สรุปรายละเอียดนโยบายความมั่นคงปลอดภัย ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับผู้ให้บริการภายนอก (Information Security Policy for Supplier)

ศูนย์เทคโนโลยีสารสนเทศ

หมายเลขเอกสาร : SD-ISMS-004 เวอร์ชัน : 1.0

ชื่อเอกสาร : สรุปรายละเอียดนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับผู้ให้บริการภายนอก (Information Security Policy for Supplier)

รายละเอียดการควบคุมเอกสาร

หมายเลขเอกสาร	SD-ISMS-004
ชื่อเอกสาร	สรุปรายละเอียดนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับผู้ให้บริการภายนอก (Information Security Policy for Supplier)
เวอร์ชัน	1.0
วันที่ปรับปรุง	6 กุมภาพันธ์ 2562
วันที่บังคับใช้	12 กุมภาพันธ์ 2562

ประวัติการปรับปรุงเอกสาร

เวอร์ชัน	วันที่ปรับปรุง	รายละเอียด	ผู้รับผิดชอบ	วันที่บังคับใช้
1.0	6 กุมภาพันธ์ 2562	เอกสารใหม่	นายชนาธิป แก้วเนิน	12 กุมภาพันธ์ 2562

หมายเลขเอกสาร : SD-ISMS-004 เวอร์ชัน : 1.0

ชื่อเอกสาร : สรุปรายละเอียดนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับผู้ให้บริการภายนอก (Information Security Policy for Supplier)

การอนุมัติเอกสาร

ผู้รับผิดชอบ	ผู้สอบทาน	ผู้อนุมัติ
ลงชื่อ _____	ลงชื่อ _____	ลงชื่อ _____
(นายชนาธิป แก้วเนิน) นักวิชาการคอมพิวเตอร์ปฏิบัติการ	(นางอรญา สุโมตยกุล) นักวิชาการคอมพิวเตอร์ ชำนาญการพิเศษ	(นางสาวสุดจิตร ลาภเลิศสุข) ผู้อำนวยการ ศูนย์เทคโนโลยีสารสนเทศ
วันที่ 12 / กพ. / 2562	วันที่ 12 / ก.พ. / 2562	วันที่ 12 / กพ / 2562

สรุปรายละเอียดนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่สามารถเข้าถึงได้โดยหน่วยงานภายนอก และเพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของหน่วยงานภายนอก

1. การปฏิบัติตามนโยบาย กฎหมาย ข้อบังคับ และการปฏิบัติงาน
   - 1.1 ผู้ให้บริการภายนอก ต้องปฏิบัติตามนโยบายฯ มาตรฐาน ขั้นตอน คู่มือ แนวทาง และข้อปฏิบัติต่างๆ ด้านสารสนเทศ รวมถึงมาตรการรักษาความปลอดภัยอื่นๆ ของกรมบัญชีกลาง และกฎหมาย ข้อบังคับ ที่ประกาศใช้ภายในประเทศโดยเคร่งครัด
   - 1.2 กฎหมาย และข้อบังคับใดๆ เช่น พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ เป็นต้น ที่ประกาศใช้ในประเทศไทยถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนัก และต้องปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ให้บริการภายนอกกระทำความผิดตามกฎหมาย หรือข้อบังคับที่ประกาศใช้ในประเทศไทยกรมบัญชีกลาง ถือว่าเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดนั้นเอง
   - 1.3 ผู้ให้บริการภายนอก ต้องไม่ใช้ระบบสารสนเทศ ของกรมบัญชีกลาง ไปในทางที่ไม่ถูกต้อง เสื่อมเสียชื่อเสียง ผิดกฎหมาย ขัดกับนโยบาย หรือแนวทางปฏิบัติการใช้ระบบสารสนเทศ
   - 1.4 ผู้ให้บริการภายนอก มีหน้าที่รับผิดชอบต่อทรัพย์สินของกรมบัญชีกลาง เสมือนเป็นทรัพย์สินของผู้ให้บริการเอง
   - 1.5 หน่วยงานภายนอกที่เข้าถึงสารสนเทศของหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร (Non-Disclosure Agreement)
   - 1.6 บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนฯ
   - 1.7 หน่วยงานภายนอกต้องระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้
     - เหตุผลในการขอใช้
     - ระยะเวลาในการใช้
     - การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
     - การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
     - การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

1.8 หน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และลงนามในสัญญาไม่เปิดเผยข้อมูลขององค์กร

1.9 องค์กรมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

1.10 ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

1.11 กรมบัญชีกลาง ขอสงวนสิทธิในการเพิกถอน หรือยกเลิก การนำเสนอข้อมูลสารสนเทศของกรมบัญชีกลาง ที่อยู่ในเครือข่ายสาธารณะในกรณีที่ดำเนินการอย่างไม่ถูกต้อง หรือส่งผลเสียหายต่อกรมบัญชีกลาง

1.12 ผู้ให้บริการภายนอก ต้องให้ความร่วมมือกับเจ้าหน้าที่ของรัฐที่ได้รับการแต่งตั้งตามกฎหมาย หรือเจ้าหน้าที่กรมบัญชีกลาง ในการตรวจสอบการใช้งาน

1.13 กรมบัญชีกลางสามารถบันทึกข้อมูลปูมเหตุการณ์ (Log) หรือข้อมูลจราจรคอมพิวเตอร์ ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

1.14 ผู้ให้บริการภายนอก ที่ไม่ปฏิบัติตามนโยบายฯ ข้อบังคับ มาตรฐาน หรือระเบียบปฏิบัติ อาจจะถูกระงับการใช้งาน หรือได้รับพิจารณาโทษตามความเหมาะสม

1.15 ห้ามผู้ให้บริการภายนอก กระทำความผิด หรือยินยอม/สนับสนุนให้มีการกระทำความผิดตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

1.16 กรมบัญชีกลาง ไม่สนับสนุน และไม่ยินยอมให้ผู้ให้บริการภายนอก หรือผู้ที่มีส่วนเกี่ยวข้อง นำระบบสารสนเทศขององค์กรไปใช้ในการกระทำความผิดตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ หากผู้ใดละเมิด หรือฝ่าฝืนกรมบัญชีกลาง ถือว่าเป็นการกระทำความผิดส่วนบุคคลที่ผู้ทำผิดนั้นต้องรับผิดชอบต่อความผิดเอง ซึ่งจะมีโทษตาม พ.ร.บ. ดังกล่าว

2. ความรับผิดชอบต่อข้อมูลสารสนเทศขององค์กร

2.1 ผู้ให้บริการภายนอก ต้องรับผิดชอบในการรักษาสารสนเทศที่ตนเป็นเจ้าของให้อยู่ในสภาพที่สมบูรณ์

2.2 ผู้ให้บริการภายนอก ต้องไม่เปิดเผยข้อมูลสารสนเทศใดๆ ที่เป็นความลับ หรือข้อมูลที่มีความสำคัญต่อองค์กรสู่ภายนอก หรือสาธารณะ

2.3 หน่วยงานภายนอกที่เข้าใช้สารสนเทศภายในชั้นความลับ จำเป็นต้องมีการระบุว่าจะไม่เปิดเผยข้อมูล

2.4 ห้ามผู้ให้บริการภายนอกที่ไม่มีสิทธิ เข้าถึงหรือแก้ไข หรือเปลี่ยนแปลงข้อมูลของระบบสารสนเทศโดยไม่ได้รับอนุญาต หรือไม่มีหน้าที่เกี่ยวข้อง

2.5 ระบบสารสนเทศ และข้อมูลที่ใช้ภายในกรมบัญชีกลาง ถือเป็นทรัพย์สินของกรมบัญชีกลาง ห้ามไม่ให้ผู้ให้บริการภายนอก นำไปใช้เป็นการส่วนตัว

2.6 ผู้ให้บริการภายนอก ต้องระมัดระวังการใช้เอกสาร รวมทั้งข้อมูลสารสนเทศทุกชนิด และปฏิบัติตามขั้นตอนปฏิบัติการจัดระดับชั้นความลับของข้อมูล

2.7 การเผยแพร่ข้อมูลของกรมบัญชีกลางสู่สาธารณะต้องได้รับเห็นชอบจากหน่วยงานเจ้าของข้อมูล หรือผู้มีอำนาจ หรือคณะกรรมการที่ได้รับการแต่งตั้งก่อนดำเนินการใดๆ

2.8 ห้ามผู้ให้บริการภายนอก เผยแพร่ข้อมูลเกี่ยวกับช่องโหว่ของระบบสารสนเทศ และข้อมูลสำคัญ/เป็นความลับออกสู่สาธารณะโดยไม่ได้รับอนุญาต

2.9 ผู้ให้บริการภายนอก ต้องไม่ละทิ้งอุปกรณ์อิเล็กทรอนิกส์ ข้อมูลสารสนเทศ และเอกสารของกรมบัญชีกลาง ในที่สาธารณะ

2.10 ผู้ให้บริการภายนอก ต้องตรวจสอบอุปกรณ์ สื่อบันทึกข้อมูลเพื่อดูว่ามีข้อมูลสำคัญขององค์กร เช่น ข้อมูลที่เป็นความลับ หรือซอฟต์แวร์ลิขสิทธิ์ เป็นต้น เก็บอยู่ในสื่อบันทึกหรือไม่ก่อนนำกลับมาใช้งานใหม่ หรือในกรณีที่ต้องทิ้งสื่อบันทึกข้อมูลทุกชนิด ต้องลบข้อมูลทิ้ง หรือทำลายสื่อบันทึกข้อมูลด้วยวิธีการที่มั่นคงปลอดภัย

2.11 ผู้ให้บริการภายนอก ต้องไม่นำทรัพย์สินระบบสารสนเทศขององค์กร เช่น ข้อมูลสารสนเทศ หรือซอฟต์แวร์ เป็นต้น ออกนอกกรมบัญชีกลาง โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล หรือเจ้าของระบบงาน

2.12 ผู้ให้บริการภายนอก ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับกรมบัญชีกลาง

3. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และการใช้อุปกรณ์สารสนเทศ

3.1 ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก

3.2 ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกให้ถูกต้องชัดเจน

3.3 ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในศูนย์เทคโนฯ

3.4 ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าออกศูนย์เทคโนฯ ได้ด้วยบัตรผู้ติดต่อ “Visitor” โดยสิทธิ์จะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าปฏิบัติงานภายในศูนย์เทคโนฯ

3.5 พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้าออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

3.6 ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตร

3.7 เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการขออนุญาตเข้าออกและตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

3.8 เจ้าหน้าที่ศูนย์เทคโนฯ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่รักษาความปลอดภัย เป็นประจำทุกเดือน

3.9 เจ้าหน้าที่ศูนย์เทคโนฯ ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ 2 ครั้ง

3.10 การนำทรัพย์สินสารสนเทศ เข้า-ออก ห้องศูนย์คอมพิวเตอร์ (Data Center) จะต้องได้รับการอนุมัติจากเจ้าหน้าที่ศูนย์เทคโนฯ ก่อนทุกครั้ง

4. การละเมิดลิขสิทธิ์ และทรัพย์สินทางปัญญา

4.1 ผู้ให้บริการภายนอก ที่ใช้ทรัพยากรสารสนเทศของกรมบัญชีกลาง ต้องไม่ละเมิดสิทธิส่วนบุคคล ละเมิดทรัพย์สินทางปัญญาของผู้อื่น

4.2 กรมบัญชีกลาง ให้ความสำคัญต่อลิขสิทธิ์ และทรัพย์สินทางปัญญา ดังนั้นกรมบัญชีกลาง ห้ามไม่ให้ผู้ให้บริการภายนอกติดตั้ง หรือใช้งานชุดซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ที่ถูกต้อง หากกรมบัญชีกลางตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ซึ่งผู้ให้บริการภายนอกต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

4.3 ซอฟต์แวร์ที่กรมบัญชีกลาง จัดหา หรือเตรียมไว้ให้ผู้ใช้งาน ถือว่าเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ให้บริการภายนอกถอดถอน เปลี่ยนแปลง หรือสำเนาไปใช้งานที่อื่นใดโดยพละการ หากมีความจำเป็นจะต้องดำเนินการใดๆ กับซอฟต์แวร์หรือส่วนที่เกี่ยวข้องที่เจ้าของระบบงาน หน่วยงานที่มีอำนาจ หรือหน่วยงานต้นสังกัดจัดเตรียมไว้ให้ ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรก่อนดำเนินการ

4.4 ลิขสิทธิ์ของชุดโปรแกรม หรือซอฟต์แวร์ที่กรมบัญชีกลาง จัดหามา สามารถใช้ได้เฉพาะเครื่องคอมพิวเตอร์ หรืออุปกรณ์ทางอิเล็กทรอนิกส์ทุกชนิดที่กรมบัญชีกลาง จัดหาให้เท่านั้น ยกเว้นกรณีที่ต้นสังกัดจะอนุญาตเป็นลายลักษณ์อักษรถึงจะนำไปใช้กับ เครื่องคอมพิวเตอร์ หรืออุปกรณ์ทางอิเล็กทรอนิกส์อื่นได้ ทั้งนี้ต้นสังกัดต้องรับผิดชอบต่อการนำไปใช้ด้วย

5. การพัฒนาระบบ การแก้ไขเปลี่ยนแปลง และการทดสอบระบบสารสนเทศ

5.1 การพัฒนาการให้บริการระบบสารสนเทศใดๆ ต้องพิจารณาถึงความมั่นคงปลอดภัยสารสนเทศตามหลักของกฎหมายเทคโนโลยีสารสนเทศ นโยบายและแนวปฏิบัติ รวมถึงแนวทาง และหลักเกณฑ์ที่ทำให้สารสนเทศมีความปลอดภัย

5.2 ผู้ให้บริการภายนอก จะต้องพัฒนาระบบสารสนเทศของกรมบัญชีกลาง ตามแนวทางการพัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัย (Secure Software Development Life Cycle)

5.3 การจัดซื้อ หรือจัดจ้างพัฒนาระบบงานใดๆ เพื่อให้ได้มาซึ่งระบบงานที่ใช้ภายในกรมบัญชีกลาง จะต้องได้รับการทดสอบช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ ก่อนส่งมอบระบบงานที่พัฒนาขึ้นใช้ภายในกรมบัญชีกลาง

6. ความรับผิดชอบต่อรหัสผ่าน
   6.1 กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม
   6.2 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
   6.3 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ครอบครองอยู่
   6.4 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
   6.5 ผู้ให้บริการภายนอก จะต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับครั้งแรกทันทีที่ทำการล็อกอินเข้าสู่ระบบสารสนเทศ
   6.6 รหัสผ่าน และกุญแจอิเล็กทรอนิกส์ถือเป็นทรัพย์สินของกรมบัญชีกลาง และเป็นความรับผิดชอบของผู้ให้บริการภายนอกที่จะต้องปกป้อง
   6.7 ผู้ให้บริการภายนอก ต้องเก็บรักษารหัสผ่าน หรือส่วนที่เกี่ยวข้องเป็นความลับ และต้องไม่เปิดเผยด้วยวิธีการใดๆ ต่อบุคคลอื่นทราบ รวมถึงต้องไม่ใช้รหัสผ่านร่วมกัน โดยไม่มีข้อยกเว้น
   6.8 เมื่อผู้ให้บริการภายนอก ไม่อยู่ที่หน้าจอคอมพิวเตอร์ ต้องล็อกออฟ (Log off) หรือล็อคหน้าจอแบบอัตโนมัติ (ไม่เกิน 10 นาที) ทุกครั้ง

7. การเชื่อมต่อเครื่องคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์กับเครือข่ายภายในของกรมบัญชีกลาง
   7.1 กรมบัญชีกลาง อนุญาตให้เฉพาะเครื่องคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ที่เป็นทรัพย์สินของกรมบัญชีกลาง เท่านั้น ที่สามารถเชื่อมกับระบบสารสนเทศของกรมบัญชีกลาง ในกรณีที่ผู้ให้บริการภายนอก นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์มาเองต้อง จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการอนุมัติจากกรมบัญชีกลาง
   7.2 เครื่องคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ ที่ผู้ให้บริการภายนอกนำมาเชื่อมกับระบบเครือข่ายภายใน หรือกรมบัญชีกลางจัดหาให้ต้องติดตั้งซอฟต์แวร์ป้องกันภัยคุกคามที่จำเป็น เช่น ซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี (Anti-virus) เป็นต้น และต้องปรับปรุงซอฟต์แวร์นี้ให้ทันสมัยอยู่เสมอ (Update signature and patch)
   7.3 การเข้าถึง และใช้งานระบบเทคโนโลยีสารสนเทศต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศและหลักเกณฑ์ของกรมบัญชีกลาง
   7.4 การใช้งานระบบสารสนเทศของกรมบัญชีกลาง ต้องผ่านการพิสูจน์ตัวตนผู้ใช้งาน ด้วยระบบงานหรือระบบที่สามารถพิสูจน์ได้ว่าเป็นผู้มีสิทธิใช้ และเข้าถึงระบบสารสนเทศนั้นๆ
   7.5 กรมบัญชีกลาง สามารถตรวจสอบปูมเหตุการณ์ได้ตลอดเวลา เพื่อให้มั่นใจว่ากรมบัญชีกลางดำเนินการควบคุมการเข้าถึงได้อย่างเหมาะสม

7.6 กรมบัญชีกลาง สามารถยกเลิกการเข้าถึงได้โดยไม่ต้องแจ้งให้ทราบ หากพบว่า ใช้งานไม่เหมาะสม และถ้าเกี่ยวข้องกับกฎหมายจะพิจารณาดำเนินคดีด้วย

7.7 ต้องไม่ติดตั้งโปรแกรมที่ส่อไปในทางไม่ดี และไม่ใช้ซอฟต์แวร์/ชุดโปรแกรมที่ผิดกฎหมาย ติดตั้งในเครื่องคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ที่นำมาเชื่อมกับระบบเครือข่ายกรมบัญชีกลาง ยกเว้นจะได้รับอนุญาตจากกรมบัญชีกลาง หรือต้นสังกัด

8. การป้องกันโปรแกรมไม่ประสงค์ดี

8.1 ห้ามนำเครื่องคอมพิวเตอร์ ซอฟต์แวร์หรือข้อมูลที่ไม่มั่นใจว่าติดมัลแวร์ (Malware) มาติดตั้งใช้งาน

8.2 ห้ามปรับแต่ง หรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันมัลแวร์ที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่องค์กรได้จัดหาให้

8.3 ผู้ให้บริการภายนอกควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบการอัปเดต (Update) ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบ หากไม่สามารถอัปเดต (Update) ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

8.4 ผู้ให้บริการภายนอก ควรแจ้งให้ผู้ดูแลระบบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อสงสัยว่ามีการติดมัลแวร์

8.5 หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malicious and mobile code) ห้ามมิให้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

9. การควบคุมการเข้าถึงระบบสารสนเทศจากทางไกล (Remote Access)

9.1 ผู้ให้บริการภายนอก ที่มีความจำเป็นต้องใช้ระบบสารสนเทศภายในจากระยะไกล (Remote Access) ต้องถูกระบุสิทธิ และได้รับอนุญาตเป็นลายลักษณ์อักษรต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนฯ และต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

9.2 การเข้าถึงระบบสารสนเทศจากระยะไกลต้องทำผ่านระบบพิสูจน์ตัวตน (Authentication) ของกรมบัญชีกลาง และต้องใช้ช่องทางเชื่อมต่อแบบปลอดภัย เช่น การใช้วีพีเอ็น (VPN) การเข้ารหัสข้อมูล (Encryption) ที่ได้มาตรฐาน (กรณีจำเป็น) เป็นต้น โดยฝ่ายสารสนเทศขอสงวนสิทธิตรวจสอบบันทึกปูมเหตุการณ์ (Log files) หรือข้อมูลจราจรคอมพิวเตอร์ของการเข้าใช้ เพื่อติดตามและตรวจสอบสิ่งที่ผิดปกติที่อาจเกิดขึ้น

9.3 ผู้ให้บริการภายนอก ต้องไม่เชื่อมต่อระบบสารสนเทศออกสู่เครือข่ายภายนอกโดยไม่ได้ผ่านความเห็นชอบจากศูนย์เทคโนฯ หรือหน่วยงานต้นสังกัด และกรณีที่มีการเชื่อมสู่ภายนอกโดยไม่ผ่านเครือข่ายของกรมบัญชีกลาง ต้องแจ้งให้ศูนย์เทคโนฯ หรือผู้บังคับบัญชาทราบด้วย

10. การใช้งานระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ต (Internet and Intranet Usage)

10.1 ระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ต เป็นทรัพย์สินของกรมบัญชีกลาง และอนุญาตให้ใช้เฉพาะงาน หรือกิจกรรมที่เกี่ยวข้องกับกรมบัญชีกลาง เท่านั้น

10.2 ผู้ให้บริการภายนอกต้องไม่ใช้อินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

10.3 ผู้ให้บริการภายนอกต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

10.4 ไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

10.5 ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

10.6 ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

10.7 ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

10.8 การใช้งานเว็บบอร์ด (Web Board) ขององค์กร ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กร

10.9 ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

10.10 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

11. การแจ้งเหตุการณ์ที่ผิดปกติ (Incident Response)

11.1 หากผู้ให้บริการภายนอกพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย หรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัย หรือการทำงานที่ผิดปกติของซอฟต์แวร์ ผู้ใช้ต้องรายงานสิ่งที่เกิดขึ้นให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร็วที่สุดเท่าที่จะทำได้

11.2 ในกรณีที่ไม่สามารถติดต่อกับผู้ดูแลระบบได้ ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น และรายงานให้หน่วยงานดูแลรับผิดชอบได้ทราบด้วย

11.3 ผู้ให้บริการภายนอกมีหน้าที่รายงานเหตุการณ์ที่น่าสงสัยว่าเป็นเหตุการณ์ละเมิดความมั่นคง เช่น เหตุการณ์ต่อไปนี้

- พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น มีไฟล์ที่ไม่รู้จัก การเปลี่ยนแปลงของค่าต่าง ๆ
- พบหรือคาดว่าสารสนเทศในระบบถูกทำลาย แก้ไข หรือลบทิ้ง
- การให้บริการของระบบเกิดการชะงัก หรือไม่สามารถให้บริการได้
- เกิดการละเมิดสิทธิ์เข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล