นโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ฉบับปี พ.ศ. 2569

งานสารสนเทศ
สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ฉบับปี พ.ศ. 2569

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)
ฉบับปี พ.ศ. 2569

1. บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสาร ได้เข้ามามีบทบาทสำคัญอย่างยิ่งต่อการดำเนินงานของสถาบัน ทั้งในด้านการบริหารจัดการและการให้บริการแก่ประชาชน อย่างไรก็ตามการขยายตัวของการใช้งานระบบเครือข่ายคอมพิวเตอร์ระบบคลาวด์ (Cloud Computing) และการปฏิบัติงานจากระยะไกล (Remote Work) ได้นำมาซึ่งความเสี่ยงและภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ ที่มีความซับซ้อนและรุนแรงมากขึ้น

เพื่อให้การใช้งานทรัพย์สินสารสนเทศของสถาบันเป็นไปอย่างมีประสิทธิภาพ มั่นคงปลอดภัย และสอดคล้องกับมาตรฐานสากล สถาบันจึงได้กำหนด "นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ" เพื่อใช้เป็นกรอบเกณฑ์มาตรฐานในการกำรดูแลรักษาความปลอดภัยของข้อมูล ระบบงาน และโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ

นโยบายฉบับนี้ จัดทำขึ้นโดยมุ่งเน้นการป้องกันการเข้าถึงข้อมูลโดยมิชอบ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ รวมถึงเพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

สถาบันมีความมุ่งมั่นที่จะสร้างวัฒนธรรมความปลอดภัยด้านสารสนเทศ โดยกำหนดให้ เจ้าหน้าที่ ทุกระดับตลอดจนบุคคลภายนอกที่เข้ามาปฏิบัติงานร่วมกับสถาบัน มีหน้าที่และความรับผิดชอบในการศึกษา ทำความเข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติฉบับนี้อย่างเคร่งครัด เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินและชื่อเสียงของสถาบัน และเพื่อให้การดำเนินภารกิจของสถาบันมีความต่อเนื่องและมั่นคงอย่างยั่งยืน

2. วัตถุประสงค์

2.1 เพื่อสร้างมาตรฐานความมั่นคงปลอดภัยสารสนเทศ โดยมีการกำหนดกรอบแนวทางและมาตรฐานในการบริหารจัดการเทคโนโลยีสารสนเทศ ระบบเครือข่าย และระบบคลาวด์ของสถาบัน ให้มีความมั่นคงปลอดภัยตามหลักสากล

2.2 เพื่อคุ้มครองทรัพย์สินสารสนเทศของสถาบัน ป้องกันการเข้าถึง การเปิดเผย การแก้ไขเปลี่ยนแปลง หรือการทำลายข้อมูลและระบบสารสนเทศโดยมิชอบ ซึ่งอาจก่อให้เกิดความเสียหายต่อการดำเนินงานและชื่อเสียงของสถาบัน

2.3 เพื่อกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ทุกระดับ ตั้งแต่ผู้บริหารระดับสูงสุดจนถึงเจ้าหน้าที่ผู้ปฏิบัติงาน ในการกำดูแลและรักษาความมั่นคงปลอดภัยสารสนเทศให้ตรวจสอบได้

2.4 เตรียมความพร้อมในการรับมือและระงับเหตุฉุกเฉินทางไซเบอร์ รวมถึงการกู้คืนระบบสารสนเทศให้สามารถกลับมาใช้งานได้ตามปกติอย่างรวดเร็วและมีประสิทธิภาพ

2.5 ส่งเสริมและสร้างความตระหนักรู้ด้านภัยคุกคามไซเบอร์ให้เจ้าหน้าที่มีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามรูปแบบใหม่ และมีวินัยในการใช้งานเทคโนโลยีสารสนเทศอย่างถูกต้องปลอดภัย

3. นิยามศัพท์

3.1 “สถาบัน” หมายถึง สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.2 “หัวหน้าสถาบัน” หมายถึง ผู้บริหารระดับสูง ภายในสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) เช่น ผู้อำนวยการ รองผู้อำนวยการ เป็นต้น

3.3 “ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) เช่น ผู้อำนวยการ รองผู้อำนวยการ ผู้อำนวยการสำนัก เป็นต้น

3.4 “ทรัพยากร (Resource)” หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศ ภายใต้การดูแลของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.5 “เครือข่ายคอมพิวเตอร์” หมายถึง เครือข่ายคอมพิวเตอร์ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.6 “ผู้ดูแลระบบ (System Administrator)” หมายถึง ผู้ซึ่งได้รับมอบหมายให้ทำหน้าที่ดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์

3.7 “บุคลากร” หมายถึง พนักงานและเจ้าหน้าที่ รวมถึง ลูกจ้าง หรือบุคคลอื่นที่ได้รับมอบหมายให้ปฏิบัติงานตามสัญญาของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.8 “ฝ่ายเทคโนโลยีสารสนเทศ” หมายถึง กลุ่มงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบ คอมพิวเตอร์ ระบบชุดคำสั่ง ชุดคำสั่งโปรแกรม และเครือข่ายในสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.9 “ผู้ใช้งานภายใน (Internal User)” หมายถึง บุคลากรภายในสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ที่มีบัญชีผู้ใช้งานที่ออกโดยฝ่ายเทคโนโลยีสารสนเทศ หรือ บุคคลหรือสถาบันภายนอกที่ได้รับอนุญาตให้ใช้เครือข่าย

3.10 “ผู้ใช้งานภายนอก (External User)” หมายถึง บุคลากรภายนอกที่สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) อนุญาตให้มีสิทธิในการเข้าถึงเครือข่ายและข้อมูล โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่และต้องรับผิดชอบในอำนาจหน้าที่ของตนเอง

3.11 “บัญชีผู้ใช้งาน (User Account)” หมายถึง บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบสารสนเทศ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบสารสนเทศ

3.12 “การพิสูจน์ตัวตน” หมายถึง ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

3.13 “สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

3.14 “แนวทางปฏิบัติ (Guideline)” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

3.15 “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

3.16 “ความมั่นคงปลอดภัยระบบสารสนเทศ” หมายถึง การรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมในการใช้งาน (Availability) ของเครือข่าย ระบบ และข้อมูลสารสนเทศ

3.17 “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ที่แสดงความเป็นไปได้ถึงความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

3.18 “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสถาบันถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

3.19 “หน้าจอภาพรวม (Desktop)” หมายถึง พื้นที่หน้าจอหลักของระบบคอมพิวเตอร์ที่ปรากฏหลังจากที่เปิดเครื่องคอมพิวเตอร์ เพื่อเข้าสู่ระบบของคอมพิวเตอร์

3.20 “ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

3.21 “สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

3.22 “ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

3.23 “ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายถึงระบบงานของสถาบันที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศ ที่สถาบันสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

3.24 “สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศ และการสื่อสารของสถาบัน เช่น อุปกรณ์ ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

3.25 “จดหมายอิเล็กทรอนิกส์ หรือ อีเมล (E-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน

3.26 “รหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการ ตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

3.27 “ระดับชั้นความลับ” หมายถึง การจัดหมวดหมู่ข้อมูลสารสนเทศตามความสำคัญและผลกระทบหากข้อมูลถูกเปิดเผย เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

ส่วนที่ 1 นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ
(Access Control Policy)

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อกำหนดหลักเกณฑ์และวิธีปฏิบัติในการเข้าถึงสารสนเทศและเครือข่ายคอมพิวเตอร์ของสถาบันให้มีความมั่นคงปลอดภัย

1.2 เพื่อป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศโดยมิชอบจากบุคคลที่ไม่มีสิทธิ์ปฏิบัติงาน

1.3 เพื่อบริหารจัดการสิทธิ์การใช้งานให้สอดคล้องกับบทบาท หน้าที่ และความรับผิดชอบของบุคลากร (Role-based Access Control) ทั้งระบบที่ติดตั้งภายใน (On-premise) และระบบคลาวด์ (Cloud Computing)

2. แนวทางปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ

2.1 การบริหารจัดการบัญชีผู้ใช้งาน (User Management)

2.1.1 การลงทะเบียนและยกเลิกบัญชีผู้ใช้งาน ผู้ดูแลระบบต้องจัดทำทะเบียนบัญชีผู้ใช้งานให้เป็นปัจจุบัน และต้องดำเนินการยกเลิกสิทธิ์การเข้าใช้งานทันทีเมื่อบุคลากรพ้นสภาพการเป็นเจ้าหน้าที่ หรือมีการเปลี่ยนแปลงหน้าที่ที่ไม่เกี่ยวข้องกับระบบเดิม

2.1.2 การตรวจสอบสิทธิ์การใช้งาน ต้องกำหนดให้มีการทบทวนสิทธิ์การเข้าถึงสารสนเทศของบุคลากรทุกระดับอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงโครงสร้างองค์กร

2.2 การกำหนดสิทธิ์ตามบทบาทหน้าที่ (Role-based Access Control: RBAC)

2.2.1 มีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศตามตำแหน่งงาน (Position-based) โดยผู้ใช้งานจะได้รับสิทธิ์เข้าถึงระบบต่างๆ (เช่น e-Office, e-Budget, Cloud Storage) ตามที่ระบุไว้ในตารางมาตรฐานสิทธิ์การเข้าถึง (Access Rights Matrix) ของสถาบัน

2.2.2 การมอบหมายสิทธิ์การเข้าถึงข้อมูลหรือการใช้งานระบบ ต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานตามหน้าที่เท่านั้น

2.2.3 ระบบที่มีความสำคัญสูงต้องมีการแยกหน้าที่ระหว่างผู้ขอใช้สิทธิ์ ผู้ตรวจสอบ และผู้อนุมัติสิทธิ์ เพื่อป้องกันการทุจริตหรือความผิดพลาด

2.2.4 การกำหนดอำนาจหน้าที่ในการอนุมัติสิทธิ์การเข้าใช้งานระบบสารสนเทศ

2.2.4.1 การขอสิทธิ์เข้าใช้งานใหม่ การขอเพิ่มสิทธิ์ หรือการขอแก้ไขสิทธิ์ในระบบสารสนเทศ ต้องได้รับการอนุมัติจากผู้บังคับบัญชาต้นสังกัดตั้งแต่ระดับผู้อำนวยการสำนักขึ้นไปเพื่อยืนยันความจำเป็นตามบทบาทหน้าที่ และต้องผ่านการตรวจสอบด้านเทคนิคจากฝ่ายเทคโนโลยีสารสนเทศหรือผู้ดูแลระบบก่อนดำเนินการทุกครั้ง

2.2.4.2 การจัดการสิทธิ์สำหรับการเข้าถึงข้อมูลที่มีระดับความลับตั้งแต่ระดับลับขึ้นไป หรือการมอบหมายสิทธิ์ในระดับผู้ดูแลระบบที่มีสิทธิ์สูงต้องได้รับการอนุมัติจากผู้อำนวยการสถาบันหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเป็นลายลักษณ์อักษรหรือผ่านระบบอนุมัติอิเล็กทรอนิกส์เท่านั้น เพื่อป้องกันความเสี่ยงและรักษาความมั่นคงปลอดภัยของข้อมูลสำคัญ

2.2.4.3 การอนุมัติสิทธิ์การเข้าถึงข้อมูลที่จำเพาะเจาะจงกับเนื้อหาของแต่ละระบบงานให้เป็นอำนาจหน้าที่ของผู้รับผิดชอบระบบงานหรือผู้ที่ได้รับมอบหมายให้ดูแลระบบงานนั้นๆ โดยต้องพิจารณาให้สิทธิ์เข้าถึงตามหลักการสิทธิ์ขั้นต่ำที่จำเป็นต่อการปฏิบัติงานเพื่อให้สอดคล้องกับภารกิจปัจจุบันของเจ้าหน้าที่

2.3 การควบคุมการเข้าถึงระบบสารสนเทศและระบบคลาวด์

2.3.1 มีการพิสูจน์ตัวตน (Authentication) การเข้าใช้งานระบบสารสนเทศและระบบคลาวด์ กลางของสถาบัน ต้องผ่านการพิสูจน์ตัวตนด้วยบัญชีผู้ใช้งานและรหัสผ่านตามมาตรฐานที่กำหนด หรือผ่านระบบการยืนยันตัวตนทางดิจิทัล (Digital ID)

2.3.2 มีการการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) เพื่อเข้าถึงระบบที่มีความสำคัญสูง หรือการเข้าถึงระบบคลาวด์จากภายนอกสถาบัน ผู้ใช้งานต้องผ่านการยืนยันตัวตนแบบหลายปัจจัย (MFA) ตามที่สถาบัน กำหนด

2.3.3 มีการจัดการสิทธิ์บนระบบคลาวด์ (Cloud Sharing Permission) สำหรับการแบ่งปันข้อมูลหรือโฟลเดอร์บนระบบคลาวด์ (เช่น Google Drive, OneDrive) ต้องกำหนดสิทธิ์ผู้เข้าถึงให้ชัดเจน และห้ามตั้งค่าเป็น "สาธารณะ" หรือ "ผู้ที่มีลิงก์ทุกคน" สำหรับข้อมูลที่มีชั้นความลับ

2.4 การเข้าถึงระบบสารสนเทศจากระยะไกล (Remote Access Control)

2.4.1 การเข้าถึงระบบภายในสถาบัน จากภายนอก ต้องกระทำผ่านช่องทางที่มั่นคงปลอดภัย เช่น Virtual Private Network (VPN) หรือการเชื่อมต่อผ่านโปรโตคอล HTTPS เท่านั้น

2.4.2 มีการบันทึกข้อมูลจราจรคอมพิวเตอร์ (Log Files) เพื่อใช้ในการตรวจสอบย้อนหลัง ทุกการเชื่อมต่อเข้าสู่ระบบจากระยะไกล

2.5 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

2.5.1 การควบคุมพื้นที่ควบคุมและห้องแม่ข่าย ห้ามมิให้ เจ้าหน้าที่ นำอาหาร เครื่องดื่ม และบุหรี่ เข้าไปในพื้นที่ห้องควบคุมระบบเครือข่าย ห้องแม่ข่าย (Server Room) หรือพื้นที่ที่ติดตั้งอุปกรณ์สารสนเทศที่สำคัญของ สถาบัน เพื่อป้องกันความเสียหายที่อาจเกิดจากสิ่งสกปรก ความชื้น และเป็นการลดความเสี่ยงต่อการเกิดเหตุอัคคีภัย

2.5.2 การบันทึกหลักฐานการเข้า-ออกพื้นที่ ให้ผู้ดูแลระบบจัดให้มีระบบบันทึกรายละเอียดการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศส่วนกลาง ทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อใช้เป็นหลักฐานประกอบการตรวจสอบย้อนหลัง (Audit Trail) ในกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย หรือพบปัญหาด้านการเข้าถึงข้อมูลโดยมิชอบ

2.5.3 การจัดการด้านอัคคีภัยและอุปกรณ์ดับเพลิง สถาบัน ต้องจัดให้มีอุปกรณ์ดับเพลิงที่มีคุณสมบัติเหมาะสมกับการใช้งานกับอุปกรณ์อิเล็กทรอนิกส์ ติดตั้งภายในอาคารและพื้นที่ปฏิบัติงานที่สำคัญ โดยอุปกรณ์ดังกล่าวต้องอยู่ในสภาพพร้อมใช้งานและได้รับการตรวจสอบตามรอบระยะเวลาที่กำหนดอย่างเคร่งครัด

2.5.4 การควบคุมพฤติกรรมและความปลอดภัยของพื้นที่ ห้ามกระทำการใดๆ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยทางกายภาพ เช่น การเปิดประตูพื้นที่ควบคุมหรือห้องแม่ข่ายค้างไว้โดยไม่มีผู้ดูแล และการนำบุคคลภายนอกเข้าสู่พื้นที่หวงห้ามต้องได้รับอนุมัติจากผู้รับผิดชอบพื้นที่ และต้องมีบุคลากรของสถาบันคอยกำกับดูแลตลอดเวลา

2.5.5 การควบคุมสภาพแวดล้อมทางเทคนิค ให้ฝ่ายเทคโนโลยีสารสนเทศดำเนินการจัดให้มีระบบควบคุมสภาพแวดล้อมภายในห้องแม่ข่ายอย่างเหมาะสม ประกอบด้วยระบบปรับอากาศเพื่อควบคุมอุณหภูมิและความชื้นให้อยู่ในเกณฑ์มาตรฐาน รวมถึงระบบสำรองไฟฟ้าที่มีประสิทธิภาพเพื่อให้ระบบสารสนเทศสามารถทำงานได้อย่างต่อเนื่องและมั่นคง

ส่วนที่ 2 การรักษาความมั่นคงปลอดภัยด้านบุคลากรและทรัพย์สิน
(Asset & Human Security)

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์และสื่อบันทึกข้อมูลทุกประเภทที่ใช้ในสถาบัน

1.2 เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครื่องคอมพิวเตอร์ส่วนบุคคลของบุคลากรให้มีความมั่นคงปลอดภัยและไม่ส่งผลกระทบต่อระบบสารสนเทศหลัก

1.3 เพื่อสร้างวินัยและความรับผิดชอบของบุคลากรในการดูแลรักษาทรัพย์สินสารสนเทศและป้องกันการรั่วไหลของข้อมูล

2. แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านบุคลากรและทรัพย์สิน

2.1 การรักษาความมั่นคงปลอดภัยด้านบุคลากร

2.1.1 ฝ่ายเทคโนโลยีสารสนเทศจะตรวจสอบประวัติและความเหมาะสมของบุคคลก่อนการมอบหมายสิทธิ์เข้าใช้งานระบบสารสนเทศที่มีความสำคัญสูง

2.1.2 บุคลากรต้องลงนามยอมรับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน และปฏิบัติตามอย่างเคร่งครัด

2.1.3 กรณีบุคลากรพ้นสภาพการเป็นเจ้าหน้าที่ หรือเปลี่ยนตำแหน่งงานที่ไม่มีความจำเป็นต้องเข้าถึงระบบเดิม ฝ่ายเทคโนโลยีสารสนเทศจะดำเนินการยกเลิกสิทธิ์และเรียกคืนอุปกรณ์ที่เป็นทรัพย์สินของสถาบัน ทันที

2.2 การควบคุมอุปกรณ์คอมพิวเตอร์พกพาและคอมพิวเตอร์ส่วนบุคคล (Bring Your Own Device: BYOD)

2.2.1 กำหนดให้มีการลงทะเบียนอุปกรณ์คอมพิวเตอร์พกพา เช่น Notebook, Tablet และเครื่องคอมพิวเตอร์ส่วนบุคคลก่อนนำมาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของสถาบัน เพื่อให้สามารถระบุตัวตนเจ้าของอุปกรณ์ได้อย่างถูกต้อง

2.2.2 อุปกรณ์คอมพิวเตอร์พกพาและคอมพิวเตอร์ส่วนบุคคลที่เข้าใช้งานระบบสารสนเทศของสถาบัน ต้องมีมาตรฐานความปลอดภัยขั้นต่ำ (Security Baseline) เช่น การติดตั้งโปรแกรมป้องกันไวรัสตามมาตรฐานที่สถาบันกำหนด การตั้งรหัสผ่านล็อกหน้าจอ และการเข้ารหัสข้อมูลสำคัญ

2.2.3 สถาบัน มีสิทธิ์จำกัดการเข้าถึงทรัพยากรบางประเภทสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เพื่อลดความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศส่วนกลาง

2.3 การจัดการทรัพย์สินสารสนเทศและสื่อบันทึกข้อมูล

2.3.1 มีการจัดทำทะเบียนทรัพย์สินสารสนเทศ (IT Asset Inventory) ให้เป็นปัจจุบัน โดยระบุประเภทอุปกรณ์ ผู้รับผิดชอบ และสถานที่จัดเก็บอย่างชัดเจน

2.3.2 การใช้งานสื่อบันทึกข้อมูลแบบพกพา (เช่น Flash Drive, External Hard Disk) ให้ฝ่ายเทคโนโลยีสารสนเทศกำหนดมาตรการและติดตั้งระบบตรวจสอบมัลแวร์อัตโนมัติ เพื่อสแกนข้อมูลทุกครั้งก่อนการใช้งาน โดย เจ้าหน้าที่ต้องปฏิบัติตามขั้นตอนการตรวจสอบอย่างเคร่งครัดเพื่อป้องกันการแพร่ระบาดของซอฟต์แวร์อันตรายเข้าสู่ระบบเครือข่ายของสถาบัน

2.3.3 กระบวนการทำลายข้อมูลในสื่อบันทึกข้อมูลอย่างถาวร (Secure Disposal and Sanitization) ก่อนการจำหน่าย บริจาค หรือทำลายซากอุปกรณ์ทรัพย์สินสารสนเทศ สถาบันต้องดำเนินการตามขั้นตอนดังนี้

2.3.3.1 การทำลายข้อมูลหรือสื่อบันทึกข้อมูลทุกประเภท ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาต้นสังกัด และได้รับการอนุมัติจาก ผู้อำนวยการสถาบัน หรือ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็นลายลักษณ์อักษรก่อนดำเนินการ เพื่อให้มั่นใจว่าข้อมูลดังกล่าวไม่มีความจำเป็นในการใช้งานหรือมีภาระผูกพันทางกฎหมายที่ต้องจัดเก็บต่อ

2.3.3.2 มาตรฐานการทำลายและหลักฐานการดำเนินงาน ต้องดำเนินการทำลายข้อมูลตามมาตรฐานเพื่อป้องกันการกู้คืนข้อมูล และมีการบันทึกหลักฐานการดำเนินงาน (Certificate of Destruction) หรือรายงานสรุปผลการทำลาย โดยมีรายละเอียดตามแต่ละชนิดสื่อ ดังนี้

1) สื่อประเภทกระดาษ ให้ดำเนินการทำลายด้วยเครื่องทำลายเอกสาร (Shredder) ในลักษณะที่ไม่สามารถนำกลับมาต่อรวมกันเพื่ออ่านเนื้อหาได้

2) สื่อบันทึกข้อมูลประเภทแม่เหล็ก (Hard Disk Drive - HDD) ให้ดำเนินการลบข้อมูลด้วยวิธีการเขียนทับ (Overwriting) อย่างน้อย 3 รอบด้วยโปรแกรมมาตรฐาน หรือใช้วิธีการทำลายอำนาจแม่เหล็ก (Degaussing) หรือการทำลายสภาพทางกายภาพ (Physical Destruction) เช่น การเจาะรูหรือบดทำลาย

3) สื่อบันทึกข้อมูลประเภท Solid State (SSD / Flash Drive / Memory Card) ให้ดำเนินการทำลายด้วยคำสั่ง Cryptographic Erase หรือการทำลายสภาพทางกายภาพในลักษณะที่แผ่นวงจรหลักแตกหักเสียหายอย่างถาวร

4) ข้อมูลบนระบบคลาวด์ (Cloud Storage) ต้องตรวจสอบให้มั่นใจว่าได้ลบข้อมูลออกจากพื้นที่จัดเก็บหลักและถังขยะรีไซเคิล (Trash/Bin) ของระบบคลาวด์แบบถาวรแล้ว รวมถึงการยกเลิกสิทธิ์การเข้าถึงของผู้ที่เกี่ยวข้องทั้งหมด

2.4 การควบคุมสภาพแวดล้อมทางกายภาพและพื้นที่ปฏิบัติงาน

2.4.1 เจ้าหน้าที่ต้องจัดเก็บเอกสารที่มีความสำคัญหรือมีชั้นความลับไว้ในตู้เอกสารที่มิดชิดและล็อกกุญแจทุกครั้งเมื่อไม่ได้อยู่ที่โต๊ะทำงาน

2.4.2 มีการตั้งค่าการล็อกหน้าจอคอมพิวเตอร์อัตโนมัติ (Screen Saver with Password) เมื่อไม่มีกิจกรรมการใช้งานตามระยะเวลาที่กำหนด เพื่อป้องกันผู้อื่นเข้าถึงข้อมูลบนหน้าจอโดยมิชอบ

2.4.3 ห้ามจดบันทึกชื่อผู้ใช้งานหรือรหัสผ่านติดไว้ที่เครื่องคอมพิวเตอร์ โต๊ะทำงาน หรือสถานที่ที่บุคคลอื่นสามารถสังเกตเห็นได้ง่าย

2.5 การจัดชั้นความลับและการจัดการข้อมูล

2.5.1 เกณฑ์การแบ่งชั้นความลับ

สถาบันกำหนดเกณฑ์การแบ่งชั้นความลับของข้อมูลสารสนเทศตามระดับความสำคัญและผลกระทบหากข้อมูลถูกเปิดเผยโดยมิชอบ ออกเป็น 4 ระดับ ดังนี้

- ลับมาก (Restricted) หมายถึง ข้อมูลที่มีความสำคัญสูงสุดของสถาบัน ซึ่งหากมีการเปิดเผยต่อบุคคลภายนอก หรือถูกนำไปใช้ในทางมิชอบ จะก่อให้เกิดความเสียหายต่อสถาบันอย่างร้ายแรงที่สุด
- ลับ (Confidential) หมายถึง ข้อมูลที่มีความสำคัญสูง ซึ่งหากเปิดเผยต่อผู้ที่ไม่มีส่วนเกี่ยวข้องจะส่งผลกระทบต่อการดำเนินงาน ชื่อเสียง หรือพันธกิจของสถาบันอย่างมีนัยสำคัญ
- จำกัดการเผยแพร่ (Internal Use) หมายถึง ข้อมูลที่ใช้สำหรับการปฏิบัติงานภายในสถาบันตามหน้าที่ความรับผิดชอบ ซึ่งไม่เปิดเผยต่อสาธารณะโดยทั่วไปแต่ไม่ถึงขั้นเป็นความลับระดับสูง
- สาธารณะ (Public) หมายถึง ข้อมูลที่สถาบันจัดทำขึ้นเพื่อเผยแพร่ต่อพนักงาน บุคคลภายนอก หรือประชาชนทั่วไป โดยไม่มีผลกระทบต่อสถาบันหากมีการเผยแพร่

ระดับความลับ	การจำกัดสิทธิ์	การจัดเก็บ / รับส่ง	การทำลาย
ลับมาก	เฉพาะผู้บริหารสูงสุดหรือผู้ได้รับอนุญาตเท่านั้น	เข้ารหัสลับข้อมูล (Encryption) และจัดเก็บในระบบที่มั่นคงสูงสุด	ทำลายทางกายภาพหรือล้างข้อมูลด้วยเทคนิคพิเศษ
ลับ	เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องตามหน้าที่ (RBAC)	จัดเก็บในระบบเครือข่ายภายในที่มีการควบคุมการเข้าถึง	ทำลายด้วยเครื่องทำลายเอกสารหรือโปรแกรมลบข้อมูลมาตรฐาน
จำกัดการเผยแพร่	เจ้าหน้าที่ของสถาบันทุกคน	ใช้ช่องทางสื่อสารปกติของสถาบัน (e-Office/Internal Mail)	ลบข้อมูลตามรอบระยะเวลาการจัดเก็บที่กำหนด
สาธารณะ	บุคคลทั่วไปและผู้มาติดต่อ	เผยแพร่ผ่านเว็บไซต์หรือสื่อประชาสัมพันธ์ของสถาบัน	ตามระเบียบงานสารบรรณทั่วไป

ส่วนที่ 3 การบริหารจัดการรหัสผ่านและการยืนยันตัวตน
(Password and Identity Management)

1. **วัตถุประสงค์ของนโยบาย**

1.1 เพื่อกำหนดมาตรฐานการใช้งานรหัสผ่านและการยืนยันตัวตนที่มีความมั่นคงปลอดภัยสูงสำหรับบุคลากรทุกระดับ

1.2 เพื่อป้องกันการสวมสิทธิ์หรือการเข้าถึงระบบสารสนเทศโดยบุคคลที่ไม่ได้รับอนุญาต ซึ่งอาจก่อให้เกิดความเสียหายต่อข้อมูลของสถาบัน

1.3 เพื่อยกระดับมาตรฐานการพิสูจน์ตัวตนให้สอดคล้องกับเทคโนโลยีการยืนยันตัวตนทางดิจิทัลและระบบคลาวด์ในปัจจุบัน

2. แนวทางปฏิบัติในการบริหารจัดการรหัสผ่านและการยืนยันตัวตน

2.1 มาตรฐานการกำหนดรหัสผ่านและการรักษาความลับ

2.1.1 การกำหนดรหัสผ่านต้องมีความยาวอย่างน้อย 8 ตัวอักษร โดยประกอบด้วยตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข และอักขระพิเศษผสมกัน เพื่อเพิ่มความซับซ้อนและป้องกันการคาดเดารหัสผ่านจากผู้ไม่มีสิทธิเข้าใช้งาน

2.1.2 หลีกเลี่ยงการกำหนดรหัสผ่านโดยใช้ข้อมูลส่วนตัวที่เปิดเผยสาธารณะ เช่น ชื่อผู้ใช้งาน วันเดือนปีเกิด หรือหมายเลขโทรศัพท์ รวมถึงห้ามบันทึกรหัสผ่านไว้ในเครื่องคอมพิวเตอร์หรือจดไว้ในที่เปิดเผยที่บุคคลอื่นสามารถเข้าถึงได้

2.1.3 ในระหว่างการพิมพ์รหัสผ่านเพื่อเข้าใช้งานระบบ ระบบสารสนเทศต้องมีการปิดบังรหัสผ่านด้วยการแสดงสัญลักษณ์แทนตัวอักษรจริง เพื่อป้องกันการล่วงรู้รหัสผ่านจากบุคคลรอบข้าง

2.2 การยืนยันตัวตนแบบหลายปัจจัยและการใช้ Digital ID

2.2.1 ส่งเสริมการนำระบบการยืนยันตัวตนทางดิจิทัล (Digital ID) มาใช้เป็นมาตรฐานหลักในการเชื่อมต่อและเข้าใช้งานแพลตฟอร์มสำคัญของสถาบัน เพื่อความถูกต้องแม่นยำในการระบุตัวบุคคล

2.2.2 กำหนดให้การเข้าถึงระบบสารสนเทศจากระยะไกล (Remote Access) หรือการเข้าใช้งานระบบคลาวด์ที่มีความสำคัญสูง ต้องผ่านการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) เพิ่มเติมจากการใช้รหัสผ่านปกติ เพื่อยกระดับความปลอดภัย

2.2.3 เจ้าหน้าที่ผู้ครอบครองอุปกรณ์หรือข้อมูลที่ใช้ในการยืนยันตัวตนชั้นที่สอง เช่น รหัส OTP หรือแอปพลิเคชันยืนยันตัวตน ต้องดูแลรักษาอุปกรณ์ดังกล่าวเสมือนเป็นทรัพย์สินสำคัญและไม่แบ่งปันสิทธิ์การใช้งานให้ผู้อื่น

2.3 การกำกับดูแลบัญชีผู้ใช้งานและรอบการเปลี่ยนแปลง

2.3.1 ผู้ดูแลระบบที่มีสิทธิ์สูง (Privileged Account) ต้องดำเนินการเปลี่ยนรหัสผ่านอย่างน้อยทุก 90 วัน และสำหรับผู้ใช้งานทั่วไปควรเปลี่ยนรหัสผ่านเมื่อตรวจพบความเสี่ยงหรือตามรอบที่สถาบัน กำหนด เพื่อลดโอกาสในการเข้าถึงระบบโดยมิชอบ

2.3.2 ระบบสารสนเทศต้องมีการตั้งค่าให้ล็อกบัญชีผู้ใช้งานชั่วคราวอัตโนมัติ ในกรณีที่มีการพยายามเข้าสู่ระบบด้วยรหัสผ่านที่ผิดติดต่อกันเกินกว่าที่กำหนด เพื่อป้องกันการโจมตีในลักษณะการสุ่มรหัสผ่าน

2.3.3 เมื่อมีการตรวจพบหรือสงสัยว่ารหัสผ่านถูกเปิดเผยหรือถูกล่วงรู้โดยบุคคลอื่น เจ้าหน้าที่ต้องดำเนินการเปลี่ยนรหัสผ่านใหม่ทันทีและรายงานเหตุการณ์ผิดปกติให้ฝ่ายเทคโนโลยีสารสนเทศทราบเพื่อดำเนินการตรวจสอบต่อไป

ส่วนที่ 4 ความมั่นคงปลอดภัยของระบบเครือข่ายและระบบคลาวด์
(Network and Cloud Security)

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อกำหนดมาตรฐานในการบริหารจัดการระบบเครือข่ายและบริการคลาวด์ของสถาบันให้มีความมั่นคงปลอดภัยและพร้อมใช้งานอย่างต่อเนื่อง

1.2 เพื่อควบคุมการเชื่อมต่อเข้าสู่ระบบสารสนเทศของสถาบันจากภายนอกให้เป็นไปตามมาตรฐานความปลอดภัยขั้นสูง

1.3 เพื่อป้องกันการบุกรุก การโจมตีระบบ หรือการดักรับข้อมูลจราจรคอมพิวเตอร์จากผู้ไม่มีสิทธิเข้าใช้งาน

2. แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายและระบบคลาวด์

2.1 การบริหารจัดการและควบคุมระบบเครือข่าย

2.1.1 จัดให้มีการแบ่งส่วนเครือข่าย (Network Segmentation) เพื่อแยกกลุ่มระบบสารสนเทศที่มีความสำคัญสูงออกจากเครือข่ายทั่วไป รวมถึงการจำกัดการเชื่อมต่อระหว่างระบบงานภายในกับระบบคลาวด์ให้เป็นไปตามความจำเป็นเท่านั้น

2.1.2 เจ้าหน้าที่ผู้ดูแลระบบต้องดำเนินการติดตั้งและปรับปรุงอุปกรณ์ป้องกันเครือข่าย (เช่น Firewall หรือระบบป้องกันการบุกรุก) ให้เป็นปัจจุบัน เพื่อทำหน้าที่คัดกรองเฉพาะข้อมูลจราจรที่ได้รับอนุญาตให้เข้า-ออกระบบของสถาบัน

2.1.3 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำและปรับปรุงแผนผังระบบเครือข่าย (Network Diagram) ให้เป็นปัจจุบันอยู่เสมอ โดยแผนผังต้องระบุขอบเขตของเครือข่ายภายในสถาบันและเครือข่ายภายนอกอย่างชัดเจน รวมถึงการระบุตำแหน่งของอุปกรณ์สำคัญ เช่น Switch, Router และจุดกระจายสัญญาณไร้สาย (Access Point) ทั้งนี้ ต้องมีการแยกส่วนเครือข่ายไร้สายสำหรับเจ้าหน้าที่ และผู้มาติดต่อออกจากกัน โดยเครือข่ายของเจ้าหน้าที่ต้องผ่านการพิสูจน์ตัวตนก่อนเข้าใช้งานทุกครั้ง

2.1.4 นักเทคโนโลยีสารสนเทศ มีหน้าที่ตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารทุกชนิดก่อนอนุญาตให้เชื่อมต่อกับเครือข่ายภายในของสถาบัน เช่น การตรวจสอบไวรัสและค่าคุณลักษณะ (Parameter) เบื้องต้น นอกจากนี้ต้องดำเนินการปิดจุดเชื่อมต่อการให้บริการ (Disable Port) หรือตัดการเชื่อมต่อทางกายภาพสำหรับจุดที่ไม่มีความจำเป็นต้องใช้งานเครือข่ายโดยสิ้นเชิง เพื่อลดพื้นที่การโจมตี (Attack Surface) ของสถาบัน

2.1.5 สถาบันต้องกำหนดตัวบุคคลหรือกลุ่มงานผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าคุณลักษณะ (Parameter) ของอุปกรณ์เครือข่ายอย่างชัดเจน โดยต้องมีการทบทวนค่าดังกล่าวอย่างน้อยปีละ 1 ครั้ง และต้องแจ้งผู้ใช้งานที่เกี่ยวข้องทราบทุกครั้งที่มีการเปลี่ยนแปลงสำคัญ ทั้งนี้ การเปลี่ยนแปลงโครงสร้างหลักหรือค่าที่มีผลกระทบสูงต้องผ่านการตรวจสอบโดย นักเทคโนโลยีสารสนเทศ และได้รับความเห็นชอบจากผู้อำนวยการสำนักยุทธศาสตร์และสารสนเทศก่อนดำเนินการ

2.2 มาตรฐานความปลอดภัยบนระบบคลาวด์ (Cloud Security)

2.2.1 การเลือกใช้บริการคลาวด์จากผู้ให้บริการภายนอก สถาบันต้องตรวจสอบมาตรฐานด้านความปลอดภัยของผู้ให้บริการเพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศตามมาตรฐานสากลหรือตามที่กฎหมายกำหนด

2.2.2 การบริหารจัดการความปลอดภัยบนระบบคลาวด์ให้ถือหลักความรับผิดชอบร่วมกัน โดยสถาบันรับผิดชอบการกำหนดสิทธิ์เข้าใช้งานและการตั้งค่าความปลอดภัยของข้อมูล ส่วนผู้ให้บริการรับผิดชอบความปลอดภัยของโครงสร้างพื้นฐานระบบ

2.2.3 เจ้าหน้าที่ต้องไม่จัดเก็บข้อมูลที่มีชั้นความลับสูงบนระบบคลาวด์สาธารณะโดยไม่มีการเข้ารหัสข้อมูล (Encryption) และต้องกำหนดสิทธิ์การเข้าถึงข้อมูลให้เฉพาะเจาะจงแก่ผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้น

2.3 การเชื่อมต่อระบบสารสนเทศจากระยะไกล (Remote Access)

2.3.1 การเข้าใช้งานระบบสารสนเทศหรือทรัพยากรบนคลาวด์ของสถาบันผ่านเครือข่ายสาธารณะหรือจากภายนอกที่ทำงาน ต้องกระทำผ่านช่องทางที่มีการเข้ารหัสข้อมูลที่มั่นคงปลอดภัย เช่น Virtual Private Network (VPN) หรือมาตรฐาน HTTPS เท่านั้น

2.3.2 ในขณะปฏิบัติงานจากภายนอก เจ้าหน้าที่ต้องหลีกเลี่ยงการเชื่อมต่อผ่านระบบเครือข่ายไร้สายสาธารณะที่ไม่มีการเข้ารหัสผ่าน และต้องมั่นใจว่าอุปกรณ์ที่ใช้เชื่อมต่อมีการติดตั้งโปรแกรมป้องกันไวรัสและได้รับการปรับปรุงระบบปฏิบัติการให้เป็นปัจจุบัน

2.3.3 ระบบการเข้าถึงจากระยะไกลต้องมีการตั้งค่าการตัดการเชื่อมต่ออัตโนมัติ (Session Time-out) เมื่อไม่มีกิจกรรมการใช้งานภายในระยะเวลาที่กำหนด เพื่อลดความเสี่ยงจากการค้างหน้าจอระบบไว้ในพื้นที่ที่ไม่ปลอดภัย

2.4 การเฝ้าระวังและตรวจสอบความปลอดภัยเครือข่าย

2.4.1 จัดให้มีระบบการเฝ้าระวังภัยคุกคามและการตรวจจับพฤติกรรมที่ผิดปกติบนระบบเครือข่ายและระบบคลาวด์ เพื่อให้สามารถยับยั้งเหตุการณ์ละเมิดความมั่นคงปลอดภัยได้อย่างทันท่วงที

2.4.2 เจ้าหน้าที่ผู้ดูแลระบบต้องตรวจสอบความเปราะบางของระบบเครือข่าย (Vulnerability Assessment) อย่างสม่ำเสมอ เพื่อนำผลมาปรับปรุงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของสถาบันให้แข็งแกร่งและลดช่องโหว่จากการถูกโจมตีทางไซเบอร์

ส่วนที่ 5 การจัดเก็บข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ (Log Management & Audit)

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อให้การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ของสถาบันเป็นไปตามที่กฎหมายกำหนด และสามารถใช้เป็นหลักฐานในการตรวจสอบข้อเท็จจริงเมื่อเกิดเหตุละเมิดความมั่นคงปลอดภัย

1.2 เพื่อเฝ้าระวังและติดตามพฤติกรรมการเข้าใช้งานระบบสารสนเทศของเจ้าหน้าที่ให้เป็นไปตามนโยบายและแนวปฏิบัติที่สถาบันกำหนด

1.3 เพื่อสร้างระบบการตรวจสอบ (Audit Trail) ที่มีความน่าเชื่อถือและป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลเหตุการณ์ที่เกิดขึ้นในระบบ

2. แนวทางปฏิบัติในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ

2.1 การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Retention)

2.1.1 สถาบันต้องจัดให้มีการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ (Log Files) ที่เกิดขึ้นจากเครือข่ายคอมพิวเตอร์ของสถาบัน เครื่องแม่ข่าย และระบบคลาวด์ ไว้ไม่น้อยกว่า 90 วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

2.1.2 ในกรณีที่มีเหตุจำเป็นหรือได้รับการประสานงานจากหน่วยงานบังคับใช้กฎหมาย สถาบันอาจพิจารณาขยายระยะเวลาการจัดเก็บข้อมูลจราจรคอมพิวเตอร์เฉพาะรายตามความเหมาะสมแต่ไม่เกินระยะเวลาที่กฎหมายกำหนด

2.1.3 ข้อมูลจราจรที่จัดเก็บต้องครอบคลุมรายละเอียดที่สำคัญ เช่น วันเวลาที่มีการเข้าและออกระบบ (Login/Logout) หมายเลขไอพี (IP Address) ของอุปกรณ์ที่ใช้เชื่อมต่อ และข้อมูลบัญชีผู้ใช้งานที่สามารถระบุตัวบุคคล (Identification) ของเจ้าหน้าที่ผู้เข้าใช้งานระบบนั้นๆ ได้

2.2 การรักษาความมั่นคงปลอดภัยของข้อมูลจราจร

2.2.1 ข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บต้องมีการป้องกันการเข้าถึงจากผู้ไม่มีสิทธิเข้าใช้งาน และต้องมีมาตรการป้องกันการแก้ไข ลบทิ้ง หรือเปลี่ยนแปลงข้อมูล เพื่อรักษาความถูกต้องแท้จริงของข้อมูลจราจร (Log Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

2.2.2 กำหนดให้มีการสำรองข้อมูลจราจรคอมพิวเตอร์อย่างสม่ำเสมอและจัดเก็บไว้ในพื้นที่ที่มั่นคงปลอดภัยแยกต่างหากจากระบบงานหลัก เพื่อป้องกันความสูญเสียในกรณีที่ระบบเกิดความขัดข้อง

2.2.3 การเข้าถึงข้อมูลจราจรคอมพิวเตอร์เพื่อการตรวจสอบ ต้องได้รับอนุมัติจากผู้บริหารที่ได้รับมอบหมาย และต้องมีการบันทึกเหตุการณ์การเข้าถึงข้อมูลดังกล่าวไว้เป็นหลักฐานทุกครั้ง

2.3 การตรวจสอบระบบสารสนเทศ (Information Systems Audit)

2.3.1 สถาบันจัดให้มีการตรวจสอบเหตุการณ์ที่ผิดปกติหรือพฤติกรรมที่มีความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ โดยเจ้าหน้าที่ผู้ดูแลระบบต้องรายงานเหตุการณ์ผิดปกติให้ผู้บริหารทราบโดยเร็ว

2.3.2 จัดให้มีการสอบทานสิทธิ์การเข้าใช้งานระบบสารสนเทศของเจ้าหน้าที่ (Access Rights Review) เพื่อตรวจสอบว่าสิทธิ์ที่ได้รับยังมีความสอดคล้องกับบทบาทหน้าที่ปัจจุบัน และดำเนินการปรับปรุงสิทธิ์ให้ถูกต้องหากพบความไม่สอดคล้อง

2.3.3 สถาบันอาจจัดให้มีการตรวจสอบความปลอดภัยโดยหน่วยงานภายนอกหรือผู้เชี่ยวชาญ เพื่อประเมินประสิทธิภาพของมาตรการควบคุมและนำข้อเสนอแนะมาปรับปรุงนโยบายให้ทันสมัยและมีประสิทธิภาพยิ่งขึ้น

2.4 การซิงโครไนซ์เวลาของระบบ (Clock Synchronization)

เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และระบบบันทึก Log ทุกประเภทของสถาบัน ต้องมีการตั้งค่าเวลาให้ตรงกันโดยอ้างอิงจากแหล่งกำเนิดเวลามาตรฐาน (Network Time Protocol: NTP) เพื่อให้ข้อมูลจราจรคอมพิวเตอร์มีความถูกต้องแม่นยำในการอ้างอิงลำดับเหตุการณ์

2.4.1 ในการเก็บข้อมูลจราจร ต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้ (Identification and Authentication) เช่น Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ Wi-Fi Hotspot เป็นต้น ต้องสามารถระบุตัวตนของผู้ใช้งานเป็นรายบุคคลได้จริง

2.4.2 สถาบันจะเก็บรักษาจราจรคอมพิวเตอร์ตามกำหนดเวลา ดังต่อไปนี้

1) กรณีทั่วไป สถาบันจะเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับตั้งแต่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

2) กรณีจำเป็น เมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามประกาศหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 หรือเพื่อประโยชน์ในการรวบรวมข้อเท็จจริงและหลักฐานเกี่ยวกับการกระทำความผิดที่เกี่ยวข้องกับความมั่นคงแห่งราชอาณาจักร การก่อการร้าย องค์กรอาชญากรรมข้ามชาติ หรือความสงบเรียบร้อยของประชาชน ซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบ หรือเป็นส่วนหนึ่งในการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิด ไม่ว่าข้อเท็จจริงในเหตุแห่งความจำเป็นดังกล่าวปรากฏต่อพนักงานเจ้าหน้าที่นั้นเอง หรือเมื่อได้รับการร้องขอจากเจ้าหน้าที่ผู้รับผิดชอบในการสืบสวนหรือสอบสวนก่อนครบกำหนดเวลาตาม (1) ให้พนักงานเจ้าหน้าที่มีคำสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ใช้บริการเป็นกรณีพิเศษ เฉพาะรายต่อไปอีกคราวละไม่เกิน 6 เดือนต่อเนื่องกัน แต่ต้องไม่เกิน 2 ปี

ส่วนที่ 6 การปฏิบัติงานจากภายนอกและการใช้งานสื่อออนไลน์
(Remote Work & Communication)

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อกำหนดมาตรฐานความปลอดภัยสำหรับการปฏิบัติงานนอกสถานที่ของเจ้าหน้าที่ ให้มีความมั่นคงปลอดภัยเทียบเท่ากับการปฏิบัติงานภายในสถาบัน

1.2 เพื่อป้องกันการรั่วไหลของข้อมูลสถาบันผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์และสื่อสังคมออนไลน์

1.3 เพื่อให้เจ้าหน้าที่มีแนวทางปฏิบัติที่ถูกต้องในการใช้เครื่องมือสื่อสารของสถาบัน เพื่อรักษาภาพลักษณ์และความน่าเชื่อถือขององค์กร

2. แนวทางปฏิบัติในการปฏิบัติงานจากภายนอกและการใช้งานสื่อออนไลน์

2.1 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

2.1.1 การเข้าปฏิบัติงานจากระยะไกล บุคลากรต้องเชื่อมต่อผ่านเครือข่ายเสมือนส่วนตัว (Virtual Private Network: VPN) การเชื่อมต่อผ่านโปรโตคอลที่มีการเข้ารหัส (เช่น HTTPS) หรือช่องทางที่สถาบันกำหนดเท่านั้น เพื่อให้การรับส่งข้อมูลมีการเข้ารหัสและป้องกันการดักรับข้อมูลจากบุคคลภายนอก

2.1.2 ในขณะปฏิบัติงานในพื้นที่สาธารณะ เจ้าหน้าที่ต้องระมัดระวังการมองเห็นหน้าจอคอมพิวเตอร์จากบุคคลรอบข้าง และต้องมั่นใจว่าอุปกรณ์ที่ใช้ไม่อยู่ในลักษณะที่เสี่ยงต่อการถูกลักขโมยหรือถูกเข้าถึงโดยผู้ไม่มีสิทธิเข้าใช้งาน

2.1.3 ห้ามเจ้าหน้าที่เชื่อมต่อระบบสารสนเทศของสถาบันผ่านเครือข่ายไร้สายสาธารณะ (Public Wi-Fi) ที่ไม่มีการป้องกันด้วยรหัสผ่าน ในกรณีที่จำเป็นต้องใช้งาน ควรเชื่อมต่อผ่านจุดกระจายสัญญาณส่วนบุคคล (Personal Hotspot) ที่มีการตั้งรหัสผ่านที่มั่นคงปลอดภัย

2.2 การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail Security)

2.2.1 เจ้าหน้าที่ต้องใช้บัญชีจดหมายอิเล็กทรอนิกส์ที่สถาบันจัดสรรให้ในการติดต่อประสานงานเรื่องราชการหรือธุรกิจของสถาบัน และห้ามใช้บัญชีดังกล่าวในการสมัครบริการส่วนตัวที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

2.2.2 ให้ระมัดระวังการเปิดเอกสารแนบหรือคลิกลิงก์จากจดหมายอิเล็กทรอนิกส์ที่ไม่ทราบแหล่งที่มาแน่ชัด เพื่อป้องกันภัยคุกคามประเภทการหลอกลวงทางอินเทอร์เน็ต (Phishing) และมัลแวร์เรียกค่าไถ่ (Ransomware)

2.2.3 การส่งข้อมูลที่มีชั้นความลับผ่านจดหมายอิเล็กทรอนิกส์ ต้องดำเนินการเข้ารหัสไฟล์ข้อมูลหรือตั้งรหัสผ่านสำหรับเปิดเอกสาร และต้องตรวจสอบที่อยู่ผู้รับให้ถูกต้องก่อนกดส่งข้อมูลทุกครั้ง

2.3 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ (Social Media Policy)

2.3.1 เจ้าหน้าที่ต้องใช้งานอินเทอร์เน็ตเพื่อประโยชน์ในการปฏิบัติงานตามหน้าที่ และต้องไม่ใช้เพื่อการเผยแพร่ข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ หรือกระทบต่อความมั่นคงปลอดภัยของสถาบัน

2.3.2 การแสดงความคิดเห็นหรือการให้ข้อมูลผ่านสื่อสังคมออนไลน์ในนามส่วนตัว เจ้าหน้าที่ต้องระมัดระวังไม่ให้เกิดความเข้าใจผิดว่าเป็นความเห็นหรือจุดยืนทางการของสถาบัน และห้ามนำข้อมูลภายในที่ยังไม่ได้ประกาศอย่างเป็นทางการไปเผยแพร่โดยเด็ดขาด

2.3.3 สถาบันสงวนสิทธิ์ในการตรวจสอบและคัดกรองการใช้งานอินเทอร์เน็ตของเจ้าหน้าที่ หากพบพฤติกรรมที่เสี่ยงต่อความเสียหายทางสารสนเทศหรือขัดต่อระเบียบปฏิบัติของสถาบัน

2.4 การรักษาความปลอดภัยของการประชุมทางไกล (Video Conference)

2.4.1 การจัดการประชุมผ่านระบบออนไลน์ที่มีเนื้อหาเป็นความลับ เจ้าหน้าที่ผู้จัดการประชุมต้องตั้งรหัสผ่านสำหรับการเข้าห้องประชุม (Meeting Password) และตรวจสอบรายชื่อผู้เข้าร่วมประชุมให้ตรงตามที่ได้รับอนุญาตเท่านั้น

2.4.2 ห้ามบันทึกภาพหน้าจอหรือวิดีโอการประชุมที่มีเนื้อหาสำคัญเพื่อนำไปเผยแพร่ภายนอก โดยไม่ได้รับอนุมัติจากประธานในที่ประชุมหรือผู้บริหารที่รับผิดชอบ

2.5 การตอบสนองต่อภัยคุกคามและความรับผิดชอบ (Incident Response and Liability)

2.5.1 สถาบันมีนโยบาย "ปฏิเสธการจ่ายเงินค่าไถ่ข้อมูล (No-Ransom Payment)" ในทุกกรณี หากเจ้าหน้าที่พบว่าเครื่องคอมพิวเตอร์ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware) ต้องหยุดการใช้งาน ตัดการเชื่อมต่อเครือข่ายทันที และแจ้งฝ่ายเทคโนโลยีสารสนเทศโดยเร็วที่สุด ห้ามเจ้าหน้าที่เจรจาหรือดำเนินการชำระเงินค่าไถ่ด้วยตนเองโดยเด็ดขาด

2.5.2 ค่าใช้จ่ายในการกู้คืนระบบหรือความเสียหายที่เกิดขึ้น หากตรวจสอบพบว่าเกิดจากการจงใจฝ่าฝืนนโยบาย หรือละเลยการแจ้งเตือนด้านความปลอดภัยของสถาบัน เจ้าหน้าที่ผู้กระทำผิดอาจต้องเข้าสู่กระบวนการพิจารณาโทษทางวินัย และรับผิดชอบความเสียหายที่เกิดขึ้นตามกฎหมาย

ส่วนที่ 7 การบริหารจัดการเหตุการณ์และภัยคุกคามไซเบอร์ (Incident Management)

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อกำหนดขั้นตอนและวิธีการตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบและรวดเร็ว

1.2 เพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นต่อระบบสารสนเทศและทรัพย์สินของสถาบันจากภัยคุกคามไซเบอร์

1.3 เพื่อให้เจ้าหน้าที่ทราบหน้าที่และช่องทางการรายงานเหตุการณ์ผิดปกติได้อย่างถูกต้องตามมาตรฐานที่สถาบันกำหนด

2. แนวทางปฏิบัติในการบริหารจัดการเหตุการณ์และภัยคุกคามไซเบอร์

2.1 การเฝ้าระวังและการรายงานเหตุการณ์ผิดปกติ

2.1.1 เจ้าหน้าที่ต้องให้ความสำคัญกับการสังเกตพฤติกรรมที่ผิดปกติของเครื่องคอมพิวเตอร์หรือระบบสารสนเทศที่ใช้งาน เช่น การทำงานที่ช้าลงอย่างผิดปกติ การปรากฏข้อความข่มขู่เรียกค่าไถ่ข้อมูล หรือการพบช่องโหว่ที่อาจนำไปสู่การบุกรุกระบบ

2.1.2 เมื่อเจ้าหน้าที่ตรวจพบหรือสงสัยว่าเกิดเหตุการณ์ละเมิดความมั่นคงปลอดภัย หรือพบว่าอุปกรณ์สารสนเทศของสถาบันสูญหาย เจ้าหน้าที่ต้องหยุดการเชื่อมต่อกับระบบที่บุกรุก และแจ้งต่อฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายโดยทันที เพื่อประเมินสถานการณ์และหาแนวทางแก้ไข

2.1.3 ห้ามเจ้าหน้าที่ดำเนินการแก้ไขปัญหาทางเทคนิคที่มีความซับซ้อนด้วยตนเองในลักษณะที่อาจทำลายหลักฐานทางดิจิทัล (Digital Evidence) เว้นแต่ได้รับคำแนะนำจากผู้เชี่ยวชาญหรือเจ้าหน้าที่ผู้ดูแลระบบ

2.2 ขั้นตอนการตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัย

2.2.1 เมื่อได้รับแจ้งเหตุ เจ้าหน้าที่ผู้ดูแลระบบต้องดำเนินการจำกัดวงความเสียหาย (Containment) เช่น การตัดการเชื่อมต่อระบบที่ถูกบุกรุกออกจากเครือข่าย เพื่อป้องกันการแพร่กระจายของมัลแวร์ไปยังส่วนอื่นของสถาบัน

2.2.2 จัดให้มีการวิเคราะห์สาเหตุของปัญหาและดำเนินการกำจัดภัยคุกคาม (Eradication) รวมถึงการกู้คืนระบบและข้อมูลจากแหล่งสำรองที่มั่นคงปลอดภัย เพื่อให้สถาบันสามารถกลับมาดำเนินงานได้ตามปกติโดยเร็วที่สุด

2.2.3 ในกรณีที่เป็นเหตุการณ์ร้ายแรงที่ส่งผลกระทบต่อข้อมูลส่วนบุคคลหรือความมั่นคงของสถาบัน ให้รายงานต่อผู้บริหารตามลำดับชั้นเพื่อพิจารณาแจ้งเหตุไปยังหน่วยงานกำกับดูแลภายนอกตามที่กฎหมายกำหนด

2.3 การบันทึกและเรียนรู้จากเหตุการณ์ (Post-Incident Activity)

2.3.1 ทุกเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องได้รับการบันทึกรายละเอียด ตั้งแต่ลักษณะของภัยคุกคาม วิธีการแก้ไข และผลกระทบที่เกิดขึ้น เพื่อใช้เป็นฐานข้อมูลในการป้องกันเหตุการณ์ในลักษณะเดียวกันในอนาคต

2.3.2 สถาบันควรนำกรณีศึกษาจากเหตุการณ์ที่เกิดขึ้นจริงมาใช้ในการสื่อสารและสร้างความตระหนักรู้แก่เจ้าหน้าที่ เพื่อให้เกิดความระมัดระวังและป้องกันการเกิดเหตุซ้ำ

2.4 การทดสอบกระบวนการตอบสนองต่อภัยคุกคาม

2.4.1 สถาบันจัดให้มีการทบทวนและทดสอบขั้นตอนการตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยอย่างสม่ำเสมอ เพื่อให้เจ้าหน้าที่ผู้เกี่ยวข้องมีความพร้อมในการปฏิบัติงานเมื่อเกิดสถานการณ์จริง

2.4.2 ปรับปรุงรายละเอียดในแนวทางการเผชิญเหตุให้สอดคล้องกับรูปแบบภัยคุกคามไซเบอร์ที่เปลี่ยนแปลงไป โดยเฉพาะภัยคุกคามที่มุ่งเป้าไปยังระบบคลาวด์และอุปกรณ์พกพาของเจ้าหน้าที่

2.4.3 สถาบันกำหนดให้มีการจำลองการโจมตีด้วยอีเมลหลอกลวง (Phishing Simulation Test) สำหรับบุคลากรอย่างน้อยปีละ 1 ครั้ง เพื่อประเมินความพร้อมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ 8 การสำรองข้อมูลและการกู้คืนระบบ
(Backup & Recovery)

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำคัญของสถาบันมีการสำรองไว้อย่างถูกต้อง ครบถ้วน และสามารถนำกลับมาใช้งานได้ทันทีเมื่อเกิดเหตุขัดข้อง

1.2 เพื่อลดความเสี่ยงจากการสูญเสียข้อมูลอันเนื่องมาจากความผิดพลาดของอุปกรณ์ ภัยพิบัติทางธรรมชาติ หรือการโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware)

1.3 เพื่อกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการบริหารจัดการข้อมูลสำรองทั้งในระบบเครือข่ายภายในและระบบคลาวด์

2. แนวทางปฏิบัติในการสำรองข้อมูลและการกู้คืนระบบ

2.1 การสำรองข้อมูลของสถาบัน (Data Backup)

2.1.1 เจ้าหน้าที่ผู้ดูแลระบบจัดทำและทบทวนแผนการสำรองข้อมูลสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อกำหนดรอบระยะเวลาการสำรองข้อมูลให้เหมาะสมกับระดับความสำคัญของข้อมูล ทั้งในระบบฐานข้อมูล เครื่องแม่ข่าย และระบบคลาวด์ โดยสถาบันต้องปฏิบัติตามมาตรฐานการสำรองข้อมูลแบบ 3-2-1 (3-2-1 Backup Rule) ได้แก่ การจัดเก็บข้อมูลสำรองไว้อย่างน้อย 3 ชุด บันทึกลงในสื่อจัดเก็บข้อมูลที่แตกต่างกัน 2 ประเภท และต้องจัดเก็บข้อมูลสำรองอย่างน้อย 1 ชุดไว้ในพื้นที่ภายนอกสถาบัน (Off-site Backup) อย่างปลอดภัย

2.1.2 ข้อมูลสำรองต้องมีการจัดเก็บไว้ในสื่อบันทึกข้อมูลที่มีความมั่นคงปลอดภัย และควรมีการจัดเก็บสำเนาข้อมูลสำรองแยกต่างหากจากสถานที่ตั้งระบบงานหลัก (Off-site Storage) หรือจัดเก็บบนระบบคลาวด์ที่เชื่อถือได้ เพื่อป้องกันความเสียหายในกรณีเกิดภัยพิบัติ ณ สถานที่ตั้งหลัก

2.1.3 การสำรองข้อมูลต้องมีการบันทึกสถานะการดำเนินงานและตรวจสอบความถูกต้องของข้อมูลหลังการสำรอง (Backup Verification) เพื่อให้มั่นใจว่าข้อมูลที่จัดเก็บนั้นมีความสมบูรณ์และไม่เสียหาย

2.2 หน้าที่ของเจ้าหน้าที่ในการสำรองข้อมูลส่วนบุคคลและงานในความรับผิดชอบ

2.2.1 บุคลากรทุกคนมีหน้าที่รับผิดชอบในการสำรองข้อมูลที่ใช้ในการปฏิบัติงานส่วนบุคคลที่จัดเก็บอยู่ในเครื่องคอมพิวเตอร์พกพา เครื่องคอมพิวเตอร์ส่วนบุคคล และพื้นที่ส่วนกลางบนระบบคลาวด์ที่สถาบันจัดสรรให้

2.2.2 ห้ามบุคลากรสำรองข้อมูลที่มีชั้นความลับของสถาบันไว้ในสื่อบันทึกข้อมูลส่วนตัวหรือระบบคลาวด์สาธารณะที่ไม่ได้รับอนุญาต เพื่อป้องกันการรั่วไหลของข้อมูลและความเสี่ยงจากการถูกเข้าถึงโดยผู้ไม่มีสิทธิเข้าใช้งาน

2.2.3 ในกรณีที่มีการลาออกหรือเปลี่ยนตำแหน่งงาน บุคลากรต้องดำเนินการตรวจสอบและส่งมอบข้อมูลสำรองที่เกี่ยวข้องกับการปฏิบัติงานให้แก่ผู้บังคับบัญชา หรือตามที่ผู้บังคับบัญชามอบหมาย

2.3 การกู้คืนระบบและข้อมูล (Data Recovery)

2.3.1 สถาบันจัดให้มีการทดสอบการกู้คืนข้อมูลจากสื่อบันทึกสำรอง (Backup Restoration Test) อย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบประสิทธิภาพของข้อมูลสำรองและเตรียมความพร้อมของเจ้าหน้าที่ในการรับมือกับเหตุการณ์ไม่คาดฝัน

2.3.2 ขั้นตอนการกู้คืนข้อมูลต้องมีการลำดับความสำคัญของระบบงาน (Prioritization) โดยให้ความสำคัญกับระบบเทคโนโลยีสารสนเทศหลักที่ส่งผลกระทบต่อการดำเนินงานของสถาบันเป็นลำดับแรก

2.3.3 เมื่อมีการกู้คืนข้อมูลเรียบร้อยแล้ว เจ้าหน้าที่ผู้ดูแลระบบต้องตรวจสอบความถูกต้องและเป็นปัจจุบันของข้อมูลอีกครั้งก่อนเปิดให้เจ้าหน้าที่ทั่วไปเข้าใช้งานตามปกติ

2.4 การป้องกันข้อมูลสำรองจากการถูกทำลาย

2.4.1 ข้อมูลสำรองที่สำคัญต้องมีการตั้งค่าการป้องกันการแก้ไขหรือลบข้อมูล (Write Once Read Many: WORM) หรือมาตรการอื่นที่เทียบเท่า เพื่อป้องกันมัลแวร์เรียกค่าไถ่เข้าถึงและทำลายข้อมูลสำรอง

2.4.2 การเข้าถึงพื้นที่จัดเก็บข้อมูลสำรองต้องจำกัดสิทธิ์เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น และต้องผ่านกระบวนการพิสูจน์ตัวตนที่เข้มงวด

2.5 การกำหนดเป้าหมายในการกู้คืนระบบและข้อมูล (Recovery Objectives: RTO/RPO)

2.5.1 การกำหนดเป้าหมายระยะเวลาที่ยอมรับได้หากข้อมูลสูญหาย (Recovery Point Objective: RPO) สถาบันต้องประเมินและกำหนดกรอบระยะเวลาย้อนหลังสูงสุดที่สามารถยอมรับได้ในกรณีที่ข้อมูลสูญหาย เพื่อนำค่าเป้าหมายดังกล่าวมาใช้เป็นเกณฑ์ในการกำหนดความถี่ของการสำรองข้อมูล (Backup Frequency) ในแต่ละระบบงานให้เหมาะสมและป้องกันความเสียหายต่อภารกิจหลัก

2.5.2 การกำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) ให้ฝ่ายเทคโนโลยีสารสนเทศร่วมกับผู้รับผิดชอบระบบงาน กำหนดกรอบระยะเวลาสูงสุดที่ยอมรับได้ในการกู้คืนระบบให้กลับมาพร้อมใช้งานตามปกติหลังจากเกิดเหตุระบบขัดข้องหรือภัยพิบัติ โดยต้องจัดลำดับความสำคัญตามผลกระทบต่อการดำเนินงานของสถาบัน

2.5.3 การใช้เกณฑ์ชี้วัดในการทดสอบและประเมินผล ผู้ดูแลระบบต้องนำเป้าหมาย RTO และ RPO ที่กำหนดไว้ของแต่ละระบบงาน มาใช้เป็นเกณฑ์มาตรฐานในการวัดผลประเมินประสิทธิภาพระหว่างการทดสอบการกู้คืนข้อมูลประจำปี เพื่อให้มั่นใจว่าทรัพยากรและแผนการกู้คืนที่มีอยู่สามารถตอบสนองต่อเหตุฉุกเฉินและกู้คืนระบบได้ตามระยะเวลาที่กำหนดจริง

2.5.4 การทบทวนเป้าหมายการกู้คืน สถาบันต้องจัดให้มีการทบทวนและปรับปรุงค่าเป้าหมาย RTO และ RPO อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงโครงสร้างระบบงานที่สำคัญ เพื่อให้สอดคล้องกับบริบทความเสี่ยงและแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ในปัจจุบันของสถาบัน

ส่วนที่ 9 การคุ้มครองข้อมูลส่วนบุคคล
(Data Privacy - PDPA)

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อกำหนดมาตรฐานและวิธีการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของสถาบัน ให้เป็นไปตามที่กฎหมายกำหนด

1.2 เพื่อป้องกันการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ ซึ่งอาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลและสถาบัน

1.3 เพื่อสร้างความตระหนักรู้ให้แก่เจ้าหน้าที่ในการจัดการข้อมูลส่วนบุคคลอย่างปลอดภัยและถูกต้องตามหลักจริยธรรม

2. แนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

2.1 การเก็บรวบรวมข้อมูลส่วนบุคคล

2.1.1 การเก็บรวบรวมข้อมูลส่วนบุคคลของบุคลากร ผู้มาติดต่อ หรือคู่ค้า ต้องกระทำภายใต้วัตถุประสงค์ที่จำกัดและจำเป็นตามภารกิจของสถาบันเท่านั้น และต้องแจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ก่อนหรือในขณะเก็บรวบรวม

2.1.2 เจ้าหน้าที่ต้องระมัดระวังการเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) เช่น ข้อมูลสุขภาพ ศาสนา หรือประวัติอาชญากรรม โดยต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล หรือเป็นไปตามข้อยกเว้นที่กฎหมายกำหนด

2.1.3 ข้อมูลส่วนบุคคลที่จัดเก็บในรูปแบบอิเล็กทรอนิกส์ ต้องมีการระบุที่จัดเก็บชัดเจนและจำกัดสิทธิการเข้าถึงเฉพาะเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบโดยตรงเท่านั้น

2.2 การใช้และการเปิดเผยข้อมูลส่วนบุคคล

2.2.1 ห้ามเจ้าหน้าที่นำข้อมูลส่วนบุคคลที่สถาบันครอบครองอยู่ไปใช้ประโยชน์ส่วนตัว หรือเปิดเผยให้แก่บุคคลภายนอกโดยไม่ได้รับอนุญาตหรือไม่มีฐานอำนาจตามกฎหมายรองรับ

2.2.2 การส่งต่อข้อมูลส่วนบุคคลผ่านระบบเครือข่ายหรือระบบคลาวด์ ต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสม เช่น การเข้ารหัสไฟล์ข้อมูล หรือการส่งข้อมูลผ่านช่องทางที่สถาบันกำหนด

2.2.3 ในกรณีที่มีการจ้างงานหน่วยงานภายนอก (Outsource) ให้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล สถาบันต้องจัดให้มีข้อตกลงประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) เพื่อควบคุมให้ผู้รับจ้างปฏิบัติตามมาตรฐานความปลอดภัยของสถาบัน

2.3 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

2.3.1 เจ้าหน้าที่ต้องปฏิบัติตามมาตรการป้องกันทางเทคนิคและทางบริหารจัดการ เพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลถูกแก้ไข เปลี่ยนแปลง หรือถูกเข้าถึงโดยผู้ไม่มีสิทธิเข้าใช้งาน

2.3.2 เมื่อมีการตรวจพบเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหล (Data Breach) เจ้าหน้าที่ต้องรายงานต่อผู้บริหารและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของสถาบันทันที เพื่อดำเนินการเยียวยาและแจ้งเหตุต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับตั้งแต่ทราบเหตุตามที่กฎหมายกำหนด

2.3.3 การทำลายเอกสารหรือสื่อบันทึกข้อมูลที่มีข้อมูลส่วนบุคคลปรากฏอยู่ ต้องดำเนินการตามกระบวนการทำลายข้อมูลอย่างถาวร

2.4 สิทธิของเจ้าของข้อมูลส่วนบุคคล

2.4.1 สถาบันจัดให้มีช่องทางและกระบวนการรองรับการใช้สิทธิของเจ้าของข้อมูล เช่น การขอเข้าถึงข้อมูล การขอแก้ไขข้อมูล หรือการขอลบข้อมูล ตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

2.4.2 เจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องกับการรับคำร้องขอใช้สิทธิ ต้องดำเนินการตรวจสอบและประสานงานเพื่อให้เจ้าของข้อมูลได้รับสิทธิตามระยะเวลาที่สถาบันกำหนด

ส่วนที่ 10 นโยบายด้านความรับผิดชอบ
(Accountability and Responsibility Policy)

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อกำหนดขอบเขตความรับผิดชอบของเจ้าหน้าที่ในการใช้งานและดูแลรักษาทรัพย์สินสารสนเทศของสถาบันให้เป็นไปตามมาตรฐานความปลอดภัย

1.2 เพื่อใช้เป็นแนวทางในการกำกับดูแลและตรวจสอบการปฏิบัติงานของเจ้าหน้าที่ให้สอดคล้องกับระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

1.3 เพื่อสร้างบรรทัดฐานที่ชัดเจนในการแสดงความรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศโดยมิชอบหรือโดยประมาท

2. หน้าที่ความรับผิดชอบแยกตามตำแหน่งงานที่เกี่ยวข้อง

2.1 ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO / ผู้อำนวยการสถาบัน)

2.1.1 เป็นผู้อนุมัติหลักการและประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของสถาบัน เพื่อให้มีผลบังคับใช้กับเจ้าหน้าที่ทุกระดับ

2.1.2 มีอำนาจสูงสุดในการตัดสินใจและสั่งการในสภาวะวิกฤต หรือกรณีเกิดเหตุฉุกเฉินร้ายแรงที่ส่งผลกระทบต่อพันธกิจหลักของสถาบัน

2.1.3 กำกับดูแลให้สถาบันมีโครงสร้างการบริหารจัดการความเสี่ยง (Risk Management) และงบประมาณที่เพียงพอต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

2.1.4 รับรายงานผลการปฏิบัติงานและสถานการณ์ความเสี่ยงจาก CIO เพื่อกำหนดทิศทางและนโยบายในภาพรวม

2.2 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

2.2.1 เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ และมีอำนาจสั่งการให้ทุกหน่วยงานระงับเหตุหรือหยุดการเชื่อมต่อระบบทันทีเพื่อป้องกันความเสียหาย

2.2.2 วิเคราะห์และประเมินสถานการณ์ความเสี่ยง แล้วรายงานข้อมูลต่อ ผู้บริหารระดับสูงสุด (CEO) เพื่อขออนุมัติแนวทางการระงับเหตุในกรณีที่มีความซับซ้อน

2.2.3 กำกับดูแลการปฏิบัติงานของเจ้าหน้าที่สารสนเทศอย่างใกล้ชิด และวางแผนการบริหารความเสี่ยงรวมถึงตรวจสอบระบบความมั่นคงปลอดภัยของฐานข้อมูลและระบบคลาวด์

2.3 ผู้ดูแลระบบและเจ้าหน้าที่สารสนเทศ (System/LAN Administrator and Staffs)

2.3.1 ปฏิบัติตามคำสั่งของ CIO ในการระงับเหตุฉุกเฉิน และดำเนินการตรวจสอบความเสียหายของทรัพย์สินสารสนเทศ (Hardware/Software) หลังเหตุการณ์สงบลง

2.3.2 ตรวจสอบค่าความปลอดภัยหลัก เช่น Firewall, Log files, Configuration ของระบบงานที่สำคัญ และตรวจสอบภัยคุกคาม (Virus/Worm/Hacker) อย่างสม่ำเสมอ

2.3.3 รับผิดชอบการสำรองข้อมูล (Backup) และเตรียมความพร้อมของอุปกรณ์กู้คืนระบบ (Disaster Recovery) เพื่อให้สถาบันสามารถดำเนินงานต่อเนื่องได้โดยเร็วที่สุด

2.4 หัวหน้าหน่วยงานที่เกิดเหตุ (On-site Manager)

2.4.1 แจ้งเหตุฉุกเฉินและอำนวยการเคลื่อนย้ายบุคลากรออกจากพื้นที่เสี่ยง พร้อมให้ข้อมูลรายละเอียดสถานที่เกิดเหตุแก่ผู้บริหารและทีมเทคนิค

2.4.2 ตรวจสภาพและสอบทานบัญชีทรัพย์สินสารสนเทศที่ขนย้ายออกมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับชั้น

2.5 บุคลากร (Staff and Users)

2.5.1 รับผิดชอบการใช้งานบัญชีและอุปกรณ์ (รวมถึงเครื่องพกพา/ส่วนบุคคล) ให้เป็นไปตามสิทธิที่ได้รับ และไม่กระทำการใดๆ ที่เป็นการเปิดช่องโหว่ให้แก่ผู้ไม่มีสิทธิเข้าใช้งาน

2.5.2 มีหน้าที่รายงานเหตุการณ์ผิดปกติทันที และไม่มีสิทธิ์อ้างความไม่รู้ในนโยบายเพื่อยกเว้นความรับผิดชอบ

3. แนวทางปฏิบัติและความรับผิดชอบรายด้าน

3.1 ความรับผิดชอบระดับบุคคล (Individual Responsibility)

3.1.1 เจ้าหน้าที่ต้องรับผิดชอบต่อกิจกรรมใดๆ ที่เกิดขึ้นภายใต้บัญชีผู้ใช้งานของตนเอง และห้ามอ้างความไม่รู้ในนโยบายที่สถาบันได้สื่อสารเผยแพร่แล้ว

3.1.2 การเข้า-ออกห้องควบคุมระบบ (Server Room) หรือการเข้าถึงระบบคลาวด์ ต้องเป็นไปตามสิทธิ์ที่ได้รับอนุมัติ (RBAC) และต้องมีการบันทึกหลักฐานการเข้าใช้งานทุกครั้ง

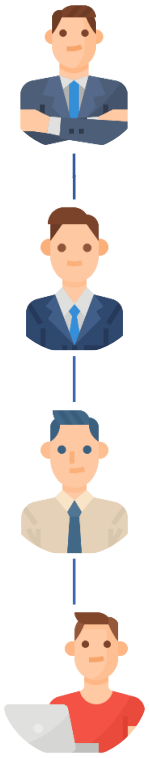
3.2 ความรับผิดชอบต่อทรัพย์สินและการควบคุม (Asset & Control Accountability)

3.2.1 การติดตั้ง หรือเปลี่ยนแปลงค่าคุณลักษณะ (Parameter) ของระบบสารสนเทศ ต้องผ่านการตรวจสอบและอนุมัติจาก CIO หรือผู้ที่ได้รับมอบหมายเท่านั้น

3.2.2 ทรัพย์สินสารสนเทศทุกชนิดต้องมีการตรวจสอบบำรุงรักษาอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบป้องกันภัย (เช่น ระบบดับเพลิงอัตโนมัติในห้อง Server) พร้อมใช้งานตลอดเวลา

3.2.3 สถาบันสงวนสิทธิ์ในการดำเนินคดีทางวินัย แพ่ง หรืออาญา หากพบว่าการละเมิดนโยบายก่อให้เกิดความเสียหายร้ายแรงต่อระบบฐานข้อมูลหรือข้อมูลส่วนบุคคล (PDPA)

แผนผังสายการบังคับบัญชา (Lines of Authority)



Chief Executive Officer (CEO)

ผู้อำนวยการสถาบัน

Chief Information Officer (CIO)

รองผู้อำนวยการ ที่ได้รับมอบหมายให้กำกับดูแล

สำนักยุทธศาสตร์และสารสนเทศ

ผู้อำนวยการสำนักยุทธศาสตร์และสารสนเทศ

กลุ่มงานสารสนเทศ

- นักเทคโนโลยีสารสนเทศ