ประกาศสำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๕๘

ตามที่ทางสำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติได้ประกาศใช้แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สศช. ๒๕๕๕ แล้ว ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ และมาตรา ๗ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้โดยทางหน่วยงานต้องจัดทำเป็นประกาศ นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ หรือต่อไปนี้เรียกว่า “สศช.” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ประสิทธิผล มีความมั่นคงปลอดภัย มีการป้องกันปัญหาหรือภัยคุกคามต่างๆ ที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของ สศช. โดยสามารถดำเนินงานได้อย่างต่อเนื่อง และเหมาะสมกับสถานะภาพการทำงานของระบบฯ ในปัจจุบัน จึงเห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สศช. พ.ศ. ๒๕๕๘ ดังต่อไปนี้

ข้อ ๑ แนวนโยบายนี้เรียกว่า “**แนวนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สศช. พ.ศ. ๒๕๕๘** ”

ข้อ ๒ คำนิยามในนโยบายนี้

“**แนวนโยบาย**” หมายถึง หลักการหรือกรอบความคิดในการดูแลและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ สศช. ที่ได้ประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของ สศช. ที่เกี่ยวข้องได้ถือปฏิบัติเป็นไปในแนวทางเดียวกัน

“**แนวปฏิบัติ**” หมายถึง ขั้นตอนวิธีการที่ สศช. ได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่ที่ปฏิบัติงานภายใต้ระบบสารสนเทศของ สศช. ที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์นั้นมีวิธีการที่มีความมั่นคงปลอดภัย และเชื่อถือได้

“**ข้อความ**” หมายความว่า เรื่องราวหรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ

"สารสนเทศ" หมายความว่า ข้อมูลในรูปแบบใดๆ อาจเป็นข้อมูลปฐมภูมิหรือทุติยภูมิก็ได้ ที่สามารถนำมาประมวลผลเพื่อใช้ในการตัดสินใจในเชิงบริหาร เช่น การวิเคราะห์ทางด้านนโยบาย การตัดสินใจในเชิงการวางแผนที่สำคัญ โดยข้อมูลบางชนิดอาจจับต้องได้ มีรูปแบบทางกายภาพ และข้อมูลบางชนิดอาจจับต้องไม่ได้ อยู่ในรูปแบบสื่ออิเล็กทรอนิกส์

"เทคโนโลยีสารสนเทศ" หมายความว่า เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งครอบคลุมถึงการรับ-ส่ง แปลง จัดเก็บ ประมวลผล และค้นคืนสารสนเทศ โดยมีองค์ประกอบ ๓ ส่วน คือ คอมพิวเตอร์ การสื่อสารและสารสนเทศ ซึ่งต้องอาศัยทำงานอยู่ร่วมกัน ตัวอย่างเช่น เครื่องคอมพิวเตอร์แม่ข่าย (คอมพิวเตอร์) เป็นองค์ประกอบสำคัญของระบบเครือข่าย (การสื่อสาร) โดยมีการส่งข้อมูลต่างๆ ไปยังเครื่องลูกข่าย (สารสนเทศ)

"ระบบเทคโนโลยีสารสนเทศ" หมายความว่า ระบบเทคโนโลยีที่รองรับการประมวลผลสารสนเทศให้สามารถทำงานได้อย่างสะดวก รวดเร็ว และมีประสิทธิภาพ

"ผู้บริหารระดับสูงสุดของสำนักงานฯ" หมายความว่า ผู้บริหารระดับสูงสุดของสำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (Chief Executive Officer : CEO) คือ เลขาธิการคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ มีอำนาจหน้าที่ในการบริหารงานของสำนักงานฯ โดยรวม รวมถึงการกำหนดนโยบาย และการแต่งตั้งมอบหมายหน้าที่ให้กับผู้รับผิดชอบงานของสำนักงานฯ ในแต่ละด้าน

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของสำนักงานฯ" หมายความว่า ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของสำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (Chief Information Officer : CIO) ซึ่งได้รับการแต่งตั้งโดยเลขาธิการคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ โดยมีอำนาจหน้าที่ตามประกาศคำสั่งของ สศช.

"ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร" หมายความว่า ผู้ที่มีอำนาจหน้าที่ในการปฏิบัติราชการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สศช. ตามประกาศคำสั่งแต่งตั้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของ สศช.

"ผู้ใช้งาน" หมายความว่า บุคคลที่ได้รับอนุญาตให้เข้ามาใช้บริการต่างๆ ในด้านงานระบบเทคโนโลยีสารสนเทศภายใต้ระบบเครือข่ายคอมพิวเตอร์ของ สศช. โดยมีสิทธิและหน้าที่ขึ้นกับบทบาทหน้าที่ภายในสำนักงานฯ โดยแบ่งระดับผู้ใช้งานไว้ ดังนี้

- ระดับผู้บริหาร หมายถึง ผู้ใช้งานที่เป็นระดับผู้บริหารของ สศช.
- ระดับผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สศช. ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์ฯ ให้มีหน้าที่รับผิดชอบในการดูแลรักษาและบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ เครื่องแม่ข่ายคอมพิวเตอร์ที่ติดตั้งอยู่ในห้องปฏิบัติการศูนย์เทคโนโลยีสารสนเทศฯ รวมถึงอุปกรณ์ด้านระบบเครือข่ายต่างๆ ที่ติดตั้งอยู่ภายในสำนักงานฯ รวมถึงการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งานระบบต่างๆ

● ระดับเจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการของ สศช.

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิในการเข้าถึงระบบปฏิบัติการ ระบบงานคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศของ สศช.

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิการเข้าถึงทรัพยากรบนระบบเครือข่ายคอมพิวเตอร์ หรือระบบสารสนเทศ ของ สศช.ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตนั้น สำหรับบุคคลภายนอก

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือระบบเครือข่ายคอมพิวเตอร์ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบปฏิบัติการ ระบบงานคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศของ สศช. ถูกบุกรุก โจมตี หรือถูกคุกคาม

"การประเมินความเสี่ยง" หมายความว่า กระบวนการตรวจสอบ การประมาณโอกาสของผลลัพธ์ใดๆ ที่ไม่พึงประสงค์ต่อสารสนเทศ และผลเสียที่อาจจะเกิดขึ้นตามมาได้

"สินทรัพย์ (assets)" หมายความว่า สิ่งใดๆ ก็ตามที่อาจมองเห็นได้หรืออาจมองเห็นไม่ได้ ที่มีอยู่ในองค์กรและมีค่าต่อองค์กร ซึ่งอาจมีมูลค่านับได้หรือนับไม่ได้ก็ตาม

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า การดำรงไว้ซึ่งองค์ประกอบ ๓ ประการด้วยกันคือ

(๑) ความลับ (Confidentiality) คือ การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลนั้นได้

(๒) ความถูกต้องครบถ้วน (Integrity) คือ การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่มีเจตนาก็ตาม

(๓) ความพร้อมใช้งาน (Availability) คือ การรับรองว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศต่างๆ พร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

"ธุรกรรม" หมายความว่า การกระทำใดๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐ

"อิเล็กทรอนิกส์" หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่างๆ เช่นที่กล่าวมา

“ธุรกรรมทางอิเล็กทรอนิกส์” หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

“เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ใดๆ ที่ส่งผลกระทบต่อการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานฯ ทำให้ระบบงานด้านเทคโนโลยีสารสนเทศของสำนักงานฯ หยุดชะงัก ไม่สามารถปฏิบัติงานได้โดยอาจส่งผลกระทบถึงระบบฯ ทั้งทางตรงและทางอ้อม

ข้อ ๓ นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ สศช. ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่อไปนี้

๓.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ครอบคลุมใน ๔ ด้าน คือ

(๑) การเข้าถึงระบบสารสนเทศ

(๒) การเข้าถึงระบบเครือข่ายคอมพิวเตอร์

(๓) การเข้าถึงระบบปฏิบัติการ (Operating System)

(๔) การเข้าถึงโปรแกรมประยุกต์ (Application)

๓.๒ การจัดให้มีระบบสารสนเทศและระบบสำรองของระบบสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๓.๔ การกำหนดแนวทางการใช้งานระบบสารสนเทศ รวมทั้งหน้าที่ความรับผิดชอบของผู้ใช้งานบนระบบเครือข่ายคอมพิวเตอร์ของ สศช.

ข้อ ๔ แนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สศช. ตามนโยบายในข้อ ๓ ให้เป็นไปตามที่กำหนดไว้ในเอกสารแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สศช. พ.ศ. ๒๕๕๘

ข้อ ๕ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดของสำนักงานฯ (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น โดยได้กำหนดระดับความรับผิดชอบไว้ดังนี้

๕.๑ ระดับนโยบายของ สศช. หมายความถึง เมื่อเกิดความเสียหายหรืออันตรายใดๆ ต่อระบบคอมพิวเตอร์หรือระบบสารสนเทศ ผู้รับผิดชอบคือ ผู้บริหารระดับสูงสุดของสำนักงานฯ (CEO)

๕.๒ ระดับการปฏิบัติ กำกับ และติดตามประเมินผลทางด้านนโยบายและการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สศช. หมายความถึง เมื่อเกิดความเสียหายหรืออันตรายใดๆ ต่อระบบคอมพิวเตอร์หรือระบบสารสนเทศ ผู้รับผิดชอบคือ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของสำนักงานฯ (CIO) และ

เจ้าหน้าที่ผู้ปฏิบัติงานของศูนย์เทคโนโลยีฯ และหากพบว่าความเสียหายหรืออันตรายดังกล่าวเกิดจากผู้ใช้งาน ผู้ใช้งานนั้นจะต้องเป็นผู้รับผิดชอบแล้วแต่กรณีไป

ข้อ ๖ การเสริมสร้างความรู้ความเข้าใจแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้กับผู้ใช้งานระบบเทคโนโลยีสารสนเทศของ สศช. เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยขาดความระมัดระวังหรือความรู้เท่าไม่ถึงการณ์ ศูนย์เทคโนโลยีสารสนเทศฯ จะทำการเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สศช.ผ่านทางระบบอีเมล์ การจัดฝึกอบรม รวมทั้งการเผยแพร่ประกาศในระบบ KM Web Portal ของสำนักงานฯ

ข้อ ๗ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สศช. เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศฉบับนี้และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๙ มิถุนายน พ.ศ. ๒๕๕๘

(นายอาคม เติมพิทยาไพสิฐ)
เลขาธิการคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ