
# นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ

(Information Security Policy)

สารบัญ

## นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ(Acceptable Use Policy)

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศกรมตรวจบัญชีสหกรณ์ เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์ให้อยู่ระดับมาตรฐานสากลโดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC ๒๗๐๐๑ อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของกรมตรวจบัญชีสหกรณ์

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ กรมตรวจบัญชีสหกรณ์ ประกอบด้วยรายละเอียดดังต่อไปนี้

## นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

---

## นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์(Firewall Policy)

ข้อ ๑ ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของไฟร์วอลล์ภายในส่วนกลาง

ข้อ ๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ ๓ ทุกเส้นทางเชื่อมต่ออินเ ตอร์เน็ตผ่านระบบเครือข่าย ของกรมตรวจบัญชีสหกรณ์ที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๓.๑ การใช้งาน Web

๓.๒ การใช้งาน E-mail

๓.๓ การใช้งาน Instant Messaging

๓.๔ การใช้งาน Video Conference/Streaming

บริการอื่นนอกจากที่ระบุไว้ข้างต้นนี้ กรมตรวจบัญชีสหกรณ์ไม่อนุญาตให้ใช้งาน

ข้อ ๔ ผู้ใช้งานอินเตอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

ข้อ ๕ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่ เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๗ การกำหนดนโยบายในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางกรมตรวจบัญชีสหกรณ์ อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความความยินยอมจากศูนย์เทคโนโลยีสารสนเทศก่อน

ข้อ ๘ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนด ค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำ เป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๙ จะต้องมีการสำรองข้อมูลการกำ หนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๐ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเตอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๑ ศูนย์เทคโนโลยีสารสนเทศ มีสิทธิที่จะระงับหรือบล็อกการใช้งาน ของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำ งานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๒ ข้อกำหนดการลงโทษผู้ซึ่งมิได้ปฏิบัติตามนโยบายด้านความปลอดภัยของไฟร์วอลล์

๑๒.๑ ให้ดำเนินการกล่าวตักเตือนด้วยวาจากับผู้ใช้งาน

๑๒.๒ ในกรณีที่ผู้ใช้งานยังคงไม่ปฏิบัติตามนโยบายและยังคงปฏิบัติอยู่เช่นเดิม ให้ดำเนินการตักเตือนเป็นลายลักษณ์อักษรถึงผู้บังคับบัญชา

---

## นโยบายความมั่นคงปลอดภัยของอีเมล์ (E-mail Policy)

ข้อ ๑ ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่ดูแลระบบ e-mail

ข้อ ๒ เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ต้องเปลี่ยนรหัสผ่าน(Password) โดยทันที

ข้อ ๓ ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ หรือติดรหัสไว้หน้าเครื่องคอมพิวเตอร์

ข้อ ๔ ควรเปลี่ยนรหัสผ่าน (Password) อย่างน้อยทุก ๑ ปี

ข้อ ๕ ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-mail) ของตน

ข้อ ๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๗ ไม่อนุญาตให้ผู้ใช้งาน E-mail ทุกคนนำข้อมูลที่เป็นความลับหรือข้อมูลที่มีความสำคัญของกรมตรวจบัญชีสหกรณ์ส่งไปยังบุคคลที่ไม่เกี่ยวข้อง

ข้อ ๘ ไม่อนุญาตให้ผู้ใช้งาน E-mail ทุกคนส่งข้อมูลหรือเผยแพร่ข้อมูลอันเป็นข้อมูลที่ผิดหรือขัดต่อกฎหมาย

ข้อ ๙ ไม่อนุญาตให้ผู้ใช้งาน E-mail ทุกคนส่งข้อมูลหรือข้อความที่เป็นในรูปแบบของ Junk Mail หรือ Spam Mail หรือการโฆษณา หรือชี้นำ หรือให้มีการซื้อขายสิ่งของหรือบริการ

---

**<u>นโยบายความมั่นคงปลอดภัยของอินเตอร์เน็ต (Internet Security Policy)</u>**

ข้อ ๑ ห้ามใช้ระบบอินเ ตอร์เน็ต (Internet) ของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

ข้อ ๓ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ของกรมตรวจบัญชีสหกรณ์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้า ยที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

ข้อ ๔ หลังจากใช้งานระบบอินเ ตอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๕ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำ การอันใดที่เป็นการละเมิดนโยบายของกรมตรวจบัญชีสหกรณ์ การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเ กี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของกรมตรวจบัญชีสหกรณ์ จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

---

**นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก**
**(Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)**

ข้อ ๑ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกรมตรวจบัญชีสหกรณ์ และเครือข่ายข้อมูลทั้งหมด

ข้อ ๒ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๓ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

ข้อ ๔ มีการตรวจสอบเหตุการณ์ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๕ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

ข้อ ๖ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๗ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๘ กรมตรวจบัญชีสหกรณ์ มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๙ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของ กรมตรวจบัญชีสหกรณ์ การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของ กรมตรวจบัญชีสหกรณ์ จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

---

**นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)**

๑. ให้มีการใช้งานเครื่องมือหรืออุปกรณ์ในการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ด้วยเครื่องสแกนลายนิ้วมือ หรืออย่างอื่นที่เหมาะสม
๒. ให้มีการเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์จากเครื่องสแกนลายนิ้วมือและสามารถเรียกบันทึกกลับขึ้นมาดูได้
๓. ให้มีการติดตั้งกล้องวงจรปิดให้สามารถมองเห็นในทุกส่วนของศูนย์คอมพิวเตอร์
๔. ให้มีภาพจากกล้องวงจรปิดปรากฏบนหน้าจอตลอดเวลา
๕. ให้มีการบันทึกภาพจากกล้องวงจรปิดและสามารถเรียกกลับมาดูย้อนหลังได้อย่างน้อย ๗ วัน

๖. เมื่อมีบุคคลภายนอกต้องการเข้ามายังห้องแม่ข่าย ต้องมีการขออนุญาตเข้าห้องแม่ข่ายและเห็นชอบจากผู้อำนวยการศูนย์สารสนเทศเป็นลายลักษณ์อักษร

๗. ต้องมีเจ้าหน้าที่ที่รับผิดชอบด้านเครือข่ายของศูนย์เทคโนโลยีสารสนเทศอยู่ภายในห้องแม่ข่ายด้วยเมื่อมีบุคคลภายนอกเข้ามายังห้องแม่ข่าย

---

**<u>หน้าที่รับผิดชอบของบุคลากรในองค์การในการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ</u>**

**๑. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ**

๑.๑ จัดให้มีการประชุมด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดแนวทางการจัดทำนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์

๑.๓ จัดให้มีการจัดทำและทบทวนนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์

๑.๔ จัดให้มีการควบคุมให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑.๕ จัดให้มีการประเมินความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์อย่างน้อยปีละ ๑ ครั้ง

๑.๖ จัดให้มีการพัฒนาและปรับปรุงด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์อย่างน้อยปีละ ๑ ครั้ง

๑.๗ จัดให้มีการเผยแพร่เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศให้เจ้าหน้าหน้าที่ทุกระดับทราบและตระหนึกถึงความสำคัญด้านความมั่นคงปลอดภัย

๑.๘ จัดให้มีการอบรมด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่เจ้าหน้าที่ของกรมฯทั้งส่วนกลางและส่วยภูมิภาค

**๒ ผู้เชี่ยวชาญด้านโปรแกรมระบบบัญชีสหกรณ์**

๒.๑ ให้คำปรึกษา แนะนำและให้ความรู้ระบบเทศโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์ แก่คณะทำงานด้านความมั่นคงปลอดภัย

๒.๒ ให้คำปรึกษาในการกำหนดนโยบายความมั่นคงปลอดภัยด้านระบบบัญชีสหกรณ์

๒.๓ ให้คำปรึกษาแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยด้านระบบบัญชีสหกรณ์

๒.๔ ให้คำปรึกษาแนวทางการปรับปรุงและพัฒนาการดำเนินงานด้านความมั่นคงปลอดภัย

**๓. ที่ปรึกษาระบบด้านสารสนเทศทางบัญชี**

๓.๑. ให้คำปรึกษา แนะนำและให้ความรู้ด้านระบบสารสนเทศทางบัญชีของกรมฯ แก่คณะทำงานด้านความมั่นคงปลอดภัย

๓.๒. ให้คำปรึกษาในการกำหนดนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศทางบัญชี

๓.๓. ให้คำปรึกษาแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศทางบัญชี

๓.๔. ให้คำปรึกษาแนวทางการปรับปรุงและพัฒนาการดำเนินงานด้านความมั่นคงปลอดภัย

**๔. ที่ปรึกษาระบบด้านสารสนเทศสำนักงาน**

๔.๑. ให้คำปรึกษา แนะนำและให้ความรู้ด้านระบบสารสนเทศทางสำนักงานของกรมฯ แก่คณะทำงานด้านความมั่นคงปลอดภัย

๔.๒. ให้คำปรึกษาในการกำหนดนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศทางสำนักงาน

๔.๓. ให้คำปรึกษาแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศทางสำนักงาน

๔.๔ ให้คำปรึกษาแนวทางการปรับปรุงและพัฒนาการดำเนินงานด้านความมั่นคงปลอดภัย

**๕. ที่ปรึกษาระบบด้านสารสนเทศการสอบบัญชี**

๕.๑. ให้คำปรึกษา แนะนำและให้ความรู้ด้านระบบสารสนเทศการสอบบัญชีของกรมตรวจบัญชีสหกรณ์แก่คณะทำงานด้านความมั่นคงปลอดภัย

๕.๒. ให้คำปรึกษาในการกำหนดนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศการสอบบัญชี

๕.๓. ให้คำปรึกษาแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศการสอบบัญชี

๕.๔. ให้คำปรึกษาแนวทางการปรับปรุงและพัฒนาการดำเนินงานด้านความมั่นคงปลอดภัย

**๖. ที่ปรึกษาระบบด้านเครือข่ายและความปลอดภัย**

๖.๑. ให้คำปรึกษา แนะนำและให้ความรู้ด้านความมั่นคงปลอดภัย แก่คณะทำงานด้านความมั่นคงปลอดภัย

๖.๒. ให้คำปรึกษาในการกำหนดนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของกรมตรวจบัญชีสหกรณ์

๖.๓. ให้คำปรึกษาแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของกรมตรวจบัญชีสหกรณ์

๖.๔. ให้คำปรึกษาแนวทางการปรับปรุงและพัฒนาการดำเนินงานด้านความมั่นคงปลอดภัย

**๗. ผู้อำนวยการกลุ่มพัฒนาระบบสารสนเทศและฐานข้อมูล**

๗.๑. กำหนดนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศและฐานข้อมูล

๗.๒. กำหนดแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและฐานข้อมูล

๗.๓. ทบทวนและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศและฐานข้อมูล

๗.๔. ทบทวนและปรับปรุงแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ และฐานข้อมูล

๗.๕. พัฒนาและปรับปรุงความมั่นคงปลอดภัยระบบสารสนเทศและฐานข้อมูล

**๘. ผู้อำนวยการกลุ่มพัฒนาระบบบัญชีคอมพิวเตอร์**

๘.๑. กำหนดนโยบายด้านความมั่นคงปลอดภัยระบบบัญชีคอมพิวเตอร์

๘.๒. กำหนดแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยระบบบัญชีคอมพิวเตอร์

๘.๓. ทบทวนและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยระบบบัญชีคอมพิวเตอร์

๘.๔. ทบทวนและปรับปรุงแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยระบบบัญชีคอมพิวเตอร์

๘.๕. พัฒนาและปรับปรุงความมั่นคงปลอดภัยระบบบัญชีคอมพิวเตอร์

**๙. ผู้อำนวยการกลุ่มพัฒนาระบบตรวจสอบบัญชีคอมพิวเตอร์**

๙.๑. กำหนดนโยบายด้านความมั่นคงปลอดภัยระบบบัญชีคอมพิวเตอร์

๙.๒. กำหนดแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยระบบตรวจสอบบัญชีคอมพิวเตอร์

๙.๓. ทบทวนและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยระบบตรวจสอบบัญชีคอมพิวเตอร์

๙.๔. ทบทวนและปรับปรุงแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยระบบตรวจสอบบัญชีคอมพิวเตอร์

๙.๕. พัฒนาและปรับปรุงความมั่นคงปลอดภัยระบบตรวจสอบบัญชีคอมพิวเตอร์

## ๑๐. ผู้อำนวยการกลุ่มระบบเครือข่ายคอมพิวเตอร์

๑๐.๑. กำหนดนโยบายด้านความมั่นคงปลอดภัยระบบบัญชีคอมพิวเตอร์

๑๐.๒. กำหนดแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์

๑๐.๓. ทบทวนและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์

๑๐.๔. ทบทวนและปรับปรุงแนวทางการควบคุมนโยบายความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์

๑๐.๕. พัฒนาและปรับปรุงความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์

๑๐.๖. ควบคุมให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑๐.๗. ดำเนินการประเมินความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมฯอย่างน้อยปีละ ๑ ครั้ง

๑๐.๘. ดำเนินการพัฒนาและปรับปรุงด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์ อย่างน้อยปีละ ๑ ครั้ง

---