นโยบายการใช้งานทรัพย์สินสารสนเทศคณะฯ อย่างมั่นคงปลอดภัย

Acceptable Use Policy

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

รหัสเอกสาร : ISMS-PL-I-003
ฉบับที่ : 2.0
ประเภทเอกสาร : เอกสารภายใน

สารบัญ

การควบคุมเอกสาร **1**

นโยบายการใช้งานทรัพย์สินสารสนเทศคณะฯ อย่างมั่นคงปลอดภัย (ACCEPTABLE USE POLICY) **1**

1. บทนำ **2**

1.1 วัตถุประสงค์ 2
1.2 ขอบเขต 2
1.3 คำจำกัดความ 2

2. นโยบาย **3**

2.1 บทนำ 3
2.2 ข้อมูลของคณะฯ 3
2.3 คอมพิวเตอร์ของคณะฯ 5
2.4 สำนักงานของคณะฯ 9
2.5 พนักงานของคณะฯ 11

การควบคุมเอกสาร

การอนุมัติใช้เอกสาร

เอกสารนี้ผ่านการทบทวนและอนุมัติโดย:

จัดเตรียมเอกสารโดย	ทบทวนเอกสารโดย	อนุมัติเอกสารโดย
(นางสาวอลิศา นิ่มวรพันธุ์) คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	(นางอัจฉราภรณ์ อังศุรัตนเวช) ผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	(ศาสตราจารย์ (เชี่ยวชาญพิเศษ) นายแพทย์บรรณกิจ โลจนาภิวัฒน์) ประธานกรรมการอำนวยการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
วันที่ 26 มกราคม 2566	วันที่ 1 กุมภาพันธ์ 2566	วันที่ 7 กุมภาพันธ์ 2566

ประวัติการปรับปรุงเอกสาร

ตารางบันทึกประวัติการปรับปรุงเอกสาร:

ฉบับที่	วันที่	รายละเอียดการปรับปรุงเอกสาร	อนุมัติโดย
1.0	9 กันยายน 2565	เริ่มต้นใช้งานเอกสาร	ศ.(เชี่ยวชาญพิเศษ) นพ. บรรณกิจ โลจนาภิวัฒน์
2.0	26 มกราคม 2566	เพิ่มระดับชั้นความลับในรหัสเอกสาร	ศ.(เชี่ยวชาญพิเศษ) นพ. บรรณกิจ โลจนาภิวัฒน์

นโยบายการใช้งานทรัพย์สินสารสนเทศคณะฯอย่างมั่นคงปลอดภัย
(Acceptable Use Policy)

1. บทนำ

1.1 วัตถุประสงค์

เพื่อกำหนดแนวทางการใช้งานข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของคณะฯ ให้เป็นไปอย่างมีความมั่นคงปลอดภัย มีความเหมาะสม มีความสอดคล้องกับกฎหมาย กฎระเบียบ ตลอดจนข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง เพื่อเป็นการปกป้องพนักงาน และทรัพย์สินของคณะฯ ให้พ้นจากความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ หรือการใช้งานที่ไม่ถูกต้อง เช่น การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การเจาะระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศของคณะฯ และการกระทำใดๆ ที่ขัดต่อกฎหมาย กฎระเบียบ เป็นต้น

1.2 ขอบเขต

นโยบายนี้ครอบคลุมถึงบุคคลทุกคน ไม่ว่าจะเป็นพนักงานประจำ พนักงานชั่วคราว คู่สัญญา คู่ค้า ที่ปรึกษา บุคคลภายนอก หรือผู้ใดก็ตามที่ ได้รับอนุญาตให้เป็นผู้ใช้งานข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ และทรัพย์สินอื่นๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของคณะฯ ภายใต้ขอบเขตการดำเนินการของระบบ ISMS

1.3 คำจำกัดความ

คำ	ความหมาย
คณะฯ	คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่
Management Representative (MR)	ตัวแทนฝ่ายบริหารระบบมาตรฐาน ในที่นี้ได้แก่ ISMR หรือ ISMA
ISMR	Information Security Management Representative
ISMA	Information Security Management Assistance
DC	ศูนย์คอมพิวเตอร์แม่ข่ายหลัก
DR Site	ศูนย์คอมพิวเตอร์แม่ข่ายสำรอง

2. นโยบาย

2.1 บทนำ

นโยบายฉบับนี้จัดทำขึ้นเพื่อปกป้องคุ้มครองข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของคณะฯ ให้มีความมั่นคงปลอดภัย โดยมีองค์ประกอบหลัก 4 ส่วน ได้แก่

2.1.1 ข้อมูลของคณะฯ: ข้อมูลของคณะฯ คือทรัพย์สินที่มีความสำคัญมากที่สุด และต้องได้รับการปกป้องให้คงไว้ซึ่ง

- ความลับ (Confidentiality)
- ความถูกต้องครบถ้วน (Integrity)
- ความพร้อมใช้งาน (Availability)

2.1.2 คอมพิวเตอร์ของคณะฯ: การดำเนินงานของคณะฯ จำเป็นต้องอาศัยคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลอิเล็กทรอนิกส์ ดังนั้น จึงถือเป็นหน้าที่ของพนักงาน และผู้ที่เกี่ยวข้องทุกคนในการรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของคณะฯ อย่างสุดความสามารถ

2.1.3 สำนักงานของคณะฯ: สำนักงานของคณะฯ คือพื้นที่ปฏิบัติงานของพนักงาน และผู้ที่เกี่ยวข้อง ซึ่งพื้นที่เหล่านี้อาจถูกล่วงละเมิดความมั่นคงปลอดภัยได้ หากไม่ได้รับการปกป้องคุ้มครองอย่างเหมาะสม

2.1.4 พนักงานของคณะฯ: พนักงานทุกคนต่างมีความรับผิดชอบต่อข้อมูลของคณะฯ ดังนั้น พนักงานจึงจำเป็นต้องทราบถึงวิธีการปกป้องข้อมูลสารสนเทศให้พ้นจากการถูกล่วงละเมิดความมั่นคงปลอดภัย ทั้งในขณะที่ปฏิบัติงานภายในพื้นที่สำนักงาน การทำงานที่บ้าน หรือการทำงานระหว่างการเดินทางไปปฏิบัติงานนอกสถานที่

2.2 ข้อมูลของคณะฯ

2.2.1 การจำแนกและระบุชั้นความลับของข้อมูล

- เจ้าของข้อมูลต้องจำแนกชั้นความลับของข้อมูลทั้งหมดที่อยู่ในความรับผิดชอบของตน โดยพิจารณาจากความจำเป็นในการเข้าถึงข้อมูลเพื่อการปฏิบัติงาน ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้องในการปกป้องข้อมูล และผลกระทบทางการดำเนินงานอื่น ๆ ที่เกี่ยวข้อง ทั้งนี้ ข้อมูลของคณะฯ ถ้าไม่มีการระบุชั้นความลับไว้ให้ถือเป็น “Internal Use Only” ทั้งหมด ข้อมูลเพิ่มเติมสามารถอ้างอิงได้จาก Information Classification and Handling Policy
- เจ้าของข้อมูลต้องดำเนินการให้มั่นใจได้ว่าข้อมูลทั้งหมดที่อยู่ในความรับผิดชอบของตนได้รับการระบุ/ติดฉลาก (Label) ชั้นความลับอย่างเหมาะสม ข้อมูลเพิ่มเติมสามารถอ้างอิงได้จาก Information Classification and Handling Policy

2.2.2 การใช้งานและการปกป้องข้อมูลลับ

- ผู้ใช้งานทุกคนต้องใช้งานข้อมูลของคณะฯ ตามกฎระเบียบและคำแนะนำที่ระบุไว้ใน Information Classification and Handling Policy อย่างเคร่งครัด

- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษในการใช้งานข้อมูลประเภท “Secret” และ “Confidential” (ซึ่งต่อไปในเอกสารนี้จะเรียกว่า “ข้อมูลลับ”) ตามที่ได้ระบุไว้ใน Information Classification and Handling Policy เพื่อป้องกันไม่ให้ข้อมูลลับถูกเข้าถึง และ/หรือ ถูกเปิดเผยโดยไม่ได้รับอนุญาต
- ข้อมูลลับของคณะฯ ต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น (ตามหลักการ “Need to Know”)
- ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลลับที่ถูกเก็บไว้ในอุปกรณ์คอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง อุปกรณ์คอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือแอพพลิเคชั่นอย่างเหมาะสม
- ข้อมูลใดที่ผู้ใช้งานพิจารณาว่าเป็นข้อมูลลับและมีจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศจำเป็นต้องได้รับการเข้ารหัส โดยอ้างอิงตาม Information Classification and Handling Policy
- ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล๊อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อบันทึกข้อมูลนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน
- เอกสารข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่างๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร ฯลฯ ทันที
- พนักงานต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล
- พนักงานต้องไม่พูดคุยหรือใช้งานข้อมูลลับของคณะฯ ในพื้นที่สาธารณะ เช่น ในลิฟท์ ร้านอาหาร ร้านกาแฟ สนามบิน ฯลฯ

2.2.3 การใช้งานสื่อบันทึกข้อมูลที่มีข้อมูลลับ

- สื่อบันทึกข้อมูล และอุปกรณ์เคลื่อนที่ต่างๆ (เช่น External Hard disk, Thumb-Drive, CD-Rom เป็นต้น) ที่มีข้อมูลลับของคณะฯ บันทึกอยู่ ต้องได้รับการดูแลรักษาความมั่นคงปลอดภัย และต้องใช้งานอย่างระมัดระวัง และสอดคล้องตาม Information Classification and Handling Policy

2.2.4 การสำรองข้อมูลสำคัญ

- ข้อมูลที่เกี่ยวข้องกับการดำเนินงานของคณะฯ ทั้งหมด ทั้งที่มีการเก็บรักษาอยู่ในอุปกรณ์คอมพิวเตอร์ของผู้ใช้งานหรือเครื่องเซิร์ฟเวอร์ที่ดูแลโดยผู้ใช้งาน ต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใดๆ เกิดขึ้น ตัวอย่างเช่น อุปกรณ์คอมพิวเตอร์ติดไวรัส ฮาร์ดดิสก์เสีย เป็นต้น

2.3 คอมพิวเตอร์ของคณะฯ

2.3.1 การใช้งานอุปกรณ์

- ระบบเทคโนโลยีสารสนเทศ และอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่คณะฯ เป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของคณะฯ การใช้งานระบบและอุปกรณ์ต่างๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่รับผิดชอบของพนักงาน
- ผู้ใช้งานต้องรับผิดชอบในการใช้งานคอมพิวเตอร์ และอุปกรณ์ต่างๆ ของคณะฯ อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นทรัพย์สินของตน
- อุปกรณ์คอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์พกพา เครื่องเซิร์ฟเวอร์ เครื่องเวิร์คสเตชั่น และเครื่องเทอร์มินัลทั้งหมดของคณะฯ ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
- ผู้ใช้งานต้องไม่เชื่อมต่ออุปกรณ์คอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายของคณะฯ เว้นแต่ได้รับการอนุมัติและลงทะเบียนอุปกรณ์คอมพิวเตอร์ส่วนตัวนั้นกับงานเทคโนโลยีสารสนเทศ
- อุปกรณ์คอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับอุปกรณ์คอมพิวเตอร์ที่ใช้งานอยู่ภายในคณะฯ ซึ่งได้แก่ การติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ ซอฟต์แวร์ป้องกันสปายแวร์ ไฟร์วอล (Firewall) การอัพเดท Security Patch ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์
- ตัวอุปกรณ์คอมพิวเตอร์ของคณะฯ ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์ใด ๆ เพิ่มเติม ก่อนได้รับอนุญาตจากหัวหน้างานเทคโนโลยีสารสนเทศ และพนักงานต้องไม่อนุญาตให้ผู้ที่ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์และ/ หรือซอฟต์แวร์ใดๆ บนอุปกรณ์คอมพิวเตอร์ของคณะฯ อย่างเด็ดขาด

2.3.2 การใช้งานซอฟต์แวร์

- ห้ามผู้ใช้งานทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของคณะฯ
- ห้ามผู้ใช้งานทำการติดตั้งซอฟต์แวร์ใดๆ ลงในอุปกรณ์คอมพิวเตอร์ของคณะฯ ก่อนได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศ
- ห้ามผู้ใช้งานนำซอฟต์แวร์ของคณะฯ ไปติดตั้งใช้งานส่วนตัวหรือทำสำเนาโดยไม่ได้รับอนุญาต
- แอพพลิเคชั่นทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของคณะฯ มีความเข้าใจและสามารถใช้งานแอพพลิเคชั่นได้
- รายชื่อซอฟต์แวร์ หรือแอพพลิเคชั่น ที่ถูกติดตั้งในอุปกรณ์คอมพิวเตอร์ของผู้ใช้งาน ต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยหัวหน้างานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของคณะฯ เท่านั้น ในกรณีที่ผู้ใช้งานจำเป็นต้องใช้ซอฟต์แวร์อื่นเพิ่มเติม ให้ดำเนินการขออนุมัติจากหัวหน้างานเทคโนโลยีสารสนเทศก่อน

2.3.3 การใช้งานอีเมล

- ผู้ใช้งานอีเมลทั้งหมดของคณะฯ จะได้รับ E-mail account จากมหาวิทยาลัยเชียงใหม่ หลังจากที่ได้รับการบรรจุเป็นพนักงานของคณะฯ

- E-mail account ต้องได้รับการปกป้องด้วยรหัสผ่าน ที่มีความมั่นคงปลอดภัย เพื่อป้องกันการถูกล่วงละเมิด และ/หรือ การนำอีเมลไปใช้ในทางที่ผิด
- E-mail account ที่มีวัตถุประสงค์พิเศษ เช่น its@cmu.ac.th อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail account กลางของแผนก และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานอย่างน้อยหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่รับผิดชอบเป็นเจ้าของ E-mail account นั้น โดยจะต้องมีการแจ้งไปยังสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ เป็นลายลักษณ์อักษร
- E-mail account ทั้งหมดและอีเมลทุกฉบับ (รวมถึงอีเมลส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์หรือระบบเครือข่ายของมหาวิทยาลัยฯ ถือเป็นทรัพย์สินของมหาวิทยาลัยฯ
- พื้นที่เก็บอีเมลบนเครื่องเซิร์ฟเวอร์ส่วนกลาง (Mailbox size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้ เมื่อปริมาณของอีเมลมากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของอีเมลมากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ-ส่งอีเมลได้ตามปกติอีกต่อไป
- ขนาดของอีเมลและไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมลและไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายตีกลับ
- ผู้ใช้งานต้องลบอีเมลที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมลให้เป็นไปตามขนาดที่มหาวิทยาลัยฯ กำหนด ทั้งนี้ ผู้ใช้งานต้องเก็บรักษาอีเมลที่เกี่ยวข้องกับการทำงาน และอีเมลตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้งาน E-mail account ของมหาวิทยาลัยฯ เพื่อกระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย เช่น ใช้งาน E-mail account ของมหาวิทยาลัยฯ เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ ขายสินค้าผิดกฎหมาย เป็นต้น
- พนักงานต้องไม่ใช้ E-mail address ของมหาวิทยาลัยฯ ในการประกาศข้อมูลใดๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว รวมถึงเครือข่ายสังคม (Social Network) เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับมหาวิทยาลัยฯ
- ข้อมูลลับต้องได้รับการเข้ารหัสเมื่อจำเป็นต้องถูกส่งผ่านทางอีเมล เพื่อป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต
- ซอฟต์แวร์สำหรับใช้งานอีเมลต้องได้รับการตั้งค่าให้อีเมลส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อคณะฯ และเบอร์โทรศัพท์ติดต่อ
- อีเมลส่งออกทุกฉบับต้องมีข้อความแสดงเจตจำนง/ข้อยกเว้นความรับผิดของคณะฯ แนบท้ายเสมอ
- ระบบต้องทำการ Block อีเมลตอบกลับอัตโนมัติสำหรับผู้ส่งที่อยู่ภายนอกระบบเครือข่ายของคณะฯ
- ห้ามผู้ใช้งานทำสำเนาข้อความหรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมลของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมลด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมลนั้นในนามตัวแทนของคณะฯ

- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล หัวจดหมายอีเมล ลายเซ็นในอีเมล หรือ E-mail account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมลโดยใช้ E-mail account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม
- ผู้ใช้งานต้องทำการส่งอีเมลให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้น ตามหลักการ “Need-to-know” และห้ามใช้คำสั่ง “Reply All” ถ้าหากอีเมลฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน
- ห้ามผู้ใช้งานส่งอีเมลที่ผู้รับไม่ได้มีความต้องการรับ ตัวอย่างเช่น อีเมลขยะ (Junk Mail) โฆษณาสินค้าต่างๆ (Spam Mail) อีเมลลูกโซ่ อีเมลหลอกลวงใดๆ (Scam Mail) โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมลที่มีรูปภาพหรือเนื้อหาดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ การพนัน หรือลามกอนาจารโดยเด็ดขาด
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษ เมื่อมีความจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัสคอมพิวเตอร์ อีเมลบอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)
- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ว่า อุปกรณ์คอมพิวเตอร์ของตนถูกโจมตีโดยไวรัสคอมพิวเตอร์ ผู้ใช้งานต้องระงับการส่งอีเมลโดยทันที จนกว่าอุปกรณ์คอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

2.3.4 การใช้งานอินเทอร์เน็ต

- คณะฯ จัดหาบริการอินเทอร์เน็ตไว้เพื่ออำนวยความสะดวกแก่พนักงานในการทำงาน การค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก ผู้รับบริการ ผู้ให้บริการภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของคณะฯ
- ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุทำให้คณะฯ หรือ บุคคลผู้ที่เกี่ยวข้องกับคณะฯ เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่าน Stand-Alone Workstation เท่านั้น คณะฯ ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งานเพื่อตรวจสอบการใช้งานที่ไม่เหมาะสม
- ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป็อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่หรืออาจโจรกรรมข้อมูลในอุปกรณ์คอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
- ห้ามผู้ใช้งานเข้าชม ใช้งาน ดาวน์โหลด รับ หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
- ห้ามใช้โปรแกรมประเภท Peer-to-peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit Torrent), อีมูล (e-mule) เป็นต้น
- ห้ามผู้ใช้งานวิพากษ์วิจารณ์บนเว็บไซต์ที่เกี่ยวข้องกับ ชาติ ศาสนา พระมหากษัตริย์ สิ่งที่ขัดต่อศีลธรรมอันดี ความมั่นคงของประเทศ และกฎหมาย

- ถ้าหากประสิทธิภาพการทำงานของอุปกรณ์คอมพิวเตอร์ของผู้ใช้งานลดลงหลังจากการเข้าชมเว็บไซต์ใดๆ ผู้ใช้งานต้องแจ้งให้ Help Desk ทราบทันทีเพื่อหาสาเหตุและดำเนินการแก้ไขปัญหา

2.3.5 การป้องกันไวรัสคอมพิวเตอร์

- ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใด ๆ ตัวอย่างเช่น ไวรัสคอมพิวเตอร์ หนอนอินเทอร์เน็ต (Worm) โปรแกรมแฝง (ม้าโทรจัน) อีเมลบอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ของคณะฯ
- ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์
- ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้นที่ได้รับอนุญาตให้สามารถรับ-ส่งผ่านระบบเครือข่ายของคณะฯ ได้ ทั้งนี้ผู้ใช้งานต้องรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ ผู้ใช้งานต้องทำการสแกนไวรัสคอมพิวเตอร์ในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ของคณะฯ ก่อนเปิดใช้งานเสมอ
- ถ้าหากผู้ใช้งานสงสัยว่าอุปกรณ์คอมพิวเตอร์ของตนติดไวรัสคอมพิวเตอร์หรือได้รับการแจ้งเตือนจากซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ว่าอุปกรณ์คอมพิวเตอร์ถูกโจมตีโดยไวรัสคอมพิวเตอร์แล้ว ผู้ใช้งานต้องหยุดการทำงานทั้งหมด และแจ้งเหตุต่อ Help Desk ทันที

2.3.6 การใช้งานรหัสผ่านอย่างมั่นคงปลอดภัย

- ผู้ใช้งานแต่ละคนต้องได้รับมอบ Unique user account เพื่อใช้ในการเข้าถึงระบบสารสนเทศและบริการต่าง ๆ ของคณะฯ ทั้งนี้ การมอบสิทธิ์ดังกล่าวต้องสอดคล้องตามหลักการ “Need-to-Know” และ “Need-to-Use” อย่างเคร่งครัด
- รหัสผ่าน (password) ต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้ใน Password Standard
- รหัสผ่าน (password) ต้องมีความมั่นคงปลอดภัยตามที่ได้กำหนดไว้ใน Password Standard
- รหัสผ่าน (password) ถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านไว้อย่างมั่นคงปลอดภัย ห้ามใช้งาน User account ร่วมกันหรืออนุญาตให้ผู้อื่นเข้าใช้งาน User account ของตนโดยเด็ดขาด ทั้งนี้ รวมถึงสมาชิกในครอบครัวเมื่อผู้ใช้งานนำงานกลับไปทำที่บ้านด้วย
- ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่าน User account และรหัสผ่านของตนทั้งหมด
- รหัสผ่านที่มีสิทธิพิเศษในระบบสารสนเทศที่สำคัญของคณะฯ ต้องได้รับการควบคุมโดยงานเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายหน้าที่อย่างเป็นทางการ
- ผู้ใช้งานทุกคนต้องได้รับการฝึกอบรม เพื่อให้มีความรู้และความตระหนักรู้ในการใช้งานรหัสผ่านอย่างถูกต้อง มั่นคงปลอดภัย และเพื่อให้รับทราบเทคนิคต่าง ๆ ที่ใช้ป้องกันการถูกหลอกลวงและนำไปสู่การถูกโจรกรรมข้อมูล
- ระบบหรือการกระทำใด ๆ ที่ไม่สอดคล้องกับนโยบายฉบับนี้ต้องได้รับการบันทึก ประเมิน และพิจารณาอนุมัติอย่างเหมาะสมเป็นกรณีไป ตัวอย่างเช่น ถ้าหากจำเป็นต้องมีการใช้งาน User account ร่วมกันโดยผู้ใช้งานตั้งแต่หนึ่งคนขึ้นไปงานเทคโนโลยีสารสนเทศ ต้องเก็บบันทึกรายชื่อผู้ที่มีสิทธิ์ใช้งาน User account ดังกล่าว และระบบทั้งหมดที่ User account นั้นมีสิทธิ์เข้าถึง

- ถ้าหากผู้ใช้งานสงสัยว่า User account หรือรหัสผ่านของตนถูกล่วงละเมิดความมั่นคงปลอดภัย ให้ผู้ใช้งานแจ้งเหตุต่อ Help Desk และทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที
- การขอ Reset Password โดยผู้ใช้งาน ต้องดำเนินการตามกระบวนการมาตรฐานของคณะฯ เท่านั้น โดยผู้ใช้งานต้องแสดงตัวตน และสิทธิ์ความเป็นเจ้าของ User account นั้น ๆ เจ้าหน้าที่ที่เกี่ยวข้องมีสิทธิ์ในการขอข้อมูลและพิสูจน์ตัวตนของผู้ใช้งานตามความเหมาะสม
- ในทางกลับกัน ผู้ใช้งานอาจได้รับการร้องขอจากงานเทคโนโลยีสารสนเทศ ให้ทำการเปลี่ยนรหัสผ่านใหม่ ถ้าหากรหัสผ่านของผู้ใช้งานไม่มีความมั่นคงปลอดภัย สามารถถูกคาดเดา หรือถูกล่วงละเมิดได้โดยง่าย ทั้งนี้ผู้ใช้งานต้องตรวจสอบความถูกต้องของแหล่งที่มาของคำร้องขอดังกล่าวด้วย เพื่อให้มั่นใจว่าการร้องขอนั้นไม่ได้เป็นการหลอกลวง

2.4 สำนักงานของคณะฯ

2.4.1 ความมั่นคงปลอดภัยทางกายภาพ

- ผู้ใช้งานต้องดูแลรักษาสภาพแวดล้อมในการทำงานเสมือนดูแลบ้านของตน
- พนักงานและบุคคลภายนอกต้องติดบัตรพนักงานหรือบัตรผู้มาติดต่อตลอดเวลาที่อยู่ในพื้นที่สำนักงาน ทั้งนี้ บัตรพนักงานและบัตรผู้มาติดต่อไม่อนุญาตให้โอนกรรมสิทธิ์ หรือหยิบยืมกันใช้งาน
- พนักงานต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรพนักงานหรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต
- ผู้ใช้งานต้องแจ้งพนักงานรักษาความปลอดภัย (รปภ.) ทันที เมื่อพบเห็นบุคคลแปลกหน้าหรือบุคคลที่ไม่แขวนบัตรพนักงานหรือบัตรผู้มาติดต่อในพื้นที่สำนักงาน
- พนักงานควรติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ภายในพื้นที่สำนักงาน
- พนักงานควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล๊อค อย่างเหมาะสม และกุญแจได้ถูกเก็บรักษาไว้อย่างมั่นคงปลอดภัย
- ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล๊อคกุญแจโดยเด็ดขาด
- ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม การทำลายข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์เหล่านี้อ้างอิงได้จาก Information Classification and Handling Policy
- พนักงานต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการและเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของคณะฯ เท่านั้น

2.4.2 ความมั่นคงปลอดภัยของระบบเครือข่าย

- ห้ามผู้ใช้งานติดตั้งอุปกรณ์เครือข่ายอื่น ๆ ที่ไม่ได้รับอนุญาตต่อกับอุปกรณ์คอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของคณะฯ โดยไม่ได้รับอนุญาต
- ห้ามบุคคลภายนอกทำการเชื่อมต่ออุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของคณะฯ โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง
- ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router, Switch, Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด
- การเข้าถึงระบบเครือข่ายของคณะฯ จากระยะไกลต้องได้รับการพิสูจน์ตัวตนผู้ใช้งานอย่างเหมาะสม
- ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของคณะฯ ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอกอื่นใดผ่านทางอุปกรณ์เชื่อมต่ออื่นๆ ที่ไม่ได้รับอนุญาตในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในคณะฯ โดยเด็ดขาด

2.4.3 การใช้งานโทรศัพท์ โทรสาร และเครื่องถ่ายเอกสาร

- ผู้ใช้งานต้องปกป้องความมั่นคงปลอดภัยของข้อมูลลับอย่างเต็มที่ เมื่อจำเป็นต้องส่งหรือรับข้อมูลนั้นผ่านเครื่องโทรสาร ทั้งนี้ รายละเอียดเพิ่มเติมดูได้จาก Information Classification and Handling Policy
- ถ้าหากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่างเช่น ส่งโทรสารผิดหมายเลข ผิดฝ่าย เป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น
- ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในบริเวณเปิด เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น
- ห้ามผู้ใช้งานบันทึกหรือฝากข้อความที่มีข้อมูลลับในเครื่องตอบรับโทรศัพท์อัตโนมัติ หรือระบบวอยซ์เมล์โดยเด็ดขาด
- ห้ามสนทนาเกี่ยวกับข้อมูลลับผ่านลำโพงของเครื่องโทรศัพท์ (Speakerphones) หรือผ่านสื่ออิเล็กทรอนิกส์ใด ๆ เช่น Voice Over IP หรือในระหว่างการประชุมทางไกล เว้นแต่
    - ผู้เข้าร่วมการประชุมทุกฝ่ายได้รับการพิสูจน์ตัวตนแล้วว่าเป็นผู้ที่เกี่ยวข้องและมีสิทธิ์รับทราบข้อมูล
    - ผู้ที่เกี่ยวข้องตรวจสอบจนมั่นใจแล้วว่าไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยินข้อมูลลับที่สนทนาอยู่
    - การประชุมทางไกลถูกจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย เช่น ห้องประชุมที่มีผนังและประตูที่เหมาะสมสามารถป้องกันเสียงลอดออกมาได้ เป็นต้น
- ผู้ใช้งานต้องสนทนาโทรศัพท์ด้วยความระมัดระวัง เพื่อป้องกันไม่ให้ข้อมูลลับถูกแอบฟังโดยบุคคลที่ไม่ได้รับอนุญาต
- ในกรณีที่ต้องมีการเปิดเผยข้อมูลลับใดๆ ทางโทรศัพท์ ผู้ให้ข้อมูลต้องทำการตรวจสอบให้มั่นใจว่าคู่สนทนานั้นเป็นผู้ที่ได้รับอนุญาตให้รับทราบข้อมูลดังกล่าว ก่อนที่จะเปิดเผยข้อมูล

- ผู้ใช้งานต้องขออนุญาตจากเจ้าของข้อมูลก่อนทำการถ่ายเอกสารหรือสแกนเอกสารที่มีข้อมูลลับ โดยสำเนาเอกสารนั้นต้องได้รับการปกป้องดูแลในระดับเทียบเท่ากับเอกสารต้นฉบับ อ้างอิงตาม Information Classification and Handling Policy
- พนักงานต้องไม่เปิดเผยสถานที่ตั้งของศูนย์คอมพิวเตอร์แม่ข่ายหลัก (Data Center) หรือศูนย์คอมพิวเตอร์สำรอง (DR Site) ต่อบุคคลภายนอกโดยเด็ดขาด เว้นแต่บุคคลภายนอกนั้นมีความจำเป็นต้องรับทราบเพื่อการปฏิบัติงาน

2.5 พนักงานของคณะฯ

2.5.1 การปฏิบัติตามกฎ และนโยบายต่าง ๆ

- พนักงานทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารสนับสนุนต่าง ๆ อย่างเคร่งครัด
- ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านบนระบบเทคโนโลยีสารสนเทศของคณะฯ ถือเป็นทรัพย์สินของคณะฯ (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของผู้รับบริการ หรือบุคคลภายนอก รวมถึงซอฟต์แวร์ หรือวัสดุอื่นๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้ คณะฯ สามารถเปิดเผย หรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่างๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า
- เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของคณะฯ ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอุปกรณ์คอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่างๆ ของคณะฯ กำหนดไว้
- คณะฯ ขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งานโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตาม คณะฯ จะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใด ๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งศาล ตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น
- ห้ามพนักงานใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของคณะฯ กระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม
- ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของคณะฯ โดยเด็ดขาด
- การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใดๆ ออกนอกประเทศต้องไม่ขัดต่อข้อกฎหมายใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

2.5.2 การรายงานเหตุล่วงละเมิดความมั่นคงปลอดภัย

- ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุล่วงละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในคณะฯ ต่อผู้บังคับบัญชา หรืองานเทคโนโลยีสารสนเทศ ทันทีที่พบเหตุล่วงละเมิดนั้น เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องดำเนินการแก้ไขปัญหาอย่างทันท่วงที

- ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อ Helpdesk หรือ งานเทคโนโลยีสารสนเทศที่เกี่ยวข้องทันที
- ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใดๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อ Helpdesk หรือ งานเทคโนโลยีสารสนเทศที่เกี่ยวข้องทันที
- ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในคณะฯ ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา และงานเทคโนโลยีสารสนเทศ และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศนั้นด้วยตนเอง

2.5.3 การกระทำอื่นๆ ที่ถือเป็นข้อห้ามของคณะฯ

การกระทำต่างๆ ที่กล่าวถึงด้านล่างนี้ถือเป็นข้อห้ามของคณะฯ ซึ่งคณะฯ ไม่ยินยอมให้พนักงานดำเนินการโดยเด็ดขาด คณะฯ ไม่ได้เขียนระบุถึงข้อห้ามทั้งหมดที่ห้ามกระทำไว้แต่เขียนเพื่อเป็นแนวทางให้แก่ผู้ใช้งานได้รับทราบเท่านั้น

<u>หมายเหตุ</u>: พนักงานบางส่วนอาจได้รับยกเว้นจากข้อห้ามที่กล่าวไว้ด้านล่างนี้ ถ้าเป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย เช่น ผู้ดูแลระบบสามารถระงับการเข้าถึงระบบเครือข่ายของอุปกรณ์ใดๆ หากการเข้าถึงนั้นรบกวนการทำงานของระบบเทคโนโลยีสารสนเทศของคณะฯ

- การใช้งานทรัพยากรของคณะฯ เพื่อการจัดหาหรือส่งต่อ วัสดุ เอกสาร หรือรูปภาพลามกอนาจาร หรือที่ขัดต่อกฎหมาย
- การฉ้อโกงโดยใช้ User account ของคณะฯ เพื่อเสนอขายสินค้า หรือบริการใด ๆ
- การให้การรับรองสิ่งใด ๆ ทั้งโดยตรงหรือโดยนัย เว้นแต่การรับรองนั้นเป็นส่วนหนึ่งของหน้าที่ที่ได้รับมอบหมาย
- การพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่าย ตัวอย่างของการล่วงละเมิดความมั่นคงปลอดภัย ได้แก่ การเข้าถึงข้อมูลหรือเครื่องเซิร์ฟเวอร์ที่ตนไม่ได้รับอนุญาต เป็นต้น ส่วนตัวอย่างของการรบกวนการทำงานของระบบเครือข่าย ได้แก่ Sniffing, Pinged Floods, Packet Spoofing, Denial of Service และ Forged Routing Information ด้วยเจตนามุ่งร้าย เป็นต้น
- การใช้งาน Bandwidth จำนวนมาก โดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P file sharing
- การทำ Port Scanning และ Security Scanning เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
- การดักฟังหรือดักจับข้อมูลที่พนักงานไม่ได้รับอนุญาตให้รับรู้ด้วยวิธีการใดๆ เว้นแต่ เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
- การค้นหาจุดบกพร่องของระบบ เพื่อทำการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต
- การหลบเลี่ยงการพิสูจน์ตัวตนผู้ใช้งานหรือมาตรการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ ระบบเครือข่ายใดๆ
- การใช้โปรแกรม/สคริปต์/คำสั่ง หรือการส่งข้อความใดๆ โดยมีเจตนารบกวน ลดประสิทธิภาพการให้บริการ หรือระงับการใช้งานของผู้ใช้งาน ทั้งโดยผ่านระบบเครือข่ายภายใน หรือผ่านระบบเครือข่ายต่างๆ

- การให้ข้อมูลลับ หรือข้อมูลส่วนบุคคล เกี่ยวกับรายชื่อพนักงาน รายชื่อผู้รับบริการ ความลับทางการค้าของคณะฯ และข้อมูลลับอื่น ๆ แก่บุคคลภายนอก
- การข่มขู่คุกคามทุกรูปแบบผ่านทางอีเมล โทรศัพท์ หรือระบบส่งข้อความ ไม่ว่าจะด้วยภาษา ความถี่ หรือขนาดของข้อความ
- การแสดงความคิดเห็น หรือส่งข้อความใดๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจำนวนมาก (Newsgroup Spam)
- การละเมิดสิทธิส่วนบุคคล ลิขสิทธิ์ของคณะฯ ความลับทางการค้า สิทธิบัตร ทรัพย์สินทางปัญญา หรือกฎหมายอื่นใด
- การ Check-in ใน Social Media เพื่อเข้าสถานที่ที่ต้องการความมั่นคงปลอดภัยและมีความอ่อนไหวสูงของคณะฯ เช่น ศูนย์คอมพิวเตอร์ (Data Center), ห้องควบคุมระบบเครือข่าย (Network Control Center), Strong Room เป็นต้น
- การ Post ข้อมูลของคณะฯ ที่มีชั้นความลับเป็น Secret, Confidential และ Internal Use Only ใน Social Media
- การแสดงความคิดเห็นใน Social Media เกี่ยวกับข้อมูลงบประมาณหรือข้อมูลด้านการเงินอื่น ๆ ของคณะฯ เช่น แผนการดำเนินงาน, รายงานผลประกอบการในอนาคตของคณะฯ เป็นต้น
- การแสดงความคิดเห็นหรือการอ้างอิงถึงใน Social Media เกี่ยวกับผู้รับบริการ ผู้ให้บริการภายนอก หรือ Supplier ของคณะฯ โดยมิได้รับอนุญาตเป็นลายลักษณ์อักษรจากบุคคลหรือคณะฯเหล่านั้น
- การดำเนินงานของคณะฯ กับผู้รับบริการ ผู้ให้บริการภายนอก หรือ Supplier ผ่าน Social Media ส่วนบุคคลของพนักงาน
- การลงทะเบียนเพื่อใช้งาน Social Media ในนามของคณะฯ