ประกาศสำนักคอมพิวเตอร์

เรื่อง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ

มหาวิทยาลัยทักษิณ

เพื่อกำหนดเป็นกรอบและเป็นแผนนำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยให้อยู่ระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001 ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลง และเป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศ มหาวิทยาลัยทักษิณ โดยมีรายละเอียดดังนี้

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ

หมวด ๑ ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ข้อ ๑.๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้าม ทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๑.๒ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๑.๓ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของมหาวิทยาลัยทักษิณ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อค หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดย

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการควรต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบเครือข่ายอินเตอร์เน็ตจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานระบบเครือข่ายอินเทอร์เน็ตต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคล ของผู้ใช้งานได้

(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอ ทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

หมวด ๒ ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ ๒.๑ ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ของสำนักคอมพิวเตอร์ ที่เป็นเขตหวงห้ามโดยเด็ดขาดเว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๒.๒ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๒.๓ ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๒.๔ ผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

ข้อ ๒.๕ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

ข้อ ๒.๖ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่มหาวิทยาลัยทักษิณมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบจะอยู่แนบท้ายเอกสารข้อบังคับนี้การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่สำนักคอมพิวเตอร์มอบหมาย

ข้อ ๒.๗ กรณีที่มีการนำครุภัณฑ์ไปใช้ภายนอกมหาวิทยาลัยทักษิณ ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของมหาวิทยาลัยทักษิณที่ได้รับมอบหมาย

ข้อ ๒.๘ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๒.๙ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับ การอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ ๒.๑๐ ทรัพย์สินและระบบสารสนเทศต่างๆ ที่มหาวิทยาลัยทักษิณ จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของมหาวิทยาลัยทักษิณเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่มหาวิทยาลัยทักษิณไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อมหาวิทยาลัยทักษิณ

ข้อ ๒.๑๑ ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๑๓ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด ๓ ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ ๓.๑ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของมหาวิทยาลัยทักษิณ หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๓.๒ ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของมหาวิทยาลัยทักษิณ ถือเป็นทรัพย์สินของมหาวิทยาลัยทักษิณ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๓.๓ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของมหาวิทยาลัยทักษิณ หรือ ข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมี ส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๓.๔ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๓.๕ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร มหาวิทยาลัยทักษิณ จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคล ใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ มหาวิทยาลัยทักษิณ ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับมหาวิทยาลัยทักษิณ ซึ่งมหาวิทยาลัยทักษิณอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด ๔ ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ ๔.๑ ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะ รหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะ เช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อ ศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๔.๒ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์(Bittorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๔.๓ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๔.๔ ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยทักษิณที่จัดเตรียมให้เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรมความมั่นคงของ ประเทศ กฎหมาย หรือกระทบต่อภารกิจของมหาวิทยาลัยทักษิณ

ข้อ ๔.๕ ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยทักษิณ เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและ ศีลธรรม หรือกระทบต่อภารกิจของมหาวิทยาลัยทักษิณ

ข้อ ๔.๖ ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยทักษิณ เพื่อประโยชน์ทางการค้า

ข้อ ๔.๗ ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่าย ระบบสารสนเทศของมหาวิทยาลัยทักษิณ โดยเด็ดขาดไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ ๔.๘ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของมหาวิทยาลัยทักษิณต้องหยุดชะงัก

ข้อ ๔.๙ ห้ามใช้ระบบสารสนเทศของมหาวิทยาลัยทักษิณ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๔.๑๐ ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะ เป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๔.๑๑ ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของมหาวิทยาลัยทักษิณ โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด ๕ ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ข้อ ๕.๑ บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบ ของมหาวิทยาลัยทักษิณ ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด ๖ ว่าด้วยซอฟต์แวร์และลิขสิทธิ์(Software Licensing and intellectual property)

ข้อ ๖.๑ มหาวิทยาลัยทักษิณ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่มหาวิทยาลัยทักษิณ อนุญาตให้ใช้งานหรือที่มหาวิทยาลัยทักษิณ มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และมหาวิทยาลัยทักษิณห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งาน ซอฟต์แวร์อื่นใดที่ไม่

มีลิขสิทธิ์หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์มหาวิทยาลัยทักษิณถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๖.๒ ซอฟต์แวร์ (Software) ที่มหาวิทยาลัยทักษิณได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด ๗ ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี(Preventing MalWare)

ข้อ ๗.๑ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti Virus) ตามที่มหาวิทยาลัยทักษิณ ได้ประกาศให้ใช้เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกันโดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๗.๒ บรรดาข้อมูล ไฟล์ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัส คอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๗.๓ ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๗.๔ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งาน ต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๗.๕ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ เครือข่าย และ ต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๗.๖ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆที่เป็นทรัพย์สิน ของมหาวิทยาลัยทักษิณ หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๗.๗ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความ เสียหายมาสู่ทรัพย์สินของมหาวิทยาลัยทักษิณ

หมวด ๘ ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์(Electronic mail)

ข้อ ๘.๑ ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้ สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสาร ได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัย ของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และ จัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บัญชาการมหาวิทยาลัยทักษิณทราบทันที

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของ หน่วยงาน

นโยบายความมั่นคงปลอดภัยของอีเมล์(E-mail Policy)

ข้อ ๑ ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่ของสำคอมพิวเตอร์

ข้อ ๒ เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที

ข้อ ๓ ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๔ ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์(e-mail) ของตน

ข้อ ๕ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๖ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

นโยบายความมั่นคงปลอดภัยของอินเตอร์เน็ต (Internet Security Policy)

ข้อ ๑ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงต่อชาติศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการ ผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๓ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลดการ อัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๔ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ ๖ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์ (Web Browser) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ