access Control Address	หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขที่จะมากับอีเทอร์เน็ตการ์ดโดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง
P๒P	Peer-to-Peer	(หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น

คำนิยาม		คำอธิบาย
SSID	Service Set Identifier	บริการระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน
SSL	Secure Socket Layer	เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องแม่ข่ายกับเว็บบราวเซอร์หรือ Application ที่ใช้งาน เพื่อให้ข้อมูลของท่านปลอดภัยจากการเข้าถึงข้อมูลจากแฮกเกอร์ โดยวิธีการเรียกใช้งาน จะเรียกผ่านโปรโตคอล HTTPS หรือโปรโตคอลความปลอดภัยอื่น ๆ ตามแต่วิธีการใช้งาน
VPN	Virtual Private Network	เครือข่ายส่วนตัวเสมือน โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
WEP	Wire Equivalent Privacy	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้
WPA	Wi-Fi Protected Access	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP
XML	Extensible Markup Language	เป็นการเข้ารหัส SOAP Message เพื่อทำให้ message ที่ส่งมีความปลอดภัยจากผู้ไม่ประสงค์ดี
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศของผู้ใช้งาน	User Access Management	การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึง โดยมิชอบเอาไว้ด้วยก็ได้
การเข้ารหัส	encryption	การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
การควบคุมการเข้าถึงสารสนเทศ	Access Control	หมายถึง การทำให้มั่นใจว่าทรัพยากรต่าง ๆ ของระบบหรือสถานที่ที่มีการควบคุมการเข้าถึง จะได้รับอนุญาตให้ถูกใช้โดยผู้ใช้ที่มีสิทธิ์เท่านั้น

คำนิยาม		คำอธิบาย
การควบคุมการใช้งาน	Usage control	การกำหนดสิทธิ์ในการเข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย
การประมวลผลข้อมูล	Data Processer	การดำเนินการหรือชุดการดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้าง เก็บรักษา เปลี่ยนแปลง หรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อมใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การกำจัด การลบหรือการทำลาย
การประมวลผลแบบกลุ่มเมฆ	Cloud Computing	การใช้ซอฟต์แวร์ระบบ และทรัพยากรของเครื่องคอมพิวเตอร์ของผู้ให้บริการผ่านอินเทอร์เน็ต ผู้ใช้สามารถเลือกกำลังการประมวลผล เลือกจำนวนทรัพยากรได้ตามความต้องการในการใช้งาน ทำให้เราสามารถเข้าถึงข้อมูลบน Cloud จากที่ไหนก็ได้
การเผยแพร่ข้อมูลเว็บไซต์	(Publish Website Information)	การนำข้อมูลตัวอักษร ข้อมูลภาพ ข้อมูลเสียง ข้อมูลภาพเคลื่อนไหว หรือไฟล์ หรือสิ่งอื่นใด เผยแพร่ออกสู่สาธารณะผ่านเว็บไซต์
การพิสูจน์ตัวตน	Authentication	กระบวนการยืนยันความถูกต้องของตัวตนว่าเป็นบุคคลที่ได้กล่าวอ้าง โดยในการพิสูจน์ตัวตนนั้น จะต้องมีขั้นตอนระบุตัวตน เพื่อแสดงตนว่าคือใคร เช่น ชื่อผู้ใช้งาน (Username) และขั้นตอนแสดงหลักฐานว่าเป็นบุคคลที่กล่าวอ้างจริง เช่น รหัสผ่าน (Password
การรับมือเหตุการณ์ผิดปกติทางไซเบอร์	(Cyber Incident Response)	คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet)
ข้อมูล	Data	ข้อเท็จจริงที่เป็นตัวเลข ข้อความ ภาพ เสียง วิดีโอ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่า ด้วยธุรกรรมทางอิเล็กทรอนิกส์
ข้อมูลจราจรทางคอมพิวเตอร์	Log	ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
ข้อมูลส่วนบุคคล	Personal Data	ข้อมูลใด ๆ ที่ระบุไปถึง “เจ้าของข้อมูล” หรือ (Data Subject) ได้

คำนิยาม		คำอธิบาย
ข้อมูลส่วนบุคคลรั่วไหล	Personal Data Breach	การรั่วไหลหรือการละเมิดมาตราการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลทำให้เกิดความเสียหาย สูญเสีย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต หรือเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
ข้อมูลอ่อนไหว	Sensitive Personal Data	เป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนหรือสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ
เข้าถึง หรือการเข้าถึง	Access	การอนุญาต หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงระบบสารสนเทศและระบบเครือข่าย
ความมั่นคงปลอดภัย	Security	สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ
ความมั่นคงปลอดภัยด้านสารสนเทศ	Information security	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ๆ ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ
เครือข่าย หรือระบบเครือข่าย	Network or network system	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless Lan) เป็นต้น
เครือข่ายสังคมออนไลน์	social network	เว็บไซต์หรือแอพพลิเคชันที่ผู้ใช้งานสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่าง ๆ
จดหมายอิเล็กทรอนิกส์, อีเมล	(electronic mail, e-mail)	ระบบรับส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเทคโนโลยีสารสนเทศ ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพนิ่ง ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน
เจ้าของข้อมูลส่วนบุคคล	Data Subject	มีลักษณะเป็นบุคคลที่ข้อมูลนั้นบ่งชี้ไปถึง ไม่ใช่เป็นเจ้าของในลักษณะทรัพย์สิน หรือเป็นสร้างข้อมูลนั้นขึ้นมา เช่น บุคลากร นักศึกษา คนไข้ ผู้ติดต่อ เป็นต้น

คำนิยาม		คำอธิบาย
ชื่อผู้ใช้งาน	Username	ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่ได้กำหนดสิทธิ์การใช้งานไว้
บัญชีผู้ใช้งาน	User account	รายชื่อผู้ใช้และรหัสผ่านในการใช้งานระบบสารสนเทศของมหาวิทยาลัย
โปรแกรมประเภทยูทิลิตี้	Use of system utilities	เป็นโปรแกรมประเภทหนึ่งที่ทำงานบนระบบปฏิบัติการ คุณสมบัติการใช้งานนั้นค่อนข้างหลากหลาย ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์ ช่วยสนับสนุน เพิ่ม หรือขยายขีดความสามารถของโปรแกรมที่ใช้งานให้มีประสิทธิภาพมากขึ้น เช่น WinRAR, AutoClicker, Auto Keyboard Presser, CPU-Z เป็นต้น
โปรแกรมประยุกต์ หรือ โปรแกรมคอมพิวเตอร์	Application / Software	โปรแกรมที่ทำให้เครื่องคอมพิวเตอร์ หรือเครื่องโทรศัพท์ทำงานเฉพาะอย่างตามความต้องการของผู้ใช้ เช่น ระบบบริหารงานบุคคล, ระบบ E-Phis, ระบบบริการการศึกษา, Browser Internet, Line, Facebook เป็นต้น
โปรแกรมประสงค์ร้าย	Malware	โปรแกรมประสงค์ร้ายที่ถูกสร้างขึ้นมา เช่น เพื่อโจมตีระบบโดยเฉพาะ, ทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล ไม่ว่าจะใช้วิธีการทำงานแบบไหนก็ตาม ทั้งหมดนี้สามารถเรียกได้ว่าเป็นมัลแวร์
ผู้ควบคุมข้อมูล	Data Controller	มหาวิทยาลัย หรือบุคคล หรือคณะกรรมการ หรือส่วนงาน หรือหน่วยงานที่มหาวิทยาลัยแต่งตั้งให้เป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล
ผู้ใช้งาน	User	พนักงานมหาวิทยาลัย ข้าราชการ ลูกจ้าง นักศึกษา และพนักงานราชการ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของส่วนงานหรือหน่วยงาน
ผู้ใช้งานภายนอก	External Users	ผู้ที่มีส่วนได้ส่วนเสียกับมหาวิทยาลัย เช่น คู่สัญญา ผู้สมัครสอบพนักงานมหาวิทยาลัย ผู้สมัครเข้าศึกษา ศิษย์เก่า ประชาชนทั่วไป ผู้ป่วย เป็นต้น
ผู้ดูแลระบบ	System Administrator	ผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนงานหรือหัวหน้าหน่วยงานให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่าย หรือระบบสารสนเทศไม่ว่าส่วนหนึ่งส่วนใด
ผู้บริหารระดับต้น หรือหัวหน้าหน่วยงาน		ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ หัวหน้าภาค/หัวหน้าฝ่าย/หัวหน้างาน หรือหน่วยงานที่มีฐานะเทียบเท่า เป็นต้น

คำนิยาม		คำอธิบาย
ผู้บริหารระดับสูง หรือหัวหน้าส่วนงาน		รองอธิการบดี หรือผู้มีอำนาจในการบังคับบัญชาในส่วนงานหรือหน่วยงาน ได้แก่ คณะบดี ผู้อำนวยการหรือเทียบเท่าเป็นต้น
ผู้บริหารระดับสูงสุด		อธิการบดีหรือเทียบเท่า
ผู้ประมวลผลข้อมูล	Data Processer	บุคคลธรรมดาหรือนิติบุคคล ซึ่งประมวลผลข้อมูลแทน “ผู้ควบคุมข้อมูล” (Data Controller)
แผนผังระบบเครือข่าย	Network Diagram	แผนผังหรือแผนภาพที่แสดงรูปแบบการจัดวางอุปกรณ์เครือข่ายในระบบเครือข่ายที่แสดงการเชื่อมโยง เพื่อให้เห็นเส้นทางการไหลเวียนของข้อมูลในเครือข่าย
ไฟร์วอลล์	Firewall	เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้า มาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย
มหาวิทยาลัย	University	หมายถึง มหาวิทยาลัยนวมินทราธิราช
มาตรการรักษาความมั่นคงปลอดภัย	Security measures	วิธีที่จัดตั้งขึ้นใช้เป็น กฎ ระเบียบ หรือกฎหมาย เพื่อทำให้มั่นใจว่ามีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ
รหัสผ่าน	Password	กลุ่มตัวอักษรหรือตัวเลขหรืออักขระที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยัน ตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล สารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย
ระบบคอมพิวเตอร์	Computer System	ขั้นตอนการปฏิบัติงานของคอมพิวเตอร์ที่มีการกำหนดอย่างชัดเจนว่าต้องทำอะไรบ้าง เพื่อให้ได้ผลออกมาตามที่ต้องการ ขั้นตอนการปฏิบัติงานจะประกอบด้วย ข้อมูลนำเข้า การประมวลผล ผลลัพธ์ และข้อมูลป้อนกลับ ซึ่งมีความสัมพันธ์เชื่อมโยงกัน
ระบบเครือข่ายไร้สาย	Wireless Lan	เทคโนโลยีในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ ๒ เครื่อง หรือกลุ่มของเครื่องคอมพิวเตอร์ รวมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายคอมพิวเตอร์ ซึ่งการสื่อสารจะไม่ใช้สายสัญญาณในการเชื่อมต่อ (LAN) แต่จะใช้คลื่นวิทยุ หรือ คลื่น อินฟาเรด ในการรับส่งข้อมูลแทน ตัวอย่างเช่น สัญญาณ WIFI เป็นต้น

คำนิยาม		คำอธิบาย
ระบบเครือข่ายสาธารณะ	Public Network	เป็นเครือข่ายครอบคลุมพื้นที่บริเวณกว้าง ที่ไม่ใช่ระบบเครือข่ายภายในมหาวิทยาลัย เช่น เครือข่ายอินเทอร์เน็ต เป็นต้น
ระบบฐานข้อมูล	Database System	ระบบที่รวบรวมข้อมูลต่าง ๆ ที่เกี่ยวข้องกันเข้าไว้ด้วยกันอย่างมีระบบ มีความสัมพันธ์ระหว่างข้อมูลต่าง ๆ ที่ชัดเจน ในระบบฐานข้อมูลจะประกอบด้วยแฟ้มข้อมูลหลายแฟ้มที่มีข้อมูลเกี่ยวข้องสัมพันธ์กันเข้าไว้ด้วยกันอย่างเป็นระบบ
ระบบเทคโนโลยีสารสนเทศ	Information system	ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ ระบบคอมพิวเตอร์ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้งานระบบ พนักงานที่เกี่ยวข้อง และ ผู้เชี่ยวชาญในสาขา ทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อ สร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งานเพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม
ระบบสารสนเทศ	information system	ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ ระบบคอมพิวเตอร์ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้งานระบบ พนักงานที่เกี่ยวข้อง และ ผู้เชี่ยวชาญในสาขา ทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อ สร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งานเพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม
ระบบสำรอง	disaster recovery site : DR site	ระบบคอมพิวเตอร์สำรองซึ่งประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่จำเป็นที่สามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา
ลงบันทึกเข้าใช้งาน	Login	กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้ระบบคอมพิวเตอร์หรือระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้งาน และรหัสผ่านให้ถูกต้อง
ลงบันทึกออก	Logout	กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์หรือ ระบบเครือข่าย
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด		สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงาน ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

คำนิยาม		คำอธิบาย
ส่วนงาน	Division	คณะ วิทยาลัย สำนักงาน หรือส่วนงานที่มีฐานะเทียบเท่าที่อยู่ในสังกัดมหาวิทยาลัยนวมินทราธิราช
สิทธิ์ของผู้ใช้งาน หรือสิทธิ์การใช้งาน	User rights	สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของส่วนงานหรือหน่วยงาน โดยส่วนงานหรือหน่วยงานจะเป็นผู้พิจารณาสิทธิ์ ในการเข้าถึงข้อมูลส่วนบุคคล หรือการใช้งานสินทรัพย์นั้น ๆ
สินทรัพย์	Asset lists	ข้อมูล ระบบฐานข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย อาทิเช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
สื่อบันทึกข้อมูล	Storage media	สื่อทั้งที่เป็นอิเล็กทรอนิกส์และไม่เป็นอิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD, DVD, Flash Drive, Handy Drive, Thumb Drive, Hard Drive, Portable Hard Drive, โทรศัพท์มือถือ กล้องถ่ายรูปดิจิตอล กล้องวิดีโอ หรือเครื่องบันทึกเสียง เป็นต้น
สื่อสังคมออนไลน์	Social Media	สังคมออนไลน์ที่ผู้ใช้สามารถสื่อสารกันผ่านการ พูดคุย แชร์เรื่องราวต่าง ๆ ได้ แต่ถ้าจะให้อธิบายแบบให้เห็นภาพง่ายที่สุดก็คือแพลตฟอร์มใด ๆ ก็ตามที่ให้คุณสามารถ แชร์ คอมเมนต์ พูดคุยหรือแสดงความคิดเห็นระหว่างคุณกับคนอื่น ๆ ได้ เพราะนั่นคือการเชื่อมโยงทุกคนเข้าหากันโดยมีสื่อกลางเป็น “อินเทอร์เน็ต” นั่นเอง
หน่วยงาน	Agency	งาน ศูนย์ ภาควิชา ฝ่าย หรือหน่วยงานที่มีฐานะเทียบเท่า ที่อยู่ในสังกัดแต่ละส่วนงาน
หมายเลขไอพีแอดเดรส	IP address	ตัวเลขประจำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่เชื่อมต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)
ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย	Computer and network control room	สถานที่ใช้สำหรับติดตั้งเครื่อง คอมพิวเตอร์/หรืออุปกรณ์บริหารจัดการเครือข่าย

คำนิยาม		คำอธิบาย
เหตุการณ์ด้านความมั่นคงปลอดภัย	Security incidents	การเกิดเหตุการณ์ สภาพของบริการ หรือ เครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
อัพเดท	Update	ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่าง ๆ ของระบบสารสนเทศให้ทันสมัยอยู่เสมอ
อินเทอร์เน็ต	Internet	เครือข่ายของคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายทั่วโลกเข้าด้วยกัน โดยอาศัยเครือข่ายโทรคมนาคมเป็นตัวเชื่อมโยง
อุปกรณ์กระจายสัญญาณข้อมูล	Switch	อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายแบบสาย LAN
อุปกรณ์กระจายสัญญาณแบบไร้สาย	Access Point	อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายแบบไร้สาย
อุปกรณ์จัดเส้นทาง	router	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทาง และค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น
อุปกรณ์สื่อสารพกพา	Portable communication device	อุปกรณ์พกพา ได้แก่ เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smartphone) แท็บเล็ต (Tablet) เป็นต้น
โฮสต์	Host	เครื่องคอมพิวเตอร์ที่สามารถเข้าถึงแบบสองทาง (two way access) ที่ไปยังเครื่องคอมพิวเตอร์อื่นในอินเทอร์เน็ต host มีการเจาะจงด้วยหมายเลขของ local หรือ host พร้อมกับหมายเลขของเครือข่ายในรูปของ IP address แบบไม่ซ้ำ ถ้าใช้การติดต่อโปรโตคอลแบบ point-to-point ไปยังผู้ให้บริการเครื่องคอมพิวเตอร์นั้นจะมี IP address แบบไม่ซ้ำ ตลอดช่วงการติดต่อในครั้งนั้นกับอินเทอร์เน็ต ทำให้เครื่องคอมพิวเตอร์เครื่องดังกล่าวมีฐานะเป็น host ในระยะเวลานั้น ดังนั้น host จึงเป็น node ในเครือข่าย

การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยด้านสารสนเทศ

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจของมหาวิทยาลัยนวมินทราธิราช

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑. ผู้ดูแลระบบ คือ ผู้ที่ได้รับการแต่งตั้งให้ดูแลระบบต่าง ๆ ของส่วนงาน หรือมหาวิทยาลัยนวมินทราธิราช ซึ่งแต่งตั้งโดยผู้บริหารระดับต้นขึ้นไป

ข้อ ๒. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากหน่วยงาน หรือส่วนงาน หรือมหาวิทยาลัย ตามความจำเป็นต่อการใช้งานของแต่ละผู้ใช้งาน (User) เท่านั้น

ข้อ ๓. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของส่วนงาน หรือมหาวิทยาลัย จะต้องขออนุญาตเป็นลายลักษณ์อักษรหรือทางระบบเอกสารอิเล็กทรอนิกส์ หรือระบบอื่นใดตามที่แต่ละส่วนงาน หรือมหาวิทยาลัยกำหนด

ข้อ ๔. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบฐานข้อมูลให้สัมพันธ์กับการเข้าใช้งานของผู้ใช้งาน (User) และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ หรือกำหนดสิทธิ์การเข้าใช้งานตามที่ผู้ขอเข้าถึงระบบเทคโนโลยีสารสนเทศได้รับการอนุญาตจากผู้มีอำนาจตามส่วนที่ ๑ ข้อ ๒ เท่านั้น รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบเทคโนโลยีสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

(๑.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข/เปลี่ยนแปลง
- อนุมัติ
- ไม่มีสิทธิ์

(๑.๒) กำหนดเกณฑ์การระงับสิทธิ์ มอบสิทธิ์ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศของผู้ใช้งาน (User Access Management)

(๑.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของส่วนงาน หรือมหาวิทยาลัยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหน่วยงานหรือส่วนงานหรือผู้ที่ส่วนงาน

มอบอำนาจให้ดำเนินการแทน หรือผู้ดูแลระบบที่ได้รับมอบหมายให้มีสิทธิในการอนุญาตการใช้งานระบบสารสนเทศนั้น ๆ ได้

ข้อ ๕. ผู้ดูแลระบบ ต้องจัดทำหรือดำเนินการใด ๆ ให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของส่วนงาน หรือมหาวิทยาลัย และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ ๖. ผู้ดูแลระบบ ต้องจัดทำหรือดำเนินการใด ๆ ให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๗. ผู้ดูแลระบบ ต้องจัดทำหรือดำเนินการใด ๆ ให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงหรือควบคุมการใช้งานสารสนเทศของผู้ใช้งาน (User Access Management)

ข้อ ๘. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานในรูปแบบเอกสารหรือไฟล์อิเล็กทรอนิกส์ หรือระบบสารสนเทศ โดยการขอสิทธิ์การใช้งานนั้นต้องได้รับการรับรองตาม ส่วนที่ ๑ ข้อ ๒

(๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานก่อนการลงทะเบียน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบและการอนุญาตให้เข้าใช้งานระบบตามส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control) ข้อ ๒

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษร หรือสื่ออิเล็กทรอนิกส์ หรืออื่น ๆ ที่สามารถแจ้งให้แก่ผู้ใช้งานทราบได้ เพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๙. ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์ เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบตามส่วนที่ ๑ ข้อ ๒

ข้อ ๑๐. ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งานอย่างสม่ำเสมอ อย่างน้อยทุก ๆ ๙๐ วัน เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์การใช้งานในระบบเทคโนโลยีสารสนเทศแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับส่วนงานโดยแยกตามหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากส่วนงานหรือหน่วยงาน

(๔) การยกเลิกสิทธิ์การใช้งานเมื่อมีบุคลากรลาออกต้องดำเนินการภายใน ๓ วันหลังจากได้รับแจ้งจากส่วนงานหรือหน่วยงาน หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน ๗ วันหลังจากได้รับแจ้งจากส่วนงานหรือหน่วยงาน

ข้อ ๑๑. การบริหารจัดการรหัสผ่าน (Password)

(๑) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา

(๒) การส่งมอบรหัสผ่าน (Password) ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการส่งผ่านบุคคลอื่นที่ไม่ใช่ผู้ใช้งานนั้น ๆ

(๓) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

(๔) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๕) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง และไม่ควรแสดงบัญชีผู้ใช้งานของตนเองให้ผู้ใช้งานคนอื่นทราบ

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานใด ๆ ที่มีสิทธิ์การใช้งานสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากส่วนงานหรือหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์การใช้งานพิเศษที่ได้รับ ว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้าง และต้อง กำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๑๒. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทที่คณะกรรมการเกี่ยวกับการบริหารจัดการข้อมูล หรือคณะกรรมการเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลที่มหาวิทยาลัยแต่งตั้งในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงฐานข้อมูลโดยตรง (Database) และการเข้าถึงผ่านโปรแกรมประยุกต์ (Application) รวมถึงวิธีการทำลายข้อมูลแต่ละประเภท มีดังต่อไปนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงฐานข้อมูลโดยตรง (Database) และการเข้าถึงผ่านโปรแกรมประยุกต์ (Application)

(๒) กำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นประเภท

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN, AES หรือ XML Encryption เป็นต้น

(๕) กำหนดให้มีการเปลี่ยนรหัสผ่าน (Password) ทุก ๆ ๙๐ วัน

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน หรือส่วนงาน หรือมหาวิทยาลัย เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อน เป็นต้น

(๗) ผู้ดูแลระบบต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานตามส่วนที่ ๒ ข้อ ๑๐

ข้อ ๑๓. ระบบเทคโนโลยีสารสนเทศที่เชื่อมโยงกัน ให้หน่วยงาน หรือส่วนงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างส่วนงานหรือมหาวิทยาลัยนวมินทราธิราชกับหน่วยงานภายนอกที่มาขอเชื่อมโยงระบบเทคโนโลยีสารสนเทศ หรือข้อมูล ตามหมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล ส่วนที่ ๑ ข้อ ๗

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๔. การใช้งานบัญชีผู้ใช้งาน (User Account) ผู้ใช้งานต้องปฏิบัติ ดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้งาน ซึ่งประกอบด้วยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีผู้ใช้งานของตนเองห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้บัญชีผู้ใช้งาน (User Account) โดยเด็ดขาด

(๒) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกจากผู้ดูแลระบบ ต้องเปลี่ยนรหัสผ่านใหม่ทันที เพื่อให้เป็นความลับเฉพาะตัว ในกรณีที่รหัสผ่านถูกเปิดเผยแล้ว ผู้ใช้งานจะต้องทำการเปลี่ยนรหัสผ่านใหม่ทันที

(๓) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character) หรือตามความสามารถสูงสุดของระบบที่รับได้ เช่น ๐๑Chutipon$

(๔) ไม่กำหนดรหัสผ่าน จากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือคำศัพท์ที่ปรากฏในพจนานุกรม

(๕) ไม่ใช้รหัสผ่าน สำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๖) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านแบบอัตโนมัติ (save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๗) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๙๐ วัน หรือทุกครั้งที่มีการ แจ้งเตือนให้เปลี่ยนรหัสผ่าน

(๙) ห้ามนำรหัสผ่านเก่ากลับมาใช้ใหม่ ป้องกันการจดจำรหัสผ่านเก่าหรือการล่วงรู้รหัสผ่านเก่า

(๑๐) หากผู้ใช้งานพบเหตุที่สงสัยว่าถูกผู้อื่นนำรหัสผ่านไปใช้ ให้ดำเนินการเปลี่ยนรหัสผ่าน และแจ้งผู้ดูแลระบบในทันที

ข้อ ๑๕. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีผู้ใช้งาน (Username) ของผู้ใช้งาน อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๑๖. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบเทคโนโลยีสารสนเทศของส่วนงานหรือมหาวิทยาลัย และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อก หรือเกิดจากความผิดพลาดใด ๆ ที่ทำให้ไม่สามารถดำเนินการได้ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที และในการใช้งานผู้ใช้งานต้องปฏิบัติตามแนวทาง ดังนี้

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งการใช้งานจะถูกบันทึกข้อมูลจราจรทางคอมพิวเตอร์

(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที

ข้อ ๑๗. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมคอมพิวเตอร์ประเภท Peer-to-Peer หรือ โปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหน่วยงาน หรือส่วนงาน หรือมหาวิทยาลัย ทั้งนี้หากได้รับอนุญาตต้องแจ้งให้ผู้ดูแลระบบทราบ และการติดตั้งต้องดำเนินการติดตั้งโดยผู้ดูแลระบบเท่านั้น

ข้อ ๑๘. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกม เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๑๙. ห้ามใช้สินทรัพย์ของส่วนงาน หรือมหาวิทยาลัย ที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของมหาวิทยาลัย

ข้อ ๒๐. ห้ามใช้สินทรัพย์ของส่วนงาน หรือมหาวิทยาลัย เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของมหาวิทยาลัย

ข้อ ๒๑. ห้ามใช้สินทรัพย์ของมหาวิทยาลัย เพื่อประโยชน์ทางการค้า หรือประโยชน์ส่วนตน

ข้อ ๒๒. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของ ส่วนงานหรือมหาวิทยาลัยโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๒๓. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของส่วนงาน หรือมหาวิทยาลัยต้องหยุดชะงัก

ข้อ ๒๔. ห้ามใช้ระบบสารสนเทศของส่วนงานหรือมหาวิทยาลัย เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหน่วยงาน หรือส่วนงานและผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๒๕. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้บัญชีผู้ใช้งานของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๒๖. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยไม่ได้รับอนุญาตจากหน่วยงาน หรือส่วนงาน และผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๒๗. บุคลากรทุกคนที่มีการกระทำที่ละเมิดกฎหมาย เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ หรือ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และ พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือละเมิดประกาศ ระเบียบ คำสั่ง ด้านความปลอดภัยด้านสารสนเทศของส่วนงานหรือมหาวิทยาลัย โดยข้อเท็จจริงของการกระทำที่ส่อเจตนาในทางที่ไม่เหมาะสมให้ถือเป็นความผิดทางวินัย

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๒๘. ผู้ใช้งานต้องไม่เข้าไปในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๒๙. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๐. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมต่อเข้าเครือข่ายเพื่อการประกอบธุรกิจ ส่วนบุคคล

ข้อ ๓๑. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๓๒. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์ตรวจ แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้ เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์ หรืออุปกรณ์ลักษณะที่ทำงานคล้ายกัน	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อ ๓๓. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่ส่วนงาน หรือมหาวิทยาลัยมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ ที่หน่วยงานหรือส่วนงานมอบหมาย

ข้อ ๓๔. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของส่วนงานหรือมหาวิทยาลัยที่ได้รับมอบไว้ให้ใช้งาน

ข้อ ๓๕. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๓๖. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์ตั้งโต๊ะ หรือคอมพิวเตอร์พกพา และอุปกรณ์สื่อสารพกพา ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงาน หรือส่วนงาน แต่การยืมนั้นให้คำนึงถึงเหตุการณ์ข้อมูลหรือข้อมูลส่วนบุคคลรั่วไหล และต้องไม่เป็นการขัดต่อนโยบายฉบับนี้ด้วย

ข้อ ๓๗. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่ส่วนงานหรือมหาวิทยาลัยจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของส่วนงานหรือมหาวิทยาลัยเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบเทคโนโลยีสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่ส่วนงานหรือมหาวิทยาลัยไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อมหาวิทยาลัย

ข้อ ๓๘. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๔๒ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๓๙. มาตรการควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่"

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่ " ให้ถูกต้องชัดเจน

(๓) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกแบบฟอร์มการขออนุญาตเข้า-ออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ ๔๐. ผู้ใช้งานที่จะนำเครื่องคอมพิวเตอร์หรืออุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ หรือระบบเครือข่ายของส่วนงานหรือมหาวิทยาลัย ต้องได้รับอนุญาตจากส่วนงานหรือมหาวิทยาลัยก่อน และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม "การขอเชื่อมต่อเครือข่าย" โดยผ่านการพิสูจน์ตัวตนการใช้งาน Internet ของส่วนงานหรือมหาวิทยาลัย

ข้อ ๔๑. การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่ส่วนงานหรือมหาวิทยาลัยรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อส่วนงานหรือมหาวิทยาลัย และผู้ขออนุญาตจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

ข้อ ๔๒. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักหรืออุปกรณ์อื่นใดในระบบเครือข่ายทั้งหมด โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๓. ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้ อย่างมีประสิทธิ์ภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของส่วนงานหรือมหาวิทยาลัย ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกส่วนงานหรือมหาวิทยาลัย ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของส่วนงานหรือมหาวิทยาลัยในลักษณะที่ผิดปกติ

(๖) การเข้าสู่ระบบเครือข่ายภายในส่วนงานหรือมหาวิทยาลัย โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการ พิสูจน์ตัวตน(Authentication) ด้วยการใช้

รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง หรือสามารถดำเนินการในรูปแบบอื่นที่สามารถพิสูจน์ตัวตนได้

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP address ภายในของระบบเครือข่ายภายในของส่วนงานหรือมหาวิทยาลัย

(๘) ผู้ดูแลระบบต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การระบุอุปกรณ์บนเครือข่าย ผู้ดูแลระบบต้องมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP address และสถานที่ติดตั้ง ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP address ของทั้งต้นทางและปลายทางได้ ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” โดยผ่านระบบ การพิสูจน์ตัวตนการใช้งาน Intranet ของส่วนงานหรือมหาวิทยาลัยหรือช่องทางอื่นตามที่ส่วนงานหรือมหาวิทยาลัยหรือผู้ดูแลระบบกำหนด ทั้งนี้ต้องเป็นไปตามแนวทางที่สอดคล้องตามประกาศนี้ การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ ๔๔. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๔๕. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

ข้อ ๔๖. กำหนดให้มีการจัดเก็บซอร์สโค้ดไลบรารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๔๗. ดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ

ข้อ ๔๘. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกส่วนงานหรือมหาวิทยาลัย เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของส่วนงาน หรือมหาวิทยาลัย จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากส่วนงาน หรือมหาวิทยาลัย

(๒) ผู้ดูแลระบบ ต้องมีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๓) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบฐานข้อมูลได้จากระยะไกลต้องได้รับการ อนุญาตจากส่วนงานหรือมหาวิทยาลัยก่อน และผู้ดูแลระบบก่อน

(๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับส่วนงานหรือมหาวิทยาลัยอย่างเพียงพอ

(๕) การเข้าสู่ระบบเครือข่ายภายใน และระบบเทคโนโลยีสารสนเทศสารสนเทศในส่วนงานหรือมหาวิทยาลัยจากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๔๙. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามกลุ่มผู้ใช้งาน เช่น การแยก SSID ระหว่างผู้ใช้งานภายในมหาวิทยาลัย และผู้ใช้งานภายนอกมหาวิทยาลัย เป็นต้น เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ ๕๐. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ผู้ดูแลระบบ ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๕๑. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกส่วนงานหรือมหาวิทยาลัย ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ ๕๒. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของส่วนงาน หรือมหาวิทยาลัย ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ ๕๓. IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของ ระบบเครือข่ายได้โดยง่าย

ข้อ ๕๔. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ข้อ ๕๕. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามส่วนที่ ๒ ข้อ ๙) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามส่วนที่ ๒ ข้อ ๑๐) เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๕๖. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหน่วยงาน หรือส่วนงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๕๗. ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ ๕๘. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานให้กับผู้ใช้งานที่ได้รับอนุญาตให้ใช้งานได้เท่านั้น ตามส่วนที่ ๑ ข้อ ๒

ข้อ ๕๙. ผู้ดูแลระบบ ต้องมีการบริหารจัดการรหัสผ่าน (Password) การเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นให้เป็นไปตาม ส่วนที่ ๒ ข้อ ๑๑

ข้อ ๖๐. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศตามประเภทของข้อมูลในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท และการเข้าถึงฐานข้อมูลโดยตรง (Database) และการเข้าถึงผ่านโปรแกรมประยุกต์ (Application) รวมถึงวิธีการทำลายข้อมูลแต่ละประเภท โดยให้ปฏิบัติตามส่วนที่ ๒ ข้อ ๑๒

ข้อ ๖๑. ผู้ดูแลระบบต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานทุก ๙๐ วัน โดยแนวทางการดำเนินการให้ปฏิบัติตามส่วนที่ ๒ ข้อ ๑๐

ส่วนที่ ๗ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malware)

ข้อ ๖๒. มหาวิทยาลัยได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่ส่วนงาน หรือมหาวิทยาลัย อนุญาตให้ใช้งานหรือที่ส่วนงาน หรือมหาวิทยาลัยมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งและถอดถอนซอฟต์แวร์ หรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว เว้นแต่ การใช้ซอฟต์แวร์ในงานด้านปฏิบัติการงานวิจัย หรืองานเฉพาะทางที่หน่วยงานได้จัดหาไว้ใช้เอง หากกรณีหน่วยงานใดมีความจำเป็นต้องใช้ซอฟต์แวร์ในการทำงานนอกเหนือจากที่หน่วยงาน หรือส่วนงาน หรือมหาวิทยาลัย กำหนดให้ดำเนินการขอความเห็นชอบจาก “ผู้บริหารกลุ่มงานเทคโนโลยีสารสนเทศ” ของส่วนงานหรือมหาวิทยาลัย

ข้อ ๖๓. ซอฟต์แวร์ (Software) ที่ส่วนงาน หรือมหาวิทยาลัยได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากส่วนงานหรือมหาวิทยาลัย หรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ ๖๔. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่น ต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๖๕. ผู้ดูแลระบบต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๖๖. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบทันที

ข้อ ๖๗. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบทันที

ข้อ ๖๘. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของส่วนงาน หรือมหาวิทยาลัย หรือของผู้อื่น หรือข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาต

ข้อ ๖๙. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิด

ความเสียหายมาสู่สินทรัพย์ของส่วนงาน หรือมหาวิทยาลัย สิทธิ์ที่จะพัฒนาโปรแกรม หรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลส่วนบุคคลของบุคคลอื่น หรือข้อมูลของบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๗๐. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของ ซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอกส่วนงาน หรือมหาวิทยาลัยต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

ส่วนที่ ๘ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๗๑. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของส่วนงาน หรือมหาวิทยาลัยจากระยะไกล มีการป้องกันไวรัสและการใช้งานเครือข่ายตามที่ส่วนงาน หรือมหาวิทยาลัยกำหนด

ข้อ ๗๒. เพื่อเพิ่มความปลอดภัยในการปฏิบัติงานจากภายนอกสำนักงาน จะต้องมีการเข้ารหัสที่มีความมั่นคงปลอดภัยหรือตามมาตรฐานสากล เช่น SSL VPN เป็นต้น

ข้อ ๗๓. ผู้ใช้งานที่ประสงค์จะปฏิบัติงานจากระยะไกลทุกคนต้องลงทะเบียนการใช้งานตามขั้นตอนที่ส่วนงานหรือมหาวิทยาลัยกำหนด โดยการปฏิบัติงานจากภายนอกสำนักงานนั้น ต้องผ่านการพิสูจน์ตัวตน และหน่วยงานส่วนงานหรือมหาวิทยาลัยมีสิทธิที่จะระงับการปฏิบัติงานจากภายนอกสำนักงาน หากมีเหตุสงสัยว่าคอมพิวเตอร์นั้นไม่ปลอดภัยต่อเครือข่าย

ข้อ ๗๔. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัว เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของส่วนงานหรือมหาวิทยาลัยจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของส่วนงาน และมหาวิทยาลัย

ข้อ ๗๕. ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ประเภทของข้อมูลที่ใช้ ระบบงานและบริการต่าง ๆ ของหน่วยงาน หรือส่วนงาน หรือมหาวิทยาลัย ที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล หากอนุญาตให้ปฏิบัติงานจากระยะไกล ต้องกำหนดวิธีการเข้าใช้งานที่มีความปลอดภัย

ข้อ ๗๖. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๙ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan Access Control)

ข้อ ๗๗. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๗๘. ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันที ที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน

ข้อ ๗๙. ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless Lan Client และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)

ข้อ ๘๐. ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น ให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๘๑. ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในส่วนงาน หรือมหาวิทยาลัย

ข้อ ๘๒. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข้อ ๘๓. ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบให้หัวหน้าหน่วยงานทราบทุก ๙๐ วัน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ ๘๔. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตให้ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของส่วนงาน หรือมหาวิทยาลัย

ข้อ ๘๕. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัย จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับอนุญาตให้ใช้งานระบบตามส่วนที่ ๑ ข้อ ๒

ข้อ ๘๖. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ตามส่วนที่ ๒ ข้อ ๘ และส่วนที่ ๒ ข้อ ๑๐

ส่วนที่ ๑๐ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๘๗. ผู้ดูแลระบบ มีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

ข้อ ๘๘. การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๘๙. ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall

ข้อ ๙๐. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall .ในทุกกรณี

ข้อ ๙๑. การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบหรือผู้ดูแลและจัดการที่ได้รับแต่งตั้งเท่านั้น

ข้อ ๙๒. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์หรือซอฟต์แวร์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๙๓. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน ผู้ดูแลระบบจะต้องทำตารางรายการพอร์ตพื้นฐานที่อนุญาตให้เชื่อมต่อ ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความเห็นชอบจากหน่วยงาน ส่วนงาน หรือมหาวิทยาลัย และผู้ดูแลระบบก่อน

ข้อ ๙๔. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

ข้อ ๙๕. ผู้ดูแลระบบจะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ Firewall เป็นประจำทุกสัปดาห์หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๙๖. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบเทคโนโลยีสารสนเทศต่าง ๆ ภายในส่วนงานหรือมหาวิทยาลัย ที่มีลักษณะที่เป็นอินทราเน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๙๗. ผู้ดูแลระบบ มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๙๘. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานของผู้ดูแลระบบก่อน

ข้อ ๙๙. ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ส่วนที่ ๑๑ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-mail)

ข้อ ๑๐๐. ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) โดยยื่นคำขอกับเจ้าหน้าที่หน่วยงานที่ได้รับมอบหมายให้รับผิดชอบในการบริหารจัดการ E-mail

ข้อ ๑๐๑. รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

ข้อ ๑๐๒. เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้เปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๑๐๓. ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน ๓ ครั้ง

ข้อ ๑๐๔. ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๑๐๕. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๙๐ วัน

ข้อ ๑๐๖. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานนั้น และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-mail) ของตน

ข้อ ๑๐๗. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๑๐๘. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล E-mail ที่ส่วนงานหรือมหาวิทยาลัยกำหนดไว้ ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-mail ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๑๐๙. ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๑๑๐. ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๑๑๑. ห้ามส่ง E-mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิ์ของบุคคลอื่น

ข้อ ๑๑๒. ห้ามส่ง E-mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๑๓. ให้ระบุชื่อของผู้ส่งใน E-mail ทุกฉบับที่ส่งไป

ข้อ ๑๑๔. ให้ทำการสำรองข้อมูล E-mail ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ ๑๑๕. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com, .bat เป็นต้น

ข้อ ๑๑๖. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๑๗. ผู้ใช้งานไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของส่วนงานหรือมหาวิทยาลัย หรือทำให้เกิดความแตกแยกระหว่างหน่วยงานหรือส่วนงาน ผ่านทางจดหมายอิเล็กทรอนิกส์ และควรระบุชื่อของผู้ส่ง ตำแหน่ง และข้อมูลติดต่อกลับไว้ในจดหมายอิเล็กทรอนิกส์ทุกฉบับ

ข้อ ๑๑๘. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองอย่างสม่ำเสมอ และใช้ความระมัดระวังและตรวจสอบจดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งข้อมูลสำคัญผิดตัวผู้รับทำให้ข้อมูลรั่วไหล

ข้อ ๑๑๙. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือ จดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ ๑๒๐. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ ที่ส่วนงานหรือมหาวิทยาลัยจัดสรรให้เท่านั้น ในการติดต่อสื่อสารทั้งภายในและภายนอกมหาวิทยาลัย ตามหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย

ข้อ ๑๒๑. ห้ามนำจดหมายอิเล็กทรอนิกส์ของส่วนงาน หรือมหาวิทยาลัย ไปลงทะเบียนตามที่อยู่เว็บไซต์ต่าง ๆ ที่ไม่มีความเกี่ยวข้องกับภารกิจงานของตนเอง

ข้อ ๑๒๒. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย ทรัพย์สินทางปัญญาหรือสิทธิของบุคคลอื่น

ข้อ ๑๒๓. ห้ามส่งอีเมล์ที่มีโปรแกรมไม่ประสงค์ดีไปให้กับผู้อื่นโดยเจตนา

ข้อ ๑๒๔. ต้องไม่ใช้จดหมายอิเล็กทรอนิกส์ของส่วนงาน หรือมหาวิทยาลัยในทางที่ละเมิดต่อกฎหมาย หรือโดยเจตนาทำให้มหาวิทยาลัยหรือส่วนงานได้รับความเสียหายอย่างร้ายแรง

ส่วนที่ ๑๒ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ ๑๒๕. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ส่วนงานหรือมหาวิทยาลัยจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่มีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าส่วนงานเป็นลายลักษณ์อักษร และได้รับการดำเนินการจากผู้ดูแลระบบที่ได้รับมอบหมายก่อน

ข้อ ๑๒๖. เครื่องคอมพิวเตอร์ตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์สื่อสารพกพาก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บบราวเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ ๑๒๗. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๑๒๘. ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของส่วนงานหรือมหาวิทยาลัย เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์หรือสื่อสังคมออนไลน์ที่มีเนื้อหาที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์หรือสื่อสังคมออนไลน์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์หรือสื่อสังคมออนไลน์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลจากแหล่งใดก็ตาม ๆ ที่อาจก่อให้เกิดความเสียหายให้กับส่วนงานหรือมหาวิทยาลัย หรือแสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจ

ข้อ ๑๒๙. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของส่วนงานหรือมหาวิทยาลัย ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๑๓๐. ระมัดระวังการดาวน์โหลดโปรแกรมใช้งาน หรือข้อมูลหรือโปรแกรมจากระบบอินเทอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๓๑. ในการใช้งานเว็บไซต์หรือสื่อสังคมออนไลน์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของส่วนงาน หรือมหาวิทยาลัย และไม่เป็นช่องทางในการบุกรุกระบบของผู้อื่น

ข้อ ๑๓๒. ในการใช้งานเว็บไซต์หรือสื่อสังคมออนไลน์ ไม่เสนอความคิดเห็น หรือส่งต่อ หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของส่วนงานหรือมหาวิทยาลัย หรือการทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ หรือ เสนอความคิดเห็นที่ขัดต่อศีลธรรม หรือกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น

ข้อ ๑๓๓. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ ๑๓๔. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บบราวเซอร์และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๑๓๕. ห้ามผู้ใช้งาน เล่นเกม ดูภาพยนตร์ ฟังเพลง หรือเข้าไปสนทนาในห้องสนทนาบนเครือข่ายอินเทอร์เน็ตในเวลาทำงาน

ข้อ ๑๓๖. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๑๓ การควบคุมการเผยแพร่ข้อมูลเว็บไซต์ (Publish Website Information)

ข้อ ๑๓๗. การเผยแพร่ข้อมูลเว็บไซต์ของหน่วยงาน ส่วนงาน หรือมหาวิทยาลัย จะต้องผ่านการตรวจสอบจากผู้บังคับบัญชาที่รับผิดชอบงานประชาสัมพันธ์ที่ส่วนงานหรือมหาวิทยาลัยแต่งตั้ง และต้องได้รับการอนุมัติก่อนทุกครั้ง

ข้อ ๑๓๘. การเผยแพร่ข้อมูลเว็บไซต์ ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมาย

ข้อ ๑๓๙. ผู้รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่บนเว็บไซต์ จะต้องตรวจทานความถูกต้อง และสมบูรณ์ของข้อมูลก่อนจะนำขึ้นเผยแพร่ และแจ้งผู้ให้ข้อมูล หรือหน่วยงานเจ้าของเรื่องตรวจสอบเมื่อดำเนินการแล้วเสร็จ

ข้อ ๑๔๐. ผู้ให้ข้อมูล จะต้องตรวจสอบข้อมูลและปรับปรุงข้อมูลที่อยู่ในความรับผิดชอบให้เป็นปัจจุบันเสมอ พร้อมทั้งเสนอผู้บังคับบัญชาที่รับผิดชอบงานประชาสัมพันธ์ที่ส่วนงานหรือมหาวิทยาลัยแต่งตั้ง อนุมัติให้ก่อนเผยแพร่บนเว็บไซต์ของหน่วยงาน ส่วนงานหรือมหาวิทยาลัย

ข้อ ๑๔๑. เมื่อพบปัญหาอุปสรรคในการดำเนินงานเผยแพร่ข้อมูล หรือมีการแต่งตั้งโยกย้าย ปรับเปลี่ยนผู้รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่บนเว็บไซต์ จะต้องแจ้งผู้ดูแลเว็บไซต์ทราบโดยเร็ว เพื่อผู้ดูแลเว็บไซต์จะได้ดำเนินการในส่วนที่เกี่ยวข้อง และสรุปปัญหาอุปสรรคการดำเนินงานเผยแพร่ข้อมูลต่อสาธารณะบนเว็บไซต์ของหน่วยงาน ส่วนงาน หรือมหาวิทยาลัย

ข้อ ๑๔๒. ควรเลือกใช้คำอธิบาย/คำบรรยายเนื้อหาที่มีความถูกต้องและเหมาะสม และจะต้องไม่ละเมิดลิขสิทธิ์ หากจำเป็นต้องนำมาเผยแพร่ให้ระบุแหล่งที่มาของข้อมูลอ้างอิงแนบท้าย

ข้อ ๑๔๓. ข้อความและรูปภาพประกอบที่นำมาใช้จะต้องไม่ละเมิดลิขสิทธิ์

ข้อ ๑๔๔. หลังจากเผยแพร่ข้อมูลแล้วผู้รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่บนเว็บไซต์ ต้องเฝ้าระวังหน้าเว็บไซต์อย่างสม่ำเสมอ ตรวจสอบว่ามีการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาตเกิดขึ้นหรือไม่ หากพบความผิดปกติให้รีบแจ้งผู้ดูแลระบบเว็บไซต์ของหน่วยงาน หรือส่วนงาน หรือมหาวิทยาลัยทันที

ข้อ ๑๔๕. จะต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นใดที่เกี่ยวข้องอย่างเคร่งครัด เพื่อป้องกันไม่ให้เกิดความเสียหายและลดโอกาสที่จะเกิดความเสียหายแก่ส่วนงานและมหาวิทยาลัย

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา หรืออุปกรณ์สื่อสารพกพา และการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๑๔๖ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของส่วนงาน โดยปฏิบัติตาม (ส่วนที่ ๒ ข้อ ๙) ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานโดยปฏิบัติตาม (ส่วนที่ ๒ ข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๑๔๗. แนวทางปฏิบัติการใช้งานทั่วไปของผู้ใช้งาน

(๑) เครื่องคอมพิวเตอร์ทั้งแบบตั้งโต๊ะและพกพา หรืออุปกรณ์สื่อสารพกพาที่ส่วนงานหรือมหาวิทยาลัยอนุญาตให้ใช้งาน เป็นสินทรัพย์เพื่อใช้ในการปฏิบัติงานของส่วนงานหรือมหาวิทยาลัย

(๒) ผู้ใช้งานต้องกำหนดบัญชีผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

(๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของตนเองร่วมกัน

(๖) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(๗) โปรแกรมประยุกต์ หรือโปรแกรมคอมพิวเตอร์ หรือระบบปฏิบัติการ ที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ทั้งแบบตั้งโต๊ะและพกพา หรืออุปกรณ์สื่อสารพกพาของผู้ใช้งาน ต้องเป็นโปรแกรมที่แต่ละส่วนงานหรือมหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๘) ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งโปรแกรมประยุกต์ หรือโปรแกรมคอมพิวเตอร์ หรือระบบปฏิบัติการที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

(๙) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ ทั้งแบบตั้งโต๊ะและพกพาที่ส่วนงาน หรือมหาวิทยาลัยมอบไว้ให้ใช้ปฏิบัติงาน

(๑๐) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงเว้นแต่จะได้รับอนุญาตจากส่วนงาน หรือผู้ดูแลระบบ

(๑๑) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของส่วนงาน หรือมหาวิทยาลัย เพื่อประโยชน์ทางการค้าหรือประโยชน์ส่วนตน หรือเพื่อการอื่นใดที่ไม่เกี่ยวข้องกับงานตามภารกิจหรือหน้าที่ความรับผิดชอบ

(๑๒) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๑๓) ห้ามผู้ใช้งาน ควบคุมคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศจากภายนอกโดยไม่ได้รับอนุญาตจากหน่วยงาน หรือส่วนงาน หรือผู้ดูแลระบบ

(๑๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ทั้งแบบตั้งโต๊ะและพกพา หรืออุปกรณ์สื่อสารพกพาตรวจซ่อมจะต้องดำเนินการ โดยเจ้าหน้าที่ด้านสารสนเทศของส่วนงาน หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับส่วนงาน หรือมหาวิทยาลัย เท่านั้น

(๑๕) ก่อนการใช้งานสื่อบันทึกข้อมูลพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสที่ส่วนงาน หรือมหาวิทยาลัยติดตั้งให้

(๑๖) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ตั้งโต๊ะและพกพา และอุปกรณ์สื่อสารพกพา หากเกิดการชำรุด เสียหาย หรือสูญหายเมื่อสอบสวนแล้วพบว่าไม่ได้ใช้ความระมัดระวังและดูแลอย่างเพียงพอ ผู้ใช้งานต้องรับผิดชอบในการชำรุด เสียหาย หรือสูญหายนั้น

(๑๗) ปิดเครื่องคอมพิวเตอร์ตั้งโต๊ะและพกพาที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๑๘) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ตั้งโต๊ะและพกพาที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๕ นาที หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

(๑๙) ห้ามนำเครื่องคอมพิวเตอร์ตั้งโต๊ะและพกพาซึ่งเป็นของส่วนตัวของผู้ใช้งาน มาใช้กับระบบเครือข่ายของส่วนงาน เว้นแต่จะมีการนำมาลงทะเบียนการใช้งานเครือข่ายและได้รับอนุมัติจากหัวหน้าหน่วยงาน หรือหัวหน้าส่วนงาน หรือมหาวิทยาลัย ทั้งนี้ต้องใช้งานตามสิทธิที่ตนเองได้รับและปฏิบัติตามประกาศนี้อย่างเคร่งครัด

ข้อ ๑๔๘. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิด สามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๑) การใช้งานโปรแกรมยูทิลิตี้ ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน

(๒) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

(๔) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

(๕) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งผู้ดูแลระบบต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมประเภทยูทิลิตี้ได้

ข้อ ๑๔๙. แนวทางปฏิบัติเพิ่มเติมสำหรับคอมพิวเตอร์แบบพกพา

(๑) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่าง ปลอดภัยและมีประสิทธิ์ภาพ

(๒) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์พกพาและรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๓) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๔) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๕) ไม่วางของทับบนหน้าจอและแป้นพิมพ์ และการเก็บเครื่องคอมพิวเตอร์แบบพกพาไม่ควรนำสิ่งของใด ๆ สอดไว้ระหว่างแป้นพิมพ์และจอหากพับเก็บลักษณะดังกล่าวจะทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๖) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๗) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๘) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

(๙) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๑๐) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

(๑๑) หน่วยงาน ส่วนงาน หรือมหาวิทยาลัย มีสิทธิในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และแบบพกพา หรืออุปกรณ์สื่อสารพกพา ทั้งที่เป็นทรัพย์สินของหน่วยงานส่วนงาน หรือมหาวิทยาลัย และทรัพย์สินส่วนบุคคล

ข้อ ๑๕๐. การสร้างรหัสผ่านเครื่องคอมพิวเตอร์ตั้งโต๊ะ และพกพา ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุตามส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๕๑. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive, External Harddisk และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เช่น ไฟล์ที่มีนามสกุล .exe, .bat, .vbs .com เป็นต้น

(๔) ผู้ใช้งานต้องตรวจสอบข้อมูลในเครื่องคอมพิวเตอร์ที่ใช้งานด้วยโปรแกรมป้องกันไวรัส (ที่ติดตั้งในเครื่องนั้น) เพื่อกำจัดไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

ข้อ ๑๕๒. การสำรองข้อมูลและการกู้คืนเครื่องคอมพิวเตอร์แบบตั้งและพกพา

(๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อ (Backup media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลหรือข้อมูลส่วนบุคคลรั่วไหล

(๓) สื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๔) สื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลสำคัญเกี่ยวข้องกับการทำงาน ที่เก็บไว้ในคอมพิวเตอร์ไม่ควรเก็บข้อมูลไว้ที่เดียว เพราะหาก Hard Disk หรือข้อมูลเสียหายไป จะส่งผลกระทบต่อการดำเนินการของส่วนงานหรือมหาวิทยาลัย ดังนั้นไม่ควรเก็บข้อมูลสำคัญไว้ที่เดียว

ข้อ ๑๕๓. การยืม - คืน เครื่องคอมพิวเตอร์ทั้งแบบตั้งโต๊ะและพกพา หรืออุปกรณ์สื่อสารพกพา ต้องปฏิบัติดังต่อไปนี้

(๑) ผู้ใช้งานที่มีความจำเป็นต้องใช้งานอุปกรณ์พกพา หรืออุปกรณ์สื่อสารพกพา หรือสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ โดยอุปกรณ์นั้นเป็นทรัพย์สินของหน่วยงาน ส่วนงาน หรือมหาวิทยาลัย จะต้องมีการดำเนินการขออนุมัติเพื่อยืมอุปกรณ์และต้องได้รับการอนุมัติก่อนนำไปใช้งาน และต้องดำเนินการคืนอุปกรณ์เหล่านั้น เมื่อเสร็จสิ้นการใช้งาน

(๒) เจ้าหน้าที่ผู้รับผิดชอบในการควบคุมการยืม - คืน เครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ ต้องตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๓) ผู้ใช้งานต้องระมัดระวังไม่ให้บุคคลภายนอกหรือบุคคลอื่น คัดลอกข้อมูลจากคอมพิวเตอร์ที่ผู้ใช้งานยืมไปใช้ เว้นแต่ข้อมูลนั้นได้มีการเผยแพร่เป็นการทั่วไป

(๔) เมื่อหมดความจำเป็นต้องใช้คอมพิวเตอร์ และอุปกรณ์แล้ว หรือครบกำหนดระยะเวลาที่ยืมใช้ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๕) เจ้าหน้าที่ผู้รับผิดชอบในการควบคุมการยืม - คืน เครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์เมื่อรับคืนเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ ต้องตรวจสอบสภาพความพร้อมใช้งานของเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์นั้น ที่รับคืนด้วย

(๖) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทของผู้นำไปใช้ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๑๕ การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS)

ข้อ ๑๕๔. IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงานให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๑๕๕. IDS/IPS Policy ครอบคลุมทุก โฮสต์ (Host) ในเครือข่ายของส่วนงานและเครือข่ายข้อมูลทั้งมหาวิทยาลัย รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๑๕๖. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๑๕๗. ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการ ให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๑๕๘. โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๑๕๙. ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

ข้อ ๑๖๐. ต้องมีการตรวจสอบเหตุการณ์ข้อมูลจราจรทางคอมพิวเตอร์ พฤติกรรมการใช้งาน กิจกรรม และบันทึก ปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๑๖๑. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๑๖๒. เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๖๓. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบพฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้หัวหน้าหน่วยงานของผู้ดูแลระบบทราบทันทีที่ตรวจพบ

ข้อ ๑๖๔. พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบ จะต้องมีการรายงานให้หัวหน้าหน่วยงานของผู้ดูแลระบบทราบภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๖๕. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๖๖. ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๖๗. ผู้ดูแลระบบมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๖๘. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของส่วนงานหรือมหาวิทยาลัย การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของส่วนงานหรือมหาวิทยาลัย จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๖ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ ๑๖๙. การปรับปรุงระบบปฏิบัติการ (Operating System Update)

(๑) ผู้ดูแลระบบ ต้องตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบอย่างสม่ำเสมอ

(๒) ผู้ดูแลระบบ ต้องติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) ผู้ดูแลระบบ ต้องกำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)

(๔) ผู้ดูแลระบบ ต้องกำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name) / IP address

(๕) ผู้ดูแลระบบ ต้องปรับปรุง หรือกำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)

(๖) ติดตั้งโปรแกรม Antivirus หรือปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

ข้อ ๑๗๐. การบริหารบัญชีผู้ใช้งาน สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)

(๑) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)

(๒) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิ์การเข้าใช้ระบบ

ข้อ ๑๗๑. การปรับปรุงการรักษาความปลอดภัยหรือ Antivirus (System Security & Antivirus Update)

(๑) ผู้ดูแลระบบ ต้องติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ

(๒) ผู้ดูแลระบบ ต้องตรวจสอบ Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

(๓) ผู้ดูแลระบบ ต้องปรับปรุง หรือกำหนดค่าระบบความปลอดภัยให้เหมาะสมกับปัญหา

(๔) ผู้ดูแลระบบ ต้องปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(๕) ผู้ดูแลระบบ ต้องดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์เป็นประจำ

ข้อ ๑๗๒. ติดตั้ง หรือปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

(๑) ผู้ดูแลระบบ ต้องติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่ส่วนงาน หรือมหาวิทยาลัยใช้งาน

(๒) ผู้ดูแลระบบ ต้องกำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง และมีประสิทธิภาพตามระบบฐานข้อมูลนั้นกำหนด

(๓) ผู้ดูแลระบบ ต้องสร้าง และ กำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่นและสิทธิ์การใช้

(๔) ผู้ดูแลระบบ ต้องปรับปรุง หรือกำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

ข้อ ๑๗๓. ผู้ดูแลระบบ ต้องติดตั้งฐานข้อมูลโปรแกรมระบบงานต่าง ๆ หรือกำหนดค่าระบบของโปรแกรมและกำหนด ผู้ใช้และสิทธิ์การเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล ดังนี้

(๑) ติดตั้ง โปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

(๒) กำหนดค่า หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด

(๔) ผู้ดูแลระบบ ต้องแจ้งผู้ใช้งาน หรือเจ้าของระบบงาน ให้สามารถเริ่มใช้งานได้ โดยแจ้งบัญชีผู้ใช้งาน รหัสผ่าน และสิทธิ์การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้

(๕) ผู้ดูแลระบบ ต้องกำหนดเกณฑ์การสำรอง หรือสำเนา และทดสอบกู้คืน (Restore Test)

(๖) ผู้ดูแลระบบ ต้องบันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้างหรือปรับปรุง

ส่วนที่ ๑๗ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ ๑๗๔. ผู้ดูแลระบบต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Proxy Engine และข้อมูลที่ใช้ในการจัดเก็บต้องไม่นำไปดำเนินการใด ๆ นอกเหนือจากที่ได้ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่มีกฎหมายให้สามารถกระทำได้

ข้อ ๑๗๕. ผู้ดูแลระบบห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้โดยเด็ดขาด

ข้อ ๑๗๖. ผู้ดูแลระบบกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๑๗๗. ผู้ดูแลระบบต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ ๑๗๘ ส่วนงานหรือมหาวิทยาลัย ต้องแต่งตั้งผู้รับผิดชอบในการประสานงานและให้ข้อมูลกับเจ้าพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งข้อมูลจราจรทางคอมพิวเตอร์นั้น เป็นไปด้วยความรวดเร็ว

ส่วนที่ ๑๘ แนวปฏิบัติเมื่อเกิดฟิชชิ่ง (Phishing) ที่เว็บเซิร์ฟเวอร์ของส่วนงานและมหาวิทยาลัย

ข้อ ๑๗๙. เมื่อผู้ดูแลระบบเครือข่ายของส่วนงานหรือมหาวิทยาลัยได้รับแจ้งหรือตรวจพบว่าเว็บเซิร์ฟเวอร์ของใด ๆ เป็นช่องทางให้ผู้ไม่หวังดีทำ ฟิชชิ่ง (Phishing) ผู้ดูแลระบบเครือข่ายที่มีหน้าที่รับผิดชอบจะดำเนินการ ดังนี้

(๑) ดำเนินการบล็อค IP address ของเว็บเซิร์ฟเวอร์ที่โดนฟิชชิ่งนั้น หรือแจ้งผู้ให้บริการเส้นทางเครือข่ายของส่วนงานหรือมหาวิทยาลัยดำเนินการโดยเร่งด่วน

(๒) แจ้งผู้ดูแลเว็บเซิร์ฟเวอร์ของหน่วยงานที่ถูกทำฟิชชิ่งทาง e-mail หรือทางโทรศัพท์ เพื่อให้ดำเนินการแก้ไขปัญหา

ข้อ ๑๘๐. เมื่อดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว ผู้ดูแลระบบเครือข่ายของส่วนงานหรือมหาวิทยาลัยที่พบปัญหา ต้องดำเนินการหรือแจ้งผู้ให้บริการเส้นทางเครือข่ายของมหาวิทยาลัย เพื่อปลดบล็อค IP address

ข้อ ๑๘๑. ผู้ดูแลเว็บเซิร์ฟเวอร์ของส่วนงานต้องตรวจสอบเว็บเซิร์ฟเวอร์และเว็บไซต์ภายในส่วนงานของตนเอง รวมทั้งติดตั้งโปรแกรมปรับปรุงช่องโหว่ (patch) อย่างสม่ำเสมอเพื่อป้องกันผู้ที่ไม่หวังดีในการเข้ามาทำฟิชชิ่ง

ส่วนที่ ๑๙ การรับมือเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response)

ข้อ ๑๘๒. ส่วนงานหรือมหาวิทยาลัย ต้องมีมาตรการในการเตรียมความพร้อมสำหรับเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ (Preparing for a Cyber security Incident)

ข้อ ๑๘๓. ส่วนงานหรือมหาวิทยาลัย ต้องมีมาตรการในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ (responding to cyber security incident)

ข้อ ๑๘๔. ส่วนงานหรือมหาวิทยาลัย ต้องมีการติดตามสถานการณ์ด้านความปลอดภัยทางไซเบอร์ (Following up the cyber security incident)

ส่วนที่ ๒๐ การใช้บริการ Cloud Computing

ข้อ ๑๘๕. ต้องกำหนดนโยบายการใช้บริการ Cloud Computing สำหรับผู้ให้บริการภายนอก

ข้อ ๑๘๖. ต้องมีแนวทางในการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้บริการ Cloud Computing

ข้อ ๑๘๗. ต้องมีการบริหารจัดการผู้ให้บริการ Cloud Computing จากภายนอก

ข้อ ๑๘๘. ต้องมีการรักษาความปลอดภัยและความลับของระบบงานและข้อมูลของการใช้บริการ Cloud Computing

ข้อ ๑๘๙. ต้องมีการดำเนินการเพื่อให้มั่นใจว่าระบบงานและข้อมูลของการใช้ระบริการ Cloud Computing มีความถูกต้องเชื่อถือได้

ข้อ ๑๙๐. ต้องมีการดำเนินการเพื่อให้มั่นใจถึงความพร้อมใช้ของการใช้บริการ Cloud Computing

ข้อ ๑๙๑. ต้องมีการดำเนินการเกี่ยวกับการคุ้มครองที่ครอบคลุมถึงผู้ใช้บริการของส่วนงาน หรือมหาวิทยาลัย

หมวดที่ ๒
การรักษาความปลอดภัยฐานข้อมูล การสำรองข้อมูล การรักษาและป้องกันความลับของข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของส่วนงานและมหาวิทยาลัยสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับมหาวิทยาลัยอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑. กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

(๑) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

(๒) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

(๒.๑) ผู้ดูแลระบบต้องกำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒.๒) ผู้ดูแลระบบต้องกำหนดเกณฑ์การระงับสิทธิ์ การมอบสิทธิ์ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้ใน หมวด ๑ ส่วนที่ ๒

(๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญของข้อมูลให้เป็นไปตามที่คณะกรรมการเกี่ยวกับการบริหารจัดการข้อมูล หรือคณะกรรมการเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลที่มหาวิทยาลัยแต่งตั้งเป็นผู้กำหนด ได้แก่ การจัดแบ่งหมวดหมู่ของข้อมูล การจัดแบ่งระดับความสำคัญของข้อมูล จัดแบ่งลำดับชั้นความลับของข้อมูล และจัดแบ่งระดับชั้นการเข้าถึง รวมถึงกำหนดรูปแบบของเอกสารอิเล็กทรอนิกส์

ข้อ ๒. ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวด ๑ ส่วนที่ ๒ ข้อ ๑๓

ข้อ ๔ การปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคล ให้ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ข้อ ๕. หน่วยงาน ส่วนงานหรือมหาวิทยาลัยเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน จะเป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๖. ข้อมูลที่สำคัญของหน่วยงาน ส่วนงาน หรือมหาวิทยาลัย ต้องกำหนดให้มีมาตรการการเข้ารหัสข้อมูลตามมาตรฐานสากล หรือให้สอดคล้องกับข้อตกลง ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้อง

ข้อ ๗. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกัน หรือการแลกเปลี่ยน หรือการขอใช้ข้อมูลระหว่างส่วนงานภายในของมหาวิทยาลัย กับหน่วยงานอื่นภายนอก ให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างส่วนงานหรือมหาวิทยาลัยกับหน่วยงานภายนอก ดังต่อไปนี้

(๑) การแลกเปลี่ยนสารสนเทศที่ผ่านช่องทางการสื่อสารทุกชนิดระหว่างส่วนงาน หรือมหาวิทยาลัยกับหน่วยงานภายนอก ต้องขออนุมัติหัวหน้าส่วนงาน หรือผู้บริหารระดับสูงสุดของมหาวิทยาลัยก่อน

(๒) การแลกเปลี่ยนสารสนเทศระหว่างส่วนงาน หรือมหาวิทยาลัยกับหน่วยงานภายนอกต้องดำเนินการการแลกเปลี่ยนข้อมูลด้วยวิธีการที่มีความมั่นคงปลอดภัยและสอดคล้องกับการจัดการระดับชั้นข้อมูลสารสนเทศ

(๓) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อควบคุม ป้องกัน และบริหารจัดการข้อมูล และสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่งร่วมกันเป็นลายลักษณ์อักษร

(๔) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

(๕) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(๖) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ

(๗) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

(๘) กำหนดสิทธิ์การเข้าถึงข้อมูล

(๙) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(๑๐) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๘. ผู้ดูแลระบบต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ ๙. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ ๑๐. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของส่วนงานและมหาวิทยาลัย พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๑. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อ ข้อมูลที่สำรองสำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบค่าคอนฟิกกูเรชันต่าง ๆ ของระบบการสำรองข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้ สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการ สำรองข้อมูลไว้อย่างชัดเจนในกรณีที่สำรองข้อมูลในรูปแบบของการใช้อุปกรณ์ภายนอก

(๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรอง กับส่วนงานหรือมหาวิทยาลัยต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับส่วนงานหรือมหาวิทยาลัย

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

(๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ ๑๒. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ คู่สัญญาที่ดูแลระบบ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ ๑๓. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๔. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ ๑๕. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๑๖. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละส่วนงานหรือมหาวิทยาลัยอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓ การรักษาและป้องกันความลับของข้อมูล

ข้อ ๑๗. ต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของส่วนงานหรือมหาวิทยาลัย หรือเป็นข้อมูลส่วนบุคคล หรือข้อมูลอื่นของบุคคลภายนอก

ข้อ ๑๘. ข้อมูลที่เป็นข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน หรือส่วนงาน หรือมหาวิทยาลัย ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำหรือทำลาย โดยไม่ได้รับอนุญาตจากผู้ที่มีอำนาจหน้าที่ตามที่ผู้ควบคุมข้อมูลกำหนด หรือเจ้าของข้อมูลส่วนบุคคล

ข้อ ๑๙. บุคลากรมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของหน่วยงาน ส่วนงาน และมหาวิทยาลัย หรือข้อมูลของผู้รับบริการ หรือข้อมูลส่วนบุคคล หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๐. ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๒๑. บุคลากรมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลตามที่ได้รับสิทธิ์ในการเข้าถึง เว้นแต่ข้อมูลนั้นเป็นข้อมูลส่วนบุคคล จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเสียก่อน ซึ่งมหาวิทยาลัยจะมีมาตรการหรือแนวทางการขอความยินยอมและแจ้งวัตถุประสงค์ในการขอใช้เก็บรวบรวมใช้และเผยแพร่ข้อมูลนั้น เพื่อให้การสนับสนุนการดำเนินงานของมหาวิทยาลัย และเคารพต่อสิทธิ์ส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใด ทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ที่มีอำนาจหน้าที่ตามที่ผู้ควบคุมข้อมูลกำหนด หรือเจ้าของข้อมูลส่วนบุคคลนั้นโดยเด็ดขาด

ข้อ ๒๒. ต้องจัดชั้นความลับของข้อมูล และปฏิบัติตามขั้นตอนการจัดระดับชั้นข้อมูลสารสนเทศ และต้องไม่เปิดเผยข้อมูลความลับต่อบุคคลที่ไม่เกี่ยวข้อง

ข้อ ๒๓. ต้องจัดเก็บเอกสารหรือข้อมูลที่เกี่ยวข้องกับงานของหน่วยงาน ส่วนงาน หรือ ในตู้หรือสถานที่จัดเก็บที่จัดเตรียมให้ เมื่อไม่มีความจำเป็นต้องใช้งานและต้องป้องกันไม่ให้เอกสารหรือข้อมูลถูกเปิดเผยอันเนื่องมาจากความประมาทในการจัดเก็บ

ข้อ ๒๔. การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

หมวดที่ ๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของส่วนงานหรือมหาวิทยาลัย (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้ส่วนงานหรือมหาวิทยาลัย ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อ ๑. จัดลำดับความสำคัญของความเสี่ยง

ข้อ ๒. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๓. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๔. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ ๕. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

ข้อ ๖. มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหาร จัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนาและมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ข้อ ๗. มีมาตรการซักซ้อมการบริหารความต่อเนื่องทางธุรกิจ

(๑) ดำเนินการซ้อมแผนการดำเนินธุรกิจอย่างต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง

(๒) บุคลากรต้องให้ความร่วมมือในการซ้อมแผนการดำเนินธุรกิจอย่างต่อเนื่อง หรือแผนการอื่นที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของส่วนงานหรือมหาวิทยาลัย (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของส่วนงานหรือมหาวิทยาลัยขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงันหรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

(๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของส่วนงานหรือมหาวิทยาลัย ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุดทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจากHuman error ลดน้อยลง

(๒) จัดทำหนังสือแจ้งเวียน เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), ข่าวไวรัสหลอกลวง (Hoax) และมัลแวร์ (Malware) โดยเฉพาะมัลแวร์เรียกค่าไถ่ (Ransomware) Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ จึงได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม ภัยจากไฟไหม้ หรือระบบไฟฟ้าขัดข้อง หรือการชำรุดของอุปกรณ์ด้านระบบเครือข่าย และเครื่องแม่ข่าย จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟ เกิดขึ้นภายในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย อุปกรณ์ตรวจจับควันจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายเพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

(๔) ต่ออายุการใช้งานหรือระยะเวลารับประกันอุปกรณ์ที่มีความสำคัญ หรือที่ประเมินแล้วหากชำรุดจะส่งผลร้ายแรงต่อระบบเทคโนโลยีสารสนเทศ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาอยู่ตลอดเวลาหรือตามสถานการณ์

(๒) กรณีใช้การ Backup ด้วยเทป ให้ถอดเทป Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

(๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

(๔) หากเครื่องแม่ข่ายอยู่ในพื้นที่เสี่ยง ให้เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง

(๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมระบบ คอมพิวเตอร์และเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

(๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้ส่วนงาน หรือผู้เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

ประเภทที่ ๕ ความเสี่ยงด้านระบบข้อมูล เป็นความเสี่ยงที่จะทำให้ข้อมูลรั่วไหล และกระทำความผิดตามพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) มีมาตรการในการจัดการสิทธิ์การเข้าถึงข้อมูล

(๒) มีมาตรการในการเข้ารหัสข้อมูลที่เป็นความลับ

(๓) มีมาตรการในการสำรองข้อมูลเพื่อให้ข้อมูลไม่สูญหาย

(๔) กำหนดให้มีการทดสอบการสู้คืนข้อมูล

หมวดที่ ๔
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของส่วนงานหรือมหาวิทยาลัย

แนวปฏิบัติ

ข้อ ๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒. ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ต้องมีลักษณะ ดังนี้

(๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะ โดยพิจารณาตามความสำคัญแล้วแต่กรณี

(๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก

(๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๔) จะต้องปิดล็อกตลอดเวลา หากมีการใช้งาน Key Card หรือ Key Pad หรือเทคโนโลยีอื่น ๆ ในการเข้าถึงพื้นที่ควบคุม ให้มีระบบสำรองไฟฟ้าในกรณีฉุกเฉินด้วย หรือการใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่ โดยการล็อกด้วยกุญแจจะต้องกำหนดเจ้าหน้าที่ในการเก็บรักษากุญแจ

(๕) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless Lan Coverage Area) เป็นต้น

ข้อ ๔. การควบคุมการเข้า-ออก อาคารสถานที่

(๑) กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้า-ออกในแต่ละ "พื้นที่ใช้งานระบบ" อย่างชัดเจน

(๒) การเข้าถึงอาคารของส่วนงานหรือมหาวิทยาลัย ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

(๓) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

(๔) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในส่วนงานหรือมหาวิทยาลัย

(๕) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(๖) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๗) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไปเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๘) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๙) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๐) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๑๒) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า- ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

(๑๓) จัดให้มีการดูแลและ เฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานใน พื้นที่หรือบริเวณที่มีความสำคัญ

(๑๔) จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของส่วนงานหรือมหาวิทยาลัยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของส่วนงานหรือมหาวิทยาลัยในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของ บุคคลภายนอก

(๗) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘. การนำทรัพย์สินออกนอกส่วนงานหรือมหาวิทยาลัย (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกส่วนงานหรือมหาวิทยาลัย

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกส่วนงานหรือมหาวิทยาลัย

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกส่วนงานหรือมหาวิทยาลัย

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของส่วนงานหรือมหาวิทยาลัยออกไปใช้งานนอกส่วนงานหรือมหาวิทยาลัย เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกส่วนงานหรือมหาวิทยาลัย (Security of Equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของส่วนงานหรือมหาวิทยาลัยออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของส่วนงานหรือมหาวิทยาลัยไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๕
การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ ๑. ระบบป้องกันผู้บุกรุก

(๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อ ๒. ระบบเครือข่าย

(๑) ดำเนินการตรวจระบบป้องกันการบุกรุกอย่างน้อยเดือนละ ๑ ครั้ง

(๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของเครือข่าย สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่เครือข่ายได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพีของเครือข่ายใดถูก Block เป็นจำนวนมาก

(๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงานของผู้ดูแลระบบ เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ต หรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

(๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในส่วนงานหรือมหาวิทยาลัยไปยังภายนอกหรือไม่

(๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของส่วนงานหรือมหาวิทยาลัยนวมินทราธิราช

(๓) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปภายนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

ข้อ ๔. การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย

(๑) เมื่อผู้ใดพบเหตุการณ์ด้านความมั่นคงปลอดภัย ให้รีบรายงานเหตุการณ์นั้นไปยังผู้ดำเนินการให้ความช่วยเหลือ โดยเร็วที่สุด

(๒) ให้ความร่วมมือและประสานงานกับผู้ดำเนินการให้ความช่วยเหลือในการดำเนินการจัดการกับเหตุการณ์นั้น

หมวดที่ ๖
การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของมหาวิทยาลัยนวมินทราธิราช

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบ คอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อ ๑. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของส่วนงานหรือมหาวิทยาลัย

ข้อ ๓. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ ๔. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อ ๖. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

ข้อ ๗. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของมหาวิทยาลัย

ข้อ ๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของมหาวิทยาลัย และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ ๗
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง คณบดี ผู้อำนวยการ หัวหน้าภาค หัวหน้าฝ่าย หัวหน้างาน เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ ๑. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CSO/CIO)
- หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือเทียบเท่าระดับหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
  - (๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ
  - (๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒. ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือ เทียบเท่าหัวหน้าฝ่าย

- (๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ
- (๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อ ๓. ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

- ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนงาน หรือผู้บริหารมหาวิทยาลัย เช่น นักวิชาการคอมพิวเตอร์ เป็นต้น
  - (๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
  - (๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ
  - (๓) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย
  - (๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด
  - (๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต
  - (๖) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต
  - (๗) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย