แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศ

กรมประมง
ประจำปี พ.ศ. 2565

INFORMATION SECURITY POLICY

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ประกาศกรมประมง

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

พ.ศ. ๒๕๖๕

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ อธิบดีกรมประมง โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงได้ออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศกรมประมง เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕”

ข้อ ๒ บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๓ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมประมงมีการดำเนินการครอบคลุมประเด็นสำคัญดังต่อไปนี้

๓.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๓.๒ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๔ รายละเอียดและองค์ประกอบของแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรของกรมประมงและบุคคลหรือหน่วยงานภายนอกที่เกี่ยวข้องรับทราบและถือปฏิบัติให้เป็นไปตามเอกสารแนบท้ายประกาศ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๕ เอกสารแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีการประกาศใช้จะเผยแพร่ผ่านเว็บไซต์ของกรมประมง

ข้อ ๖ กรมประมงจะมีการทบทวนปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ที่มีผลกระทบต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๖.๑ การปรับปรุงแก้ไขหรือเปลี่ยนแปลงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ดำเนินการโดยออกประกาศแก้ไขเพิ่มเติม หรือยกเลิกประกาศฉบับเดิมแล้วออกประกาศฉบับใหม่ทดแทนแล้วแต่กรณี

๖.๒ การปรับปรุงแก้ไขแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ดำเนินการโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรมประมง หรือคณะทำงานพัฒนาและส่งเสริมการใช้ระบบสารสนเทศของกรมประมง หรือคณะทำงานบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ หรือคณะทำงานที่เกี่ยวข้อง เสนอความเห็นชอบต่ออธิบดีกรมประมง ในการพิจารณาและประกาศเผยแพร่แก่บุคลากร หน่วยงานที่เกี่ยวข้องรับทราบและถือปฏิบัติ

ข้อ ๗ อธิบดีกรมประมง ในฐานะผู้บริหารสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๘ ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๓ สิงหาคม พ.ศ. ๒๕๖๕

(นายเฉลิมชัย สุวรรณรักษ์)
อธิบดีกรมประมง

แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ

INFORMATION SECURITY POLICY

กรมประมง
ประจำปี พ.ศ. 2565

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

เอกสารแนบท้ายประกาศ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมประมง ประจำปี พ.ศ. 2565

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นในการได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชน รวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการพัฒนาประเทศ ขณะเดียวกันการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชนมักเกิดปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วน หัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศคือหลักแนวคิด CIA ประกอบด้วย Confidentiality (การธำรงไว้ซึ่งความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้องครบถ้วน) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (สภาพพร้อมใช้งาน) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศในหลากหลายรูปแบบ ส่งผลกระทบด้านลบเพิ่มมากขึ้นเรื่อย ๆ ทั้งในและต่างประเทศ ซึ่งปัญหาเกิดจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดแนวนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ โดยคณะอนุกรรมการความมั่นคงปลอดภัย ภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

กรมประมง จึงได้จัดทำแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมประมง ประจำปีงบประมาณ พ.ศ. 2565 ขึ้น เผยแพร่แก่บุคลากรและหน่วยงานที่เกี่ยวข้องรับทราบและถือปฏิบัติ เพื่อให้บุคลากรทุกคนในกรมประมงมีความรู้ เข้าใจแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมประมง และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

กรมประมง

สิงหาคม 2565

สารบัญ

บทที่ 1 บทนำ

1.1 หลักการ 1

1.2 วัตถุประสงค์และขอบเขต 1

1.3 องค์ประกอบของนโยบาย 2

1.4 บทบังคับใช้ 2

1.5 การเผยแพร่และทบทวน 2

บทที่ 2 คำนิยาม 3

บทที่ 3 นโยบายการรักษาความมั่นคงปลอดภัย

หมวด 1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

ส่วนที่ 1 นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security Policy) 6

การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย 6

การควบคุมการเข้า-ออก อาคาร สถานที่ 7

การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) 7

ส่วนที่ 2 นโยบายการควบคุมการเข้า - ออกห้องควบคุมระบบเครือข่าย (Network System Control Room Policy) 10

การควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย 10

ส่วนที่ 3 นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control Policy) 12

ประเภทข้อมูลลำดับชั้นความลับของข้อมูล 12

การควบคุมการเข้าถึงระบบ 14

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ 14

การบริหารจัดการการเข้าถึงขอผู้ใช้ 15

การบริหารจัดการการเข้าถึงระบบเครือข่าย 19

การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย 20

การบริหารจัดการการบันทึกและตรวจสอบ 20

การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร 21

การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก 21

ส่วนที่ 4 นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third Party Access Control Policy) 22

ส่วนที่ 5 นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control) 24
การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย 24
ส่วนที่ 6 นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) 28
การเข้าใช้งานที่มั่นคงปลอดภัย 28
การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) 29
การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities) 29
การหมดเวลาใช้งานระบบสารสนเทศ (Session Time - out) 29
ส่วนที่ 7 นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application Information Access Control) 30
การจำกัดการเข้าถึงสารสนเทศ (Information Access Control) 30
การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time) 31
การจัดการกับระบบซึ่งไวต่อการรบกวน 32
การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) 32
ปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time - out) 32
ส่วนที่ 8 นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer Policy) 34
การควบคุมการเข้าถึงระบบปฏิบัติการ 34
การใช้รหัสผ่าน 35
การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware) 35
การสำรองข้อมูลและการกู้คืน 35
ส่วนที่ 9 นโยบายการใช้งานเครื่องคอมพิวเตอร์พกพา (Use of Notebook Computer Policy) 36
การป้องกันความปลอดภัยทางด้านกายภาพ 37
การควบคุมการเข้าถึงระบบปฏิบัติการ 37
การใช้รหัสผ่าน 37
การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware) 37
การสำรองข้อมูลและการกู้คืน 38
ส่วนที่ 10 นโยบายการใช้งานอุปกรณ์สื่อสารแบบพกพา (Smart Device Policy) 39
การป้องกันความปลอดภัยทางด้านกายภาพ 39
การควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ 40
ส่วนที่ 11 นโยบายการการประชุมผ่านสื่ออิเล็กทรอนิกส์ (Conference Policy) 41
ส่วนที่ 12 นโยบายการใช้งานอินเทอร์เน็ต (Internet Security Policy) 43
ส่วนที่ 13 นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail Policy) 45

ส่วนที่ 14 นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy) 47
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย 47
การเข้าใช้เครือข่ายไร้สายกรมประมง 48
ส่วนที่ 15 นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious software Protection Policy) 49
การป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี 49
ส่วนที่ 16 นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก (Firewall & IPS Policy) 50
การป้องกันระบบเครือข่ายและตรวจจับการบุกรุก 50
หมวด 2 ระบบสารสนเทศและระบบสำรองของสารสนเทศ
ส่วนที่ 17 นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy) 52
การคัดเลือกการสำรองข้อมูล 52
การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ 53
การสำรองและกู้คืนข้อมูล 53
หมวด 3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
ส่วนที่ 18 นโยบายการตรวจสอบและประเมินความเสี่ยง 55
ส่วนที่ 19 นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ 57
หมวด 4 การสร้างความตระหนักด้านความปลอดภัยสารสนเทศ
ส่วนที่ 20 นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness policy) 59
ส่วนที่ 21 นโยบายด้านการปฏิบัติตามข้อบังคับ (Compliance Policy) 60

บทนำ

1. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ในมาตรา 5 *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับหน่วยงาน ซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัยเช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบสร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีสำคัญอย่างยิ่งต่อหน่วยงาน ที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ กรมประมงจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมายและมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในหน่วยงาน และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

2. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมประมง หรือต่อไปนี้เรียกว่า "องค์กร" เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์กรและหน่วยงานในสังกัด อีกทั้งเป็นการดำเนินงานตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังนี้

2.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

2.2 เพื่อให้องค์กรมีการกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยอ้างอิงตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 มาตรฐาน ISO/IEC 27001 Annex A และศึกษารายละเอียดวิธีปฏิบัติทางเทคนิคจาก ISO/IEC 17799:2005 รวมทั้งมีการปรับปรุงอย่างต่อเนื่อง

2.3 เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2.5 การกำหนดความรับผิดชอบกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้อธิบดีกรมประมงเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

2.6 นโยบายนี้ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา 1 ครั้งต่อปี

3. องค์ประกอบของนโยบาย

องค์ประกอบของแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมประมง จัดทำขึ้นเพื่อกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ให้สอดคล้องตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 และมาตรา 7 ซึ่งกำหนดให้หน่วยงานภาครัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยแนวปฏิบัตินี้ประกอบด้วย วัตถุประสงค์ ผู้รับผิดชอบ และแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมประมง

4. บทบังคับใช้

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของกรมประมง บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุน และติดตามการประยุกต์ใช้ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรมประมง

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อธิบดีกรมประมงจะเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

5. การเผยแพร่และทบทวน

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมประมงฉบับนี้จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยแนวนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) ของกรมประมง จัดพิมพ์เผยแพร่เพื่อให้บุคลากรของกรมประมง และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามแนวนโยบายนี้อย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **องค์กร** หมายถึง กรมประมง
- **ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)** หมายถึง อธิบดีกรมประมง
- **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)** หมายถึง รองอธิบดีกรมประมงที่ได้รับแต่งตั้งให้ทำหน้าที่และรับผิดชอบในการกำกับดูแล การดำเนินงานด้านเทคโนโลยีสารสนเทศของกรมประมง
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
- **ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร
- **ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร มีบทบาทหน้าที่และความรับผิดชอบในการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศขององค์กร
- **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ ดังนี้
  - **ผู้บริหาร** หมายถึง อธิบดี รองอธิบดี ผู้เชี่ยวชาญ ผู้ตรวจราชการกรมประมง ผู้อำนวยการกองฯ ศูนย์ฯ สถานีฯ ประมงจังหวัด หัวหน้าหน่วยงานราชการ
  - **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
  - **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการขององค์กร
- **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอก ที่กรมประมงอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
- **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ เช่น ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น
  - ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
  - ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
- **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
- **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น
  - พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
  - พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
  - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)
  - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)
  - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

- **สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
- **จดหมายอิเล็กทรอนิกส์** (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน มาตรฐานที่ใช้ในการรับ - ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP3 และ IMAP เป็นต้น
- **รหัสผ่าน** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการควบคุมการเข้าถึงการใช้งานสารสนเทศสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย
- **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non - Repudiation) และความน่าเชื่อถือ (Reliability)
- **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
- **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

หมวดที่ 1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

ส่วนที่ 1
นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security Policy)

1. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติการกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

3.1 ภายในองค์กร ควรมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

3.2 จัดให้มีเวรยาม รักษาอาคารและห้องควบคุมระบบเครือข่ายและอุปกรณ์เชื่อมโยงเครือข่ายภายในอาคาร เพื่อป้องกันการแอบลักลอบเข้าสู่พื้นที่ปฏิบัติงานภายในเพื่อการลักลอบก่อวินาศกรรม การโจรกรรม หรือการทำลายอุปกรณ์ ระบบประมวลผล ระบบฐานข้อมูลและระบบเครือข่าย

3.3 ผู้บริหาร ควรกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage area) เป็นต้น

3.4 ผู้บริหารต้องกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

3.4.1 จัดทำ “ทะเบียนผู้มีสิทธิเข้า - ออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศ

3.4.2 ทำการบันทึกการเข้า - ออกพื้นที่ใช้งาน และกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า - ออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้า - ออกพื้นที่”

3.4.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า - ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า - ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ 1 ครั้ง

4. แนวปฏิบัติการควบคุมการเข้า - ออก อาคาร สถานที่

4.1 จัดทำเอกสารระบุสิทธิของผู้ใช้ และ “หน่วยงานภายนอก” ในการเข้าถึงสถานที่ โดยแบ่งแยกได้ดังนี้

4.1.1 องค์กรต้องกำหนดสิทธิผู้ใช้ที่มีสิทธิผ่านเข้า - ออก และช่วงเวลาที่มีสิทธิในการผ่านเข้า - ออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

4.1.2 รณรงค์หรือออกกฎให้เจ้าหน้าที่องค์กรแขวนบัตรพนักงานเพื่อใช้ระบุตัวตนก่อนเข้าอาคารหรือสถานที่สำคัญของหน่วยงาน

4.1.3 การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้า - ออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

4.1.4 บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจน ตลอดเวลาที่อยู่ในองค์กร

4.1.5 กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะต้องลงบันทึกในแบบฟอร์มการเข้า - ออกในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้อง

4.1.6 กรณีที่บุคคลภายนอกเข้ามาติดต่อ เจ้าหน้าที่จะต้องลงชื่ออนุญาตการเข้า – ออกในแบบฟอร์มการเข้า - ออกให้ถูกต้อง

4.1.7 บุคคลภายนอกหรือผู้ติดต่อต้องคืนแบบฟอร์มการเข้า – ออกและบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และ รปภ. ต้องตรวจสอบผู้ติดต่ออุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

4.2 ผู้ใช้จะได้รับสิทธิให้เข้า - ออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

4.3 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้ ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้ จะต้องแสดงบัตรประจำตัวที่องค์กรออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้า - ออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

5. แนวปฏิบัติการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

5.1 การจัดทำบริเวณล้อมรอบ (Physical Security Perimeter)

5.1.1 มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในองค์กร

5.1.2 มีการประเมินความเสี่ยงทางกายภาพและกำหนดมาตรการลดความเสี่ยง

5.1.3 ผนังล้อมรอบของสำนักงานหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในควรสร้างเป็นผนังทึบ

5.1.4 ประตูหรือทางเข้าสำนักงานหรืออาคารออกแบบเพื่อป้องกันการบุกรุกทางกายภาพ

5.1.5 ประตูหรือทางเข้าของห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายต้องมีระบบที่สามารถล็อคได้เพื่อป้องกันการบุกรุกทางกายภาพ

5.1.6 บุคลากรที่ปฏิบัติงานภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องปิดประตูและหน้าต่างให้ล็อคอยู่เสมอภายหลังเลิกงานและนอกเวลาราชการ

5.1.7 มีการจัดระบบการรักษาความปลอดภัยโดยมีพนักงานรักษาความปลอดภัย (รปภ.) และควรมีการติดตั้งกล้องวงจรปิดภายในลิฟต์เพื่อควบคุมการเข้าถึงของบุคคลภายนอก

5.1.8 ประตูหนีไฟและผนังในบริเวณข้างเคียงต้องมีการก่อสร้างให้มีความทนทานต่อความร้อนอย่างเพียงพอ

5.1.9 ต้องแยกพื้นที่สำหรับระบบเทคโนโลยีสารสนเทศขององค์กรออกจากพื้นที่ที่มีการดูแลหรือบริหารจัดการโดยผู้ให้บริการภายนอก

5.2 การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access Delivery and Loading Areas)

5.2.1 จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

5.2.2 จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

5.2.3 ควรจัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายในองค์กร

5.2.4 ต้องตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

5.2.5 กำหนดให้มีการลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกโดยให้สอดคล้องกับระเบียบพัสดุหรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร

5.3 การจัดวางและการป้องกันอุปกรณ์ (Equipment Siting and Protection)

5.3.1 ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในหน่วยงานหรือสำนักงานให้น้อยที่สุด

5.3.2 ต้องจัดวางระบบเทคโนโลยีสารสนเทศในตำแหน่งที่เหมาะสมเพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจากบุคคลภายนอกโดยการหันหน้าจอเข้ามาภายในโดยไม่ให้บุคคลผู้ซึ่งไม่มีสิทธิสามารถมองเห็นหน้าจอนั้นได้

5.3.3 ต้องแยกเก็บอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่งเพื่อดูแลความมั่นคงปลอดภัย

5.3.4 ห้ามไม่ให้มีการนำอาหาร เครื่องดื่มและสูบบุหรี่ในบริเวณหรือพื้นที่ห้องควบคุมระบบเครือข่าย/ระบบคอมพิวเตอร์/ระบบเครื่องคอมพิวเตอร์แม่ข่าย

5.3.5 ดำเนินการตรวจสอบสอดส่องระดับอุณหภูมิ และดูแลสภาพแวดล้อมภายในบริเวณห้องควบคุมระบบเครือข่าย/ระบบคอมพิวเตอร์/ระบบเครื่องคอมพิวเตอร์แม่ข่ายเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว

5.3.6 มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอนหรือไฟฟ้ากระชาก

5.4 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

5.4.1 ต้องมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์กรที่เพียงพอต่อความต้องการใช้งาน เช่น ระบบปรับอากาศ ระบบระบายอากาศ ระบบกระแสไฟฟ้าสำรอง เป็นต้น และต้องมีการตรวจสอบหรือทดสอบระบบสนับสนุนดังกล่าวอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

5.4.2 ต้องมีการใช้ระบบยูพีเอสกับระบบเทคโนโลยีสารสนเทศเพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้า และต้องทดสอบระบบยูพีเอสอย่างสม่ำเสมอ โดยทดสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้

5.5 การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่น ๆ

5.5.1 เจ้าหน้าที่ทุกคนต้องปฏิบัติการป้องกันทรัพย์สิน

5.5.2 เจ้าหน้าที่ต้องออกจากระบบทันทีเมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

5.5.3 ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย เช่น ในตู้เอกสารที่มีกุญแจล็อค และไม่ทิ้งเอกสารที่สำคัญไว้บนโต๊ะเพื่อความปลอดภัยของทรัพย์สินของราชการ

5.5.4 ต้องป้องกันเครื่องโทรสารเมื่อไม่มีผู้ใช้งานและป้องกันตู้หรือบริเวณที่ใช้ในการรับ - ส่งเอกสารไปรษณีย์เพื่อความปลอดภัยของข้อมูล

5.5.5 ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ต่าง ๆ เช่น เครื่องคอมพิวเตอร์ กล้องดิจิตอล เครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น โดยไม่ได้รับอนุญาต

5.5.6 นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

5.6 มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์

5.6.1 ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

5.6.2 ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการทำลายหรือจำหน่าย

5.6.3 ต้องทำการฟอร์แมต (Format) ฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์ โดยการใช้วิธีแบบเขียนทับซ้ำจำนวน 1 ครั้ง ตามมาตรฐาน NIST 800-88 สำหรับข้อมูลที่มีความลับระดับต่ำ หรือแบบเขียนทับซ้ำจำนวน 3 ครั้ง ตามมาตรฐาน DoD 5220.22-M สำหรับข้อมูลที่มีความลับระดับปานกลางหรือแบบเขียนทับซ้ำจำนวน 7 ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลที่มีความลับระดับสูง

5.6.4 ควรลบข้อมูลออกจากฐานข้อมูลที่มีอายุตั้งแต่ 5 ปีขึ้นไป และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

5.6.5 ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายสื่อบันทึกข้อมูลหรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

ส่วนที่ 2
นโยบายการควบคุมการเข้า - ออกห้องควบคุมระบบเครือข่าย
(Network System Control Room Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้า – ออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้า - ออกห้องควบคุมระบบเครือข่าย

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. กองบริหารจัดการเรือประมงและการทำการประมง
3. หน่วยงานที่มีห้องควบคุมระบบเครือข่าย (Data Center)
4. ผู้ดูแลระบบที่ได้รับมอบหมาย

3. คำจำกัดความของผู้เกี่ยวข้อง

3.1 ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศภายในห้องควบคุมระบบเครือข่าย

3.2 เจ้าหน้าที่ หมายถึง เจ้าหน้าที่องค์กรที่มีสิทธิในการเข้า - ออกสถานที่ อาคาร ห้อง ตามที่กำหนดในทะเบียนผู้มีสิทธิเข้า - ออกพื้นที่

3.3 ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของห้องควบคุมระบบเครือข่าย

4. บทบาทและความรับผิดชอบ

4.1 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

4.1.1 อนุมัติสิทธิเข้า - ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

4.1.2 อนุมัติกระบวนการควบคุมการเข้า - ออก ห้องควบคุมระบบเครือข่าย

4.2 ผู้ดูแลระบบ ห้องควบคุมระบบเครือข่าย

4.2.1 ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องควบคุมระบบเครือข่าย ให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด

4.2.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้า - ออกห้องควบคุมระบบเครือข่าย ต้องติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจำตัวขององค์กรเท่านั้น

5. แนวปฏิบัติการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย

5.1 ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่องค์กร มีแนวทางปฏิบัติ ดังนี้

5.1.1 ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ควรจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

5.1.2 ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิบุคคลในการเข้า - ออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

5.1.3 สิทธิในการเข้า - ออกห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

5.1.4 เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้า-ออกห้องควบคุมระบบเครือข่าย ตามกระบวนการที่ระบุใน ข้อ 6 (6.4) “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน” ในนโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

5.1.5 ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกห้องควบคุมระบบเครือข่าย ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้า - ออกพื้นที่”

5.1.6 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้า - ออกห้องควบคุมระบบเครือข่าย ก็ต้องมีการควบคุมอย่างรัดกุม

5.1.7 การเข้าถึงห้องควบคุมระบบเครือข่าย ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้า - ออกพื้นที่” และต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้า - ออก ทุกคนต้องกรอกแบบฟอร์มดังกล่าว

5.1.8 กรณีผู้ติดต่อจากหน่วยงานภายนอก มีความจำเป็นต้องเข้าห้องควบคุมระบบเครือข่าย เจ้าหน้าที่ผู้ดูแลระบบขององค์กรจะต้องเป็นผู้นำพาเข้าไป และคอยสอดส่อง กำกับดูแลตลอดการปฏิบัติงาน

5.2 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

5.2.1 ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า - ออกพื้นที่”

5.2.2 ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า - ออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า - ออกพื้นที่” ให้ถูกต้องชัดเจน

5.2.3 ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในห้องควบคุมระบบเครือข่ายหรือศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

5.2.4 พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้า - ออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

5.2.5 ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัยซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและตรวจสอบแบบฟอร์มการขออนุญาตเข้า - ออกว่ามีเจ้าหน้าที่ลงนามอนุญาตแล้วทุกครั้ง

5.2.6 เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการขออนุญาตเข้า - ออกและตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

5.2.7 เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้า - ออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ส่วนที่ 3
นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Access Control Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างถูกต้อง

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานที่ใช้งานระบบเทคโนโลยีสารสนเทศ
3. หน่วยงานที่เป็นเจ้าของระบบสารสนเทศ
4. ผู้ดูแลระบบที่ได้รับมอบหมาย
5. เจ้าหน้าที่ประจำโครงการขององค์กร

3. ข้อกำหนดเกี่ยวกับประเภทข้อมูลลำดับชั้นความลับของข้อมูลเวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

3.1 ประเภทข้อมูลขององค์กร แบ่งได้ดังนี้

3.1.1 ข้อมูลสารสนเทศด้านการบริหาร

- นโยบาย
- ข้อมูลยุทธศาสตร์
- ข้อมูลคำรับรองการปฏิบัติราชการ
- ข้อมูลบุคลากร
- ข้อมูลงบประมาณการเงินและบัญชี

3.1.2 ข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน

- ข้อมูลการดำเนินงานตามภารกิจของกรมประมง
- ข้อมูลกฎ ระเบียบ กฎหมายประมง
- ข้อมูลการติดต่อสื่อสารภายในกรมประมง
- ข้อมูลติดตามการดำเนินงานตามภารกิจของกรมประมง
- ข้อมูลติดตามการใช้จ่ายงบประมาณ
- ข้อมูลรายงานผลการปฏิบัติงาน

3.1.3 ข้อมูลสารสนเทศด้านการให้บริการประชาชน

- ข้อมูลทะเบียนเกษตรกรผู้เพาะเลี้ยงสัตว์น้ำ
- ข้อมูลทะเบียนผู้ประกอบการด้านการประมง
- ข้อมูลทะเบียนเรือ
- ข้อมูลใบอนุญาตและใบรับรองด้านการประมง

- ข้อมูลวิชาการและองค์ความรู้ด้านการประมง
- ข้อมูลด้านการวิจัย
- ข้อมูลภูมิสารสนเทศด้านการประมง
- ข้อมูลสถิติการประมง
- ข้อมูลการแจ้งเรือประมงต่างประเทศเข้าเทียบท่า
- ข้อมูลใบรับรองการแปรรูปสัตว์น้ำ
- ข้อมูลแรงงานต่างด้าว
- ข้อมูลการแจ้งเข้า - ออก เรือประมงไทย
- ข้อมูลพิกัดเรือ
- ข้อมูลฟาร์มเพาะเลี้ยงสัตว์น้ำ
- ข้อมูลด้านการประมงอื่น ๆ ที่ให้บริการประชาชน

3.2 ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

3.2.1 การกำหนดชั้นความลับตามความสำคัญของข้อมูลในเอกสารกำหนดไว้ 3 ระดับ ได้แก่ ลับ ลับมาก ลับที่สุด และมีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสารและการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

3.2.2 การควบคุมเอกสาร โดยกำหนดให้มีมาตรการควบคุมต่าง ๆ คือ การจัดทำทะเบียน การตรวจสอบ การจัดทำเอกสารการสำเนา และการแปลการโอนการส่ง และการรับ การเก็บรักษา การยืม การทำลาย การปฏิบัติในเวลาฉุกเฉินเวลาสูญหาย รวมถึงการเปิดเผยข้อมูลในเอกสาร

3.3 เวลาที่ได้เข้าถึง

3.3.1 การเข้าถึงสารสนเทศในเวลาราชการ (08.30 - 16.30 น.)

3.3.2 การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา 08.30 - 16.30 น.)

3.3.3 การเข้าถึงสารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และ วันหยุดนักขัตฤกษ์)

3.3.4 การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง ต้องระบุช่วงเวลาและจำนวนระยะเวลาการเข้าถึง ระยะเวลาการเข้าถึง ได้แก่

- 1 - 3 วัน
- 1 สัปดาห์
- 1 เดือน
- 3 เดือน
- ครึ่งปีงบประมาณ
- ตามเวลาที่ร้องขอ

3.4 ช่องทางการเข้าถึง

3.4.1 ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

3.4.2 เคาน์เตอร์บริการ (เข้าถึงได้ในเวลาราชการ)

3.4.3 โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)
3.4.4 หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)
3.4.5 ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)
3.4.6 ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)
3.4.7 ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)
3.4.8 ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)
3.4.9 เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลาหรือ ในช่วงเวลาพิเศษที่กำหนด)
3.4.10 การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และในช่วงเวลาพิเศษเป็นรายครั้ง)

4. แนวปฏิบัติในการควบคุมการเข้าถึงระบบ

4.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า - ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

4.2 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทุก 6 เดือนเป็นอย่างน้อย ทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

4.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

4.4 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

4.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า - ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

5. แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

5.1 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ ได้แก่ ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

5.2 เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

5.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

6. แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้

6.1 การลงทะเบียนเจ้าหน้าที่ใหม่ขององค์กร

6.1.1 จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเทคโนโลยีสารสนเทศขององค์กร

6.1.2 ผู้ดูแลระบบต้องตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิจากเจ้าของระบบ สำหรับการใช้งานระบบสารสนเทศและบริการอย่างถูกต้อง ต้องมีการอนุมัติรับรองการได้สิทธิจากผู้บริหารอย่างชัดเจน

6.1.3 ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานโดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

6.1.4 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบและมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยขององค์กร

6.1.5 ผู้ดูแลระบบต้องมอบเอกสารรับรองสิทธิการเข้าถึงแก่ผู้ใช้ เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

6.1.6 ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

6.1.7 การลงทะเบียนผู้ใช้งานผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

6.1.8 การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

6.1.8.1 เจ้าหน้าที่ใหม่ขององค์กรกรอกข้อมูลคำขอใช้บริการลงแบบฟอร์มลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ เช่น คำขอใช้อินเทอร์เน็ต ระบบอีเมล์ หรือระบบงานต่าง ๆ

6.1.8.2 ยื่นคำขอกับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารผู้ที่ได้รับมอบหมาย

6.1.9 การให้สิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

6.1.9.1 ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบ ลายเซ็นของบุคคลผู้มีสิทธิอนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

6.1.9.2 ผู้ดูแลระบบตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

6.1.9.3 ผู้ดูแลระบบให้สิทธิการใช้งานระบบตามคำขอในแบบฟอร์ม

6.1.10 การแจ้งยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

6.1.10.1 หัวหน้างานหรือผู้บังคับบัญชา กรอกข้อมูลลงในแบบฟอร์ม และยื่นคำขอกับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

6.1.10.2 ผู้ดูแลระบบยกเลิกสิทธิการใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

6.2 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

6.3 ผู้ใช้ต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

6.4 การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน

6.4.1 ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

6.4.2 การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

6.4.3 การส่งรหัสผ่านชั่วคราวให้กับผู้ใช้ ควรใช้วิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลที่สามหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

6.4.4 ควรกำหนดให้ผู้ใช้ตอบยืนยันการได้รับรหัสผ่าน

6.4.5 ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

6.4.6 การกำหนดชื่อผู้ใช้หรือรหัส ID ต้องเป็นหนึ่งเดียวคือไม่ซ้ำกัน

6.4.7 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

6.4.7.1 ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

6.4.7.2 ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

6.4.7.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6.4.7.4 ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

6.4.8 สิทธิพิเศษควรได้รับการมอบหมายให้กับรหัสผู้ใช้ที่ต่างจากรหัสผู้ใช้ที่ใช้งานตามปกติ

6.5 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

6.5.1 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานระยะเวลาในการเข้าถึง ช่องทางในการเข้าถึง รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับดังต่อไปนี้

6.5.1.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

6.5.1.2 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

6.5.1.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6.5.1.4 การรับ - ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลเช่น SSL VPN หรือ XML Encryption เป็นต้น

6.5.1.5 ควรกำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

6.5.1.6 ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

6.5.2 ผู้ใช้สามารถนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544

6.5.3 เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลอย่างน้อยปีละ 4 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

6.6 การบริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน

6.6.1 ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานหรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ

6.6.2 ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจากลำดับชั้นความลับของข้อมูลหรือความสำคัญตามภารกิจ และรหัสผ่านที่กำหนดใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม

6.6.3 ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ควรเปลี่ยนรหัสผ่านที่ได้รับโดยทันที

6.6.4 ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานตามหลักเกณฑ์ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

6.6.5 ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับและระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่นและไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ ทั้งสิ้น เว้นแต่กรณีผู้ใช้งานที่มีอำนาจอนุมัติใด ๆ ในระบบเทคโนโลยีสารสนเทศไม่สามารถปฏิบัติราชการอันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าว เพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิและหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้วให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

6.6.6 กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวเลขและสัญลักษณ์เข้าด้วยกัน)

6.6.7 ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “12345”

6.6.8 ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วันเดือนปีเกิด ที่อยู่

6.6.9 ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

6.6.10 กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดไม่เกิน 3 ครั้ง

6.6.11 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

6.6.12 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

6.6.13 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

6.6.14 ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที

6.6.15 เมื่อมีปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่าน

6.6.16 การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึกและประทับตรา “ลับ” และส่งไปยังผู้ใช้งานและแนบเอกสาร “แนวปฏิบัติสำหรับการบริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

6.7 การใช้งานรหัสผ่าน

6.7.1 เก็บรหัสผ่านไว้เป็นความลับ

6.7.2 หลีกเลี่ยงการบันทึกรหัสผ่าน (เช่น บันทึกลงในกระดาษในแฟ้มข้อมูลหรือในอุปกรณ์พกพาต่าง ๆ) นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับการอนุมัติแล้ว

6.7.3 เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

6.7.4 กำหนดรหัสผ่านที่มีคุณภาพและมีความยาวเพียงพอสำหรับ

6.7.4.1 ง่ายสำหรับจดจำ

6.7.4.2 ไม่อยู่บนพื้นฐานของสิ่งที่คนอื่นสามารถคาดเดาได้ง่ายหรือสามารถหาได้จากข้อมูลเกี่ยวกับตน เช่น ชื่อ หมายเลขโทรศัพท์ และวันเกิด เป็นต้น

6.7.4.3 ไม่สร้างจุดอ่อนโดยการใช้คำที่อยู่ในพจนานุกรม

6.7.4.4 ไม่มีคำซ้ำหรือตัวอักษรซ้ำ ไม่ควรเป็นตัวเลขทั้งหมดหรือไม่ควรเป็นตัวอักษรทั้งหมด

6.7.5 เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิพิเศษควรได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) และหลีกเลี่ยงการวนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

6.7.6 กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

6.7.7 ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ

6.7.8 ไม่ใช้รหัสผ่านร่วมกับผู้อื่น

6.7.9 ไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้ส่วนตัว

6.7.10 ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบและจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัวควรแนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพข้างต้นสำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

6.8 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

6.8.1 สิทธิการเข้าถึงข้อมูลของผู้ใช้ควรได้รับการพิจารณาทบทวนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เช่น ทุก ๆ 6 เดือน และทุกครั้งที่มีการปรับเปลี่ยน เช่น การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง เป็นต้น

6.8.2 สิทธิการเข้าถึงข้อมูลควรได้รับการทบทวนและจัดสรรใหม่เมื่อมีการเคลื่อนย้ายบุคลากรภายในองค์กร

6.8.3 การให้อำนาจสำหรับสิทธิการเข้าถึงพิเศษควรมีการทบทวนบ่อยกว่า เช่น ทำทุก 3 เดือน เป็นต้น

6.8.4 การจัดสรรสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้ที่ไม่ได้รับมอบอำนาจ

6.8.5 ความเปลี่ยนแปลงของผู้ใช้ที่ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน

6.9 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

6.9.1 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องคอมพิวเตอร์พกพาโดยทันทีเมื่อเสร็จสิ้นงาน

6.9.2 ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

6.9.3 ผู้ดูแลระบบต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตน โดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

7. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่าย

7.1 ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

7.2 การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเทอร์เน็ตหรืออินทราเน็ต จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนที่จะสามารถใช้งานได้ในทุกกรณี

7.3 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

7.4 ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

7.5 ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

7.6 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

7.7 ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กรควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

7.8 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

7.9 การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

7.10 IP address ภายในของระบบงานเครือข่ายภายในขององค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

7.11 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบัน อยู่เสมอ

7.12 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

7.13 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

8. แนวปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

8.1 ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

8.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

8.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ Telnet Ftp หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

8.4 ควรดำเนินการติดตั้งอัพเดตระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

8.5 ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

8.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

9. แนวปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

9.1 ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า - ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน

9.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

9.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

10. แนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

10.1 การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กร การควบคุมบุคคลที่

เข้าสู่ระบบขององค์กรจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

10.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

10.3 ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

10.4 ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

10.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

11. แนวปฏิบัติการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ไม่ว่าจะเป็นการเข้าสู่ระบบสารสนเทศทางอินเทอร์เน็ต หรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร อย่างน้อย 1 วิธี สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

1. การแสดงตัวตน (Identification) คือ ขั้นตอนป้อนชื่อผู้ใช้ (Username)
2. การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนป้อนรหัสผ่าน (Password)

ส่วนที่ 4
นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Third Party Access ControlPolicy)

1. วัตถุประสงค์

การใช้บริการจากหน่วยภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานเจ้าของระบบสารสนเทศ
3. ผู้ดูแลระบบที่ได้รับมอบหมาย
4. เจ้าหน้าที่ประจำโครงการขององค์กร

3. แนวปฏิบัติทั่วไป

3.1 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

3.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

3.2.1 บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

3.2.2 จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

3.2.2.1 เหตุผลในการขอใช้

3.2.2.2 ระยะเวลาในการใช้

3.2.2.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

3.2.2.4 การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

3.2.2.5 การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

3.2.3 หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

3.2.4 องค์กรควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศที่เข้าไปปฏิบัติงาน

3.2.5 เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนาม ในสัญญาไม่เปิดเผยข้อมูล

3.2.6 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

3.2.7 องค์กรมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจว่า องค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

3.2.8 ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ 5
นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
(Network Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศขององค์กร โดยมีการกำหนดนโยบายและแนวปฏิบัติควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

3.1 การใช้งานบริการเครือข่าย

3.1.1 ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบขององค์กร

3.1.2 องค์กรไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อ หรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูล โดยคิดค่าบริการการให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

3.1.3 ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียวองค์กรไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

3.1.4 ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

3.1.5 องค์กรให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

3.1.6 บัญชีผู้ใช้งาน (User Account) ที่องค์กรให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้นรวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

3.1.7 กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

3.1.8 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

3.1.9 ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิงในระหว่างปฏิบัติงาน

3.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน

จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

3.2.1 ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

3.2.2 ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูลโดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ด เป็นต้น

3.2.3 จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนสำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงานอย่างน้อย 1 วิธี

3.2.4 ต้องมีการตรวจสอบผู้ใช้งานเมื่อมีเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต

3.3 ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่องค์กรมีแนวทางปฏิบัติ ดังนี้

3.3.1 ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิบุคคลในการเข้า - ออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์และเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

3.3.2 สิทธิในการเข้า – ออกห้องต่าง ๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจากหัวหน้ากลุ่มบริหารจัดการระบบเครือข่ายและความปลอดภัยเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

3.3.3 ต้องจัดทำระบบเก็บบันทึกการเข้า - ออกองค์กร ตามกระบวนการที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า - ออกพื้นที่”

3.3.4 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้า - ออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

3.3.5 การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า - ออกพื้นที่”

3.4 ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติ ดังนี้

3.4.1 ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า - ออกพื้นที่”

3.4.2 ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กรมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า - ออก ตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า - ออกพื้นที่” ให้ถูกต้องชัดเจน

3.4.3 เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน

3.5 การระบุอุปกรณ์บนเครือข่าย

3.5.1 ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการรายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

3.5.2 กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอกต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

3.5.3 อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

3.5.4 ผู้ขอใช้บริการต้องทำหนังสือเป็นลายลักษณ์อักษรถึงผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง “การขอเชื่อมต่อเครือข่าย” และต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

3.6 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

3.6.1 ผู้ดูแลระบบต้องกำหนดการเปิด - ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่าย

3.6.2 บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องควบคุมระบบเครือข่าย/ระบบคอมพิวเตอร์ จะต้องลงชื่อเข้า-ออกใน “แบบฟอร์มการเข้า - ออกพื้นที่” ให้ถูกต้องและได้รับการอนุมัติจากหัวหน้ากลุ่มบริหารจัดการระบบเครือข่ายและความปลอดภัยเทคโนโลยีสารสนเทศก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

3.6.3 บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษาบริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

3.6.4 ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

3.7 การแบ่งแยกเครือข่าย

3.7.1 องค์กรแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

3.7.2 องค์กรจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอกเพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ

3.7.3 องค์กรติดตั้ง Firewall เพื่อป้องกันทางเข้าเครือข่ายจากผู้ไม่หวังดี

3.8 การควบคุมการเชื่อมต่อทางเครือข่าย

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

3.8.1 มีการตรวจสอบการเชื่อมต่อเครือข่าย

3.8.2 จำกัดสิทธิความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

3.8.3 ระบุอุปกรณ์เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

3.8.4 มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

3.8.5 ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

3.9 การควบคุมการจัดเส้นทางบนเครือข่าย

ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

3.9.1 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

3.9.2 กำหนดให้มีการแปลงหมายเลขเครือข่ายเพื่อแยกเครือข่ายย่อย

3.9.3 กำหนดมาตรการการบังคับใช้เส้นทางเครือข่ายสามารถเชื่อมเครือข่ายปลายทางผ่านทางที่กำหนดไว้หรือจำกัดสิทธิในการใช้บริการเครือข่าย

ส่วนที่ 6
นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการรวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัดอันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และมีความพร้อมใช้งานอยู่เสมอ (Availability)

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

3.1 ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

3.2 ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

3.3 ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ Username และ Password ทุกครั้ง

3.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

3.5 ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.6 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงเว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

3.7 ซอฟต์แวร์ที่องค์กรใช้มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

3.8 ซอฟต์แวร์ที่องค์กรจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

3.9 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นขององค์กรเพื่อประโยชน์ทางการค้า

3.10 ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

3.11 ห้ามผู้ใช้ระบบสารสนเทศขององค์กร เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

4. แนวปฏิบัติการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

4.1 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศเพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

4.2 ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

4.3 ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่ายหรือจ่ายแจกให้ผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

4.4 ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

5. แนวปฏิบัติการใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities)

5.1 มีการกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ระดับสิทธิของผู้ขออนุมัติ และการระบุและพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน

5.2 ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

5.3 มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

5.4 ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งานรวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

6. แนวปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

6.1 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานอุปกรณ์เครือข่าย เป็นต้น มีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 45 นาที หรือตามความเหมาะสมของระบบสารสนเทศ

6.2 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 45 นาที หรือตามความเหมาะสมของระบบสารสนเทศ เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

6.3 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้น สำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ส่วนที่ 7
นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศขององค์กรและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรได้อย่างถูกต้อง

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานที่ใช้โปรแกรมประยุกต์หรือแอพพลิเคชั่น
3. หน่วยงานที่เป็นเจ้าของโปรแกรมประยุกต์หรือแอพพลิเคชั่น
4. ผู้ดูแลระบบที่ได้รับมอบหมาย
5. เจ้าหน้าที่ประจำโครงการขององค์กร

3. แนวปฏิบัติการจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

3.1 ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กรควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

3.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

3.3 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกินกว่า 45 นาที หรือตามความเหมาะสมของระบบสารสนเทศ ระบบจะยุติการใช้งาน (Session Time-out) ผู้ใช้งานต้องทำการ Login เข้าระบบสารสนเทศอีกครั้ง

3.4 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

3.4.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

3.4.2 ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

3.4.3 กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

3.4.4 กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

3.4.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

3.4.6 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

3.5 เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์องค์กรให้กำหนดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญที่องค์กรพัฒนาในรูปแบบของ Webbase Application โดยเข้าถึงได้ผ่านระบบเครือข่ายภายในซึ่งสามารถใช้งานได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายดังกล่าว

3.6 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

3.6.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

3.6.2 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

3.6.3 กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3.6.4 การรับ - ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

3.6.5 กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

3.6.6 กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

4. แนวปฏิบัติการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

4.1 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ 45 นาที หรือตามความเหมาะสมของระบบสารสนเทศ ต่อการเชื่อมต่อหนึ่งครั้ง

4.2 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูงระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์กร) เป็นต้น มีการจำกัดช่วงระยะเวลาในการเชื่อมต่อ

4.3 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศที่ต้องมีการจำกัดช่วงระยะเวลาการใช้งานมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ทุก ๆ 45 นาที หรือตามความเหมาะสมของระบบสารสนเทศ

5. แนวปฏิบัติการจัดการกับระบบซึ่งไวต่อการรบกวน

5.1 ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อองค์กร ได้แก่ ระบบ GFMIS หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ เป็นระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณการบัญชีการจัดซื้อจัดจ้างการเบิกจ่ายและการบริหารทรัพยากร ซึ่งดูแลรับผิดชอบโดยกรมบัญชีกลางจะได้รับการแยกออกจากระบบงานอื่น ๆ ขององค์กร

5.2 ระบบซึ่งไวต่อการรบกวนต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วนและต้องมีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นเข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

6. แนวปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

6.1 ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อนซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกลก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

6.2 ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์กรก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

6.3 ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึกอาคารสำนักงานและสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร

6.4 ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรในสถานที่ดังกล่าว

6.5 ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรรวมทั้งมาตรการควบคุมการใช้เครือข่ายไร้สายที่บ้าน

6.6 ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่องค์กรต้องการ

6.7 ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกลการจัดเก็บข้อมูลและอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

6.8 องค์กรไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยองค์กร

6.9 องค์กรต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกลชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

6.10 องค์กรต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกลการกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงานและการคืนอุปกรณ์ที่ใช้งาน เมื่อมีการยกเลิกการปฏิบัติงาน

7. แนวปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

7.1 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ มีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา 45 นาที หรือตามความเหมาะสมของระบบสารสนเทศ

7.2 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา 45 นาที หรือตามความเหมาะสมของระบบสารสนเทศ เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

7.3 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้น สำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ส่วนที่ 8
นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
(Use of Personal Computer Policy)

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ จัดทำขึ้นเพื่อช่วยให้ผู้ใช้ทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้ควรทำความเข้าใจ และปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้เป็นความลับ มีความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. ผู้ใช้งาน

3. แนวปฏิบัติทั่วไป

3.1 เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร

3.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

3.3 ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร

3.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ขององค์กรเท่านั้น

3.5 การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

3.6 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

3.7 ไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

3.8 ไม่ควรสร้าง Shortcut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร

3.9 ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติดังนี้

3.9.1 ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

3.9.2 ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

4. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

4.1 ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

4.2 ผู้ใช้ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

4.3 ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Logout ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver เมื่อไม่มีการใช้งานโดยตั้งเวลาประมาณ 10 นาที

4.4 มีการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ เมื่อไม่มีการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

5. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้ปฏิบัติตามแนวทางการใช้รหัสผ่านตาม ข้อ 6 (6.7) “การใช้งานรหัสผ่าน” ในนโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

6. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

6.1 ผู้ใช้ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

6.2 ผู้ใช้มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

6.3 ผู้ใช้ควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

6.4 ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

6.5 ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

7. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

7.1 ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD DVD External Hard Disk เป็นต้น

7.2 ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

7.3 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

ส่วนที่ 9
นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Use of Notebook Computer Policy)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์กร เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์กรให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. ผู้ใช้งาน

3. แนวปฏิบัติทั่วไป

3.1 เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร

3.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพา หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

3.3 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

3.4 การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

3.5 ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

3.6 ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

3.7 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

3.8 ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสียงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

3.9 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

3.10 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

3.11 ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์

3.12 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

3.13 ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

3.14 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

3.15 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

3.16 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

3.17 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

3.18 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

4. แนวปฏิบัติการป้องกันความปลอดภัยทางด้านกายภาพ

4.1 ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

4.2 ผู้ใช้ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน หรือความชื้น หรือฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

4.3 ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

5. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

5.1 ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

5.2 ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในข้อ 6 (6.7) “การใช้งานรหัสผ่าน” ในนโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

5.3 ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

5.4 ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

6. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้ปฏิบัติตามแนวทางการใช้รหัสผ่านตาม ข้อ 6 (6.7) “การใช้งานรหัสผ่าน” ในนโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

7. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

7.1 ผู้ใช้ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

7.2 ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

7.3 หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

8. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

8.1 ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

8.2 ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

8.3 แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

8.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ 10
นโยบายการใช้งานอุปกรณ์สื่อสารแบบพกพา
(Smart Device Policy)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารแบบพกพาที่เป็นทรัพย์สินของทางราชการ ได้แก่ แท็ปเล็ต (Tablet) หรือ สมาร์ทโฟน (Smartphone) เพื่อให้การใช้งานอย่างเป็นระบบ มีแบบแผนและสามารถจัดการปัญหาความปลอดภัยที่อาจจะเกิดขึ้น ได้อย่างรวดเร็ว ในการเชื่อมต่อเครือข่าย ซึ่งอาจมีการถูกโจมตีและเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. ผู้ใช้งาน

3. แนวปฏิบัติทั่วไป

3.1 ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

3.2 ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของอุปกรณ์สื่อสารแบบพกพาที่เป็นขององค์กรและรักษาสภาพให้มีสภาพเดิม

3.3 ไม่ควรใส่อุปกรณ์สื่อสารแบบพกพาที่เป็นขององค์กรในกระเป๋าที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

3.4 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอให้เป็นรอยขีดข่วนหรือทำให้จอแตกเสียหายได้

3.5 ไม่ควรใช้หรือวางอุปกรณ์สื่อสารแบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

3.6 ไม่ควรวางอุปกรณ์สื่อสารแบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

3.7 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

4. แนวปฏิบัติการป้องกันความปลอดภัยทางด้านกายภาพ

4.1 ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

4.2 ผู้ใช้ไม่ควรเก็บหรือใช้งานอุปกรณ์สื่อสารแบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

4.3 ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

4.4 ห้ามมิให้ผู้ใช้ติดตั้งหรือเปลี่ยนแปลงแก้ไขซอฟต์แวร์ผิดกฎหมายบนอุปกรณ์สื่อสารแบบพกพา (Jailbreak)

5. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ

5.1 กรณีที่ต้องการเชื่อมต่อระบบเครือข่ายต้องปฏิบัติตามนโยบายส่วนที่ 14 นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

5.2 กรณีที่ต้องการเข้าถึงระบบสารสนเทศต้องปฏิบัติตามนโยบายส่วนที่ 3 นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 11
นโยบายการการประชุมผ่านสื่ออิเล็กทรอนิกส์
(Conference Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและแนวทางในการประชุมผ่านสื่ออิเล็กทรอนิกส์ขององค์กรให้กระทำผ่านระบบควบคุมการประชุมที่มีกระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การประชุมผ่านสื่ออิเล็กทรอนิกส์สามารถดำเนินการได้อย่างมีประสิทธิภาพ

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. ผู้ดูแลระบบที่ได้รับมอบหมาย
3. ผู้ควบคุมระบบ

3. คำจำกัดความ

3.1 ระบบควบคุมการประชุม หมายความว่า ระบบเครือข่ายคอมพิวเตอร์หรืออุปกรณ์สื่อสารอิเล็กทรอนิกส์ใด ๆ ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่เชื่อมโยงกันเป็นเครือข่าย และมีการสื่อสารข้อมูลกัน โดยใช้เทคโนโลยีสารสนเทศและการสื่อสารหรือการโทรคมนาคม เพื่อให้ผู้ร่วมประชุมสามารถเข้าถึงและใช้งานสำหรับการประชุมผ่านสื่ออิเล็กทรอนิกส์ไม่ว่าจะเป็นการประชุมด้วยเสียงหรือทั้งเสียงและภาพ

3.2 การประชุมผ่านสื่ออิเล็กทรอนิกส์ หมายความว่า การประชุมของกรมประมงที่กระทำผ่านสื่ออิเล็กทรอนิกส์โดยผู้ร่วมประชุมมิได้อยู่ในสถานที่เดียวกันและสามารถประชุมปรึกษาหารือและแสดงความคิดเห็นระหว่างกันได้ผ่านสื่ออิเล็กทรอนิกส์

3.3 ผู้ควบคุมระบบ หมายความว่า ผู้ทำหน้าที่ดูแลและบริหารจัดการระบบการประชุมผ่านสื่ออิเล็กทรอนิกส์ ตั้งแต่เริ่มทำการประชุมจนกระทั่งเสร็จสิ้นการประชุมในแต่ละครั้ง

4. บทบาทและความรับผิดชอบของผู้ควบคุมระบบ

4.1 ทำให้ผู้ร่วมประชุมสามารถสื่อสารถึงกันได้ด้วยเสียงหรือทั้งเสียงและภาพ โดยผ่านเทคโนโลยีสารสนเทศและการสื่อสารหรือการโทรคมนาคม ทั้งประเภทที่ใช้สายและไร้สาย ได้แก่ เครือข่ายโทรศัพท์ เครือข่ายคอมพิวเตอร์ภายในองค์กรหรือแลน (Local Area Network : LAN) อินเทอร์เน็ตความเร็วสูงแบบวงจรเช่า (Leased Line) เครือข่ายบริการสื่อสารร่วมระบบดิจิทัลหรือไอเอสดีเอ็น (Integrated Services Digital Network : ISDN หรือเครือข่ายแบบ Wide Area Network : WAN) เครือข่ายอินเทอร์เน็ต เครือข่ายไมโครเวฟ เครือข่ายวิทยุโทรคมนาคม เครือข่ายการสื่อสารโดยใช้ดาวเทียม เป็นต้น

4.2 เชื่อมโยงสถานที่ประชุมตั้งแต่สองแห่งขึ้นไปเข้าด้วยกัน

4.3 ทำให้ผู้ร่วมประชุมสามารถสื่อสารหรือมีปฏิสัมพันธ์กันได้สองทาง

4.4 มีอุปกรณ์นำเข้าข้อมูลจากที่หนึ่งไปยังอีกที่หนึ่งโดยผ่านเทคโนโลยีสารสนเทศและการสื่อสารหรือการโทรคมนาคม ได้แก่ โทรศัพท์ ไมโครโฟน เครื่องคอมพิวเตอร์ เครื่องโทรสาร เป็นต้น

4.5 มีอุปกรณ์เพื่อทำหน้าที่เชื่อมโยงหรือแปลงสัญญาณเสียงหรือทั้งเสียงและภาพที่เหมาะสมกับเทคโนโลยีสารสนเทศและการสื่อสาร หรือการโทรคมนาคมที่เอื้ออำนวยต่อการรับซมและรับฟัง ของผู้ร่วมประชุม แล้วแต่กรณี

5. แนวปฏิบัติทั่วไปในการประชุมของผู้ร่วมประชุม

5.1 มีอุปกรณ์แสดงผลข้อมูลที่ถูกส่งผ่านมาจากระบบเทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือการโทรคมนาคมให้เป็นข้อมูลที่ผู้ร่วมประชุมสามารถรับรู้ได้ เช่น ลำโพง จอภาพ เครื่องฉายภาพวีดิทัศน์ (Video Projector) อุปกรณ์แสดงผลที่เป็นเอกสาร (Hard Copy) เป็นต้น

5.2 กรณีมีการประชุมในห้องประชุมจะต้องมีการติดตั้งวัสดุเพื่อทำหน้าที่ซับเสียงที่เหมาะสมกับสภาพของห้องประชุม เพื่อป้องกันเสียงก้องหรือเสียงสะท้อน

5.3 เมื่อผู้ทำหน้าที่ประธานในที่ประชุมกำหนดให้จัดการประชุมผ่านสื่ออิเล็กทรอนิกส์ในการประชุมครั้งใดแล้ว ผู้มีหน้าที่จัดการประชุมต้องดำเนินการเพื่อให้มีการใช้ระบบควบคุมการประชุมเป็นลายลักษณ์อักษรหรือจดหมายอิเล็กทรอนิกส์หรือโดยวิธีการใด ๆ ก่อนจัดการประชุม โดยจะต้องจัดให้มีผู้ควบคุมระบบที่สามารถบริหารจัดระบบเพื่อตรวจสอบการทำงานและแก้ไขปัญหาให้กับผู้ร่วมประชุมโดยการเข้าถึงระบบแบบระยะไกล (Remote Access) ได้ด้วย ทั้งนี้ ระบบควบคุมการประชุมจะต้องพร้อมทำงานก่อนการประชุมและจะต้องมีการทดสอบระบบเสียง ภาพกับผู้เข้าร่วมประชุมก่อนการประชุมทุกครั้ง

5.4 ในการบริหารจัดการระบบตามข้อ 5.3 ประธานในที่ประชุม และ/หรือผู้ควบคุมระบบจะต้องสามารถตัดสัญญาณเสียงหรือสัญญาณภาพหรือทั้งสัญญาณเสียงและสัญญาณภาพ หรือหยุดการส่งข้อมูลให้เครื่องหรืออุปกรณ์สื่อสารของผู้ร่วมประชุมเครื่องใดเครื่องหนึ่งภายในระบบได้ทันทีหากมีเหตุจำเป็นหรือมีกรณีฉุกเฉิน

5.5 ในระหว่างการประชุมผู้ร่วมประชุมทุกคนต้องสามารถดูข้อมูลการประชุมที่กำลังนำเสนอในที่ประชุมผ่านเครื่องหรืออุปกรณ์สื่อสารของตนเองได้ตลอดระยะเวลาการประชุม เว้นแต่จะมีการตัดสัญญาณเสียงหรือสัญญาณภาพหรือทั้งสัญญาณเสียงและสัญญาณภาพ หรือหยุดการส่งข้อมูลให้เครื่องหรืออุปกรณ์สื่อสารของผู้ร่วมประชุมนั้น โดยมีเหตุจำเป็นหรือมีกรณีฉุกเฉินตามข้อ 5.4

6. แนวปฏิบัติทั่วไปของการบันทึกเสียงหรือทั้งเสียงและภาพของผู้ร่วมประชุม

6.1 มีเทคโนโลยีหรือมาตรการป้องกันมิให้มีการเปลี่ยนแปลงหรือแก้ไขเกิดขึ้นกับข้อมูลนั้น เว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใด ๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงซึ่งไม่มีผลต่อความหมายของข้อมูลนั้น เพื่อให้สามารถยืนยันได้ว่าได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อมูลตั้งแต่การสร้างจนเสร็จสมบูรณ์และสามารถแสดงข้อมูลนั้นในภายหลังได้

6.2 ในกรณีที่มีการบันทึกเสียงหรือทั้งเสียงและภาพด้วยระบบควบคุมการประชุมให้มีวิธีการที่เชื่อถือได้ในการระบุตัวตนผู้ที่เกี่ยวข้องกับระบบควบคุมการประชุม เพื่อให้สามารถยืนยันได้ว่าข้อมูลที่ได้บันทึกไว้ได้ดำเนินการโดยผู้มีสิทธิในการเข้าถึงเท่านั้น โดยอย่างน้อยต้องครอบคลุมเรื่อง ดังต่อไปนี้

6.2.1 การระบุตัวตน (Identification)

6.2.2 การยืนยันตัวตน (Authentication)

6.2.3 การอนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)

6.2.4 ความรับผิดชอบต่อผลของการกระทำ (Accountability)

7. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ

7.1 กรณีที่ต้องการเชื่อมต่อระบบเครือข่ายต้องปฏิบัติตามนโยบาย ส่วนที่ 5 นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control) หรือส่วนที่ 14 นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

7.2 กรณีที่ต้องการเข้าถึงระบบสารสนเทศต้องปฏิบัติตามนโยบาย ส่วนที่ 3 นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 12
นโยบายการใช้งานอินเทอร์เน็ต
(Internet Security Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. ผู้ดูแลระบบที่ได้รับมอบหมาย
4. ผู้ใช้งาน

3. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

3.1 ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy Firewall IPS/IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem ยกเว้นแต่มีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษรแล้ว

3.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

3.3 ในการรับ - ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการสแกนไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับ - ส่งข้อมูลทุกครั้ง

3.4 ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

3.5 ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

3.6 ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

3.7 ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

3.8 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

3.9 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

3.10 ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ต ก่อนนำข้อมูลไปใช้งาน

3.11 ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

3.12 ในการเสนอความคิดเห็นผ่านเว็บบอร์ด (Webboard) ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กร และต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

3.13 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ 13
นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์
(E-mail Policy)

1. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. ผู้ดูแลระบบที่ได้รับมอบหมาย
4. ผู้ใช้งาน

3. แนวปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

3.1 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

3.2 ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

3.3 สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

3.4 การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามข้อ 6 (6.7) “การใช้งานรหัสผ่าน” ในนโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.5 รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

3.6 ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการ Logout ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

3.7 ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

3.8 ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3 - 6 เดือน

3.9 ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

3.10 ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่าน รับ - ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

3.11 ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น

3.12 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

3.13 ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

3.14 ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

3.15 ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพ หรือรับ - ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

3.16 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

3.17 ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

3.18 ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

3.19 ผู้ใช้ไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้น ไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ส่วนที่ 14
นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. ผู้ดูแลระบบที่ได้รับมอบหมาย
4. ผู้ใช้งาน

3. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

3.1 ผู้ใช้งานจะต้องมีบัญชีผู้ใช้งานระบบเครือข่ายขององค์กร จึงจะสามารถใช้งานระบบเครือข่ายไร้สายนี้ได้ กรณีที่องค์กรมีนโยบายในการใช้ชื่อผู้ใช้กลาง ให้ผู้ใช้งานติดต่อเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อรับค่า SSID (Service Set Identifier) และ Network Key ในการระบุตัวตนก่อนเข้าใช้งานระบบเครือข่ายไร้สาย

3.2 ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับ - ส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

3.3 ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น

3.4 ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

3.5 ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อ Login และรหัสผ่านที่มีการคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

3.6 ผู้ดูแลระบบต้องกำหนดค่าใช้ WEP หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น

3.7 ผู้ดูแลระบบต้องจะมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

3.8 ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

3.9 ในการใช้งานเครือข่ายไร้สายผู้ใช้งานต้องปฏิบัติตามนโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด ทางองค์กรสงวนสิทธิ์ในการยกเลิกสิทธิในการเข้าใช้เครือข่ายไร้สาย โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

4. แนวปฏิบัติในการเข้าใช้เครือข่ายไร้สายกรมประมง

4.1 การตรวจสอบยืนยันตัวตนการเข้าใช้เครือข่ายไร้สายกรมประมง สามารถแบ่งเป็น 3 กลุ่ม ดังนี้

4.1.1 กลุ่มผู้บริหารกรมประมง (DOF-VIP) สำหรับผู้บริหารกรมประมง และผู้อำนวยการกองระดับสูงหรือเทียบเท่า ยืนยันตัวตนโดยการลงทะเบียนหมายเลข Mac Address ของอุปกรณ์ (Notebook, Tablet, Smartphone) เพียง 1 ครั้งต่อ 1 อุปกรณ์ สามารถเชื่อมต่อ Wifi ชื่อ DOF-VIP ได้ทุกห้องประชุม

4.1.2 กลุ่มเจ้าหน้าที่กรมประมงส่วนกลาง (DOF-Officer) สำหรับเจ้าหน้าที่กรมประมงส่วนกลาง ทั้งข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว จ้างเหมา ยืนยันตัวตนโดยป้อน Username และ Password เข้าใช้ Internet กรมประมง ผ่านหน้าเว็บไซต์ยืนยันตัวตนและต้องทำการยืนยันตัวตนทุกครั้งที่เข้าใช้งาน สามารถเชื่อมต่อ Wifi ชื่อ DOF-Officer ได้ทุกห้องประชุมกำหนดตัด session ทุก 3 ชั่วโมง

4.1.3 กลุ่มผู้ใช้งานชั่วคราว (DOF-Guest) สำหรับเจ้าหน้าที่กรมประมงส่วนภูมิภาค บุคคลภายนอกที่มาประชุมผู้มาติดต่อขอรับบริการจากหน่วยงานกรมประมง ยืนยันตัวตนโดยป้อน Username และ Password ที่แจกให้รายครั้งผ่านหน้าเว็บไซต์ยืนยันตัวตน ซึ่งจะมีการจัดเก็บเลขบัตรประจำตัวประชาชนของผู้ใช้งาน สามารถใช้งานได้ตามระยะเวลาที่กำหนดโดยประมาณ 1 วัน และสามารถเชื่อมต่อ Wifi ชื่อ DOF-Guest ได้ทุกห้องประชุม

4.1.4 การเข้าใช้งานจะจำกัดเพียง 1 Session ต่อ 1 อุปกรณ์เท่านั้น ไม่สามารถใช้ Username เดียวกันเข้าใช้พร้อมกันได้

ส่วนที่ 15
นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี
(Virus and Malicious Software Protection Policy)

1. วัตถุประสงค์

เพื่อควบคุมและป้องกันซอฟต์แวร์และข้อมูลขององค์กร จากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. ผู้ดูแลระบบที่ได้รับมอบหมาย
4. ผู้ใช้งาน

3. แนวปฏิบัติในการป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

3.1 ก่อนนำซอฟต์แวร์จากภายนอกมาใช้งานภายในองค์กร ผู้ใช้งานต้องทำการตรวจสอบซอฟแวร์ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้น ๆ ไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่

3.2 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชั่นล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และเครื่องเซิร์ฟเวอร์

3.3 ผู้ดูแลระบบต้องกำหนดให้โปรแกรมค้นหาไวรัสทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะที่มีการใช้ระบบด้วย นอกจากนี้ผู้ดูแลระบบต้องมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ

3.4 ผู้ดูแลระบบต้องทำการตรวจทานระบบข้อมูลเพื่อตรวจหาไวรัสและซอฟต์แวร์อันตรายอยู่เป็นประจำ

3.5 ผู้ใช้งานต้องตรวจหาไวรัสของไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตก่อนนำไปใช้งาน

3.6 ห้ามมิให้เจ้าหน้าที่ดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนาไวรัสหรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ

3.7 ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกองค์กรมาใช้ ผู้ใช้งานสื่อข้อมูลนั้นต้องตรวจสอบไวรัสคอมพิวเตอร์ก่อนใช้งานทุกครั้ง

3.8 ผู้ใช้งานจะต้องตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ หากพบว่าโปรแกรมไม่ทำงานตามปกติ ให้แจ้งผู้ดูแลระบบเพื่อดำเนินการแก้ไข

3.9 ห้ามมิให้ผู้ใช้งานดำเนินการถอนโปรแกรมป้องกันไวรัสโดยพละการ หากมีความจำเป็นให้แจ้งผู้ดูแลระบบเป็นผู้ดำเนินการ

3.10 หากเครื่องคอมพิวเตอร์ไม่ติดตั้งโปรแกรมป้องกันไวรัส ตามที่หน่วยงานกำหนดจะไม่สามารถเข้าใช้งานระบบอินเทอร์เน็ตของกรมประมงได้

3.11 คอมพิวเตอร์ของผู้ใช้งานจะต้องติดตั้งโปรแกรมป้องกันไวรัส ตามที่หน่วยงานกำหนด เว้นแต่มีเหตุจำเป็นที่ไม่สามารถติดตั้งโปรแกรมป้องกันไวรัสของกรมฯ ได้ เช่น เครื่องไม่รองรับการติดตั้งโปรแกรมฯ เป็นต้น โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ส่วนที่ 16
นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก
(Firewall & Intrusion Prevention System Policy)

1. วัตถุประสงค์

เพื่อควบคุมการใช้งานเครือข่ายและกรองแพ็กเก็ตที่ผ่านเข้ามาในเครือข่ายองค์กร

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวปฏิบัติในการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

3.1 อนุญาตเฉพาะบริการเครือข่ายที่จำเป็นต่อการใช้งานบริการเครือข่ายอื่น ๆ ที่เหลือปิดให้หมด

3.2 ไม่อนุญาตให้สแกนเพื่อตรวจสอบเครือข่ายด้วยโปรแกรมประเภท Network Scanning Tools เช่น Nmap เป็นต้น

3.3 ปิดบริการรวมทั้งซอฟต์แวร์ที่ไม่จำเป็นบนไฟร์วอลล์

3.4 จำกัดบริการเครือข่ายที่ทำงานบนไฟร์วอลล์ให้มีน้อยที่สุดโดยให้แยกบริการอื่น ๆ เหล่านั้นไปทำงานบนเครื่องอื่น

3.5 จำกัดชื่อบัญชีผู้ใช้บนเครื่องไฟร์วอลล์ให้มีน้อยที่สุดและไม่รันไฟร์วอลล์โดยใช้ชื่อบัญชีผู้ใช้ที่เป็น Root หรือ Administrator

3.6 เปลี่ยนรหัสผ่านสำหรับ Root หรือ Administrator ที่ผู้ขายกำหนดมาให้ให้เป็นรหัสอื่นที่ยากต่อการเดา

3.7 ควรใช้ไฟร์วอลล์หลายชนิดร่วมกัน เช่น ไฟร์วอลล์แบบกรองแพ็กเก็ต ไฟร์วอลล์แบบพร็อกซี่ เพื่อเป็นการเสริมความมั่นคงปลอดภัยในแง่มุมที่ต่างกัน

3.8 ควรใช้ระบบอื่นทำงานร่วมกับไฟร์วอลล์ ได้แก่ ระบบป้องกันการบุกรุก (IPS) ไฟร์วอลล์ส่วนตัว (Personal Firewall) โปรแกรมป้องกันไวรัส (Antivirus) โปรแกรมกรองอีเมล์และกรองเว็บ (Anti Spam) ซึ่งเป็นการเสริมการรักษาความมั่นคงปลอดภัยภาพรวมได้สูงขึ้น

3.9 กำหนดกฎในไฟร์วอลล์ให้กรองทิ้งแพ็กเก็ตที่ไม่ประสงค์ดีตามรายการช่องโหว่ที่แพร่ระบาดอยู่ในปัจจุบันเสมอ

3.10 ป้องกันการเข้าถึงทางกายภาพต่อไฟร์วอลล์ให้มีความแข็งแกร่ง เช่น จัดทำเป็นห้องที่มีการควบคุมการเข้า-ออกอย่างเข้มงวด

3.11 หมั่นตรวจสอบกฎของไฟร์วอลล์ เพื่อกำจัดกฎที่ไม่มีความจำเป็นทิ้งไป เพื่อเพิ่มประสิทธิภาพของการประมวลผลกฎที่กำหนดไว้ของไฟร์วอลล์

3.12 เมื่อเพิ่มกฎข้อใหม่เข้าไปในไฟร์วอลล์ ตรวจสอบว่ากฎที่ใส่เข้าไปนั้นไม่ขัดแย้งกับกฎที่มีอยู่แล้วเดิม รวมทั้งทดสอบด้วยว่าไฟร์วอลล์สามารถป้องกันได้จริงตามกฎข้อใหม่นั้น

3.13 ตรวจสอบว่ากฎที่กำหนดไว้บนไฟร์วอลล์ไม่มีข้อใดขัดแย้งกับนโยบายความมั่นคงปลอดภัยขององค์กรอย่างน้อยปีละครั้ง

3.14 ไม่อนุญาตให้เข้าถึงไฟร์วอลล์จากทางไกลโดยโปรแกรมประเภท Telnet หรือแม้แต่ SSH โดยการเข้าถึงให้ทำได้จากตัวเครื่องไฟร์วอลล์โดยตรง

3.15 สร้างความแข็งแกร่งให้กับระบบปฏิบัติการของไฟร์วอลล์ โดยการ Update Patch อยู่เสมอ

3.16 ตรวจสอบและติดตั้งโปรแกรมอุดช่องโหว่สำหรับระบบปฏิบัติการของไฟร์วอลล์อย่างสม่ำเสมอ

3.17 ก่อนการอัพเกรดหรือแก้ไขช่องโหว่ของไฟร์วอลล์ให้ทำสำรองข้อมูลแบบ Full Backup ของเครื่องไฟร์วอลล์นั้นเก็บไว้ก่อน หากมีปัญหาจะได้นำกลับมาติดตั้งและใช้งานได้อย่างรวดเร็ว

3.18 ใช้ไฟร์วอลล์ร่วมกับเราท์เตอร์ เพื่อป้องกันปัญหา DoS (Denial of Service) และปัญหาการเจาะระบบเข้าสู่ไฟร์วอลล์ได้โดยตรง

3.19 ใช้ไฟร์วอลล์เพื่อกั้นเครือข่ายภายใน ในกรณีที่มีความจำเป็น เช่น เครือข่ายส่วนนั้นอนุญาตให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นในการเข้าถึง

3.20 บันทึกข้อมูล Log ของการเข้าถึงไฟร์วอลล์เก็บไว้ รวมทั้งหากไฟร์วอลล์มีขีดความสามารถในการแจ้งเตือนให้เปิดใช้ขีดความสามารถนี้ด้วย

3.21 ใช้เซิร์ฟเวอร์ เช่น Syslog แยกต่างหากอีกเครื่องหนึ่งจากเครื่องของไฟร์วอลล์ เพื่อเก็บบันทึกข้อมูล Log ของการเข้าถึงไฟร์วอลล์ไว้บนเซิร์ฟเวอร์นั้น ซึ่งจะทำให้การเปลี่ยนแปลงแก้ไขข้อมูล Log โดยผู้บุกรุกทำได้ยากขึ้น

3.22 หากหน่วยงานอื่นต้องการนำระบบขึ้น จะต้องทำเป็นหนังสือผ่านผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร แจ้งเจ้าหน้าที่ให้ดำเนินการเป็นกรณีไป

หมวดที่ 2 ระบบสารสนเทศและระบบสำรองของสารสนเทศ

ส่วนที่ 17
นโยบายการสำรองและกู้คืนข้อมูล
(Backup and Recovery Policy)

1. วัตถุประสงค์

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. หน่วยงานภายในกรมประมง
3. หน่วยงานที่เป็นเจ้าของระบบสารสนเทศ
4. ผู้ดูแลระบบที่ได้รับมอบหมาย
5. ผู้ใช้งาน

3. แนวปฏิบัติในการคัดเลือกการสำรองข้อมูล

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

3.1 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรองและจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

3.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูลหากระบบใดที่มีการเปลี่ยนแปลงบ่อยควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

3.3 กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้และความถี่ในการสำรอง

3.4 กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

3.5 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

3.6 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศข้อมูล Configuration ข้อมูลในฐานข้อมูล เป็นต้น

3.7 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

3.8 จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

3.9 ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

3.10 ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

3.11 จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

3.12 กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

4. แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามแนวทางต่อไปนี้

4.1 มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์โดยมีรายละเอียดอย่างน้อย ดังนี้

4.1.1 มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

4.1.2 มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นและกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

4.1.3 มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

4.1.4 มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

4.1.5 มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

4.1.6 การสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

4.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจอย่างน้อยปีละ 1 ครั้ง

5. แนวปฏิบัติในการสำรองและกู้คืนข้อมูล

เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ฮาร์ดดิสก์เสียหาย ไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูลโดยผู้ใช้งานเอง โดยมีมาตรการ ดังนี้

5.1 การสำรองข้อมูล

5.1.1 ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบไม่ต่ำกว่า 1 ครั้งต่อเดือน

5.1.2 ผู้ดูแลระบบต้องตั้งค่าสำรองข้อมูลอัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (Web Server)

5.1.3 ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป จะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม ไม่ต่ำกว่า 1 ครั้งต่อเดือน

5.1.4 เมื่อองค์กรประกาศให้มีการสำรองข้อมูลเนื่องจากจะได้มีการดำเนินการที่อาจส่งผลต่อข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้ ผู้ใช้จะต้องทำการสำรองข้อมูลดังกล่าวภายในระยะเวลาที่กำหนด

5.1.5 หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บสำรองไว้ในรูปของเอกสารกระดาษ (Hard Copy)

5.1.6 แผนกผู้ดูแลระบบต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยต้องมีการทดสอบอย่างน้อยปีละ 1 ครั้ง ซึ่งการทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริง แต่ทดสอบบนระบบทดสอบ

5.1.7 ผู้ดูแลระบบต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กร และเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร โดยต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่สำคัญด้วย

5.2 การกู้คืนข้อมูล

เพื่อให้การฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลต่อเครื่องคอมพิวเตอร์ หรือการประมวลผลของคอมพิวเตอร์หยุดทำงานอย่างกะทันหัน หรือเปลี่ยนการทำงานไปจากเดิม ทำให้ไม่สามารถบันทึกข้อมูลได้ทันเวลา หรือไม่สามารถใช้งานคอมพิวเตอร์ได้ตามปกติ มีมาตรการในการกู้คืนข้อมูล ดังนี้

5.2.1 ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา

5.2.2 ผู้ดูแลระบบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่เพื่อทดแทนของเดิมที่เสียหาย

5.2.3 ผู้ดูแลระบบจะต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

หมวดที่ 3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ 18
นโยบายการตรวจสอบและประเมินความเสี่ยง

1. วัตถุประสงค์

1) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

2) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

3) เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

2. ผู้รับผิดชอบ

1) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3) ผู้ตรวจสอบภายใน

4) กลุ่มพัฒนาระบบบริหาร

3. แนวทางปฏิบัติ

1. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

1.1 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ 1 ครั้ง

1.2 ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

2. มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

2.1 มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ 1 ครั้ง

2.2 มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

2.3 มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

2.4 มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

2.4.1 กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว

2.4.2 ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งการทำลายหรือลบข้อมูลโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างเหมาะสม

2.4.3 กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

2.4.4 กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อก (Log) แสดงการเข้าถึง วันและเวลาที่เข้าถึงระบบ

2.4.5 ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ 19
นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. วัตถุประสงค์

การสอบทานการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มั่นใจว่านโยบายและมาตรฐานต่าง ๆ ด้านความปลอดภัยสารสนเทศมีการปฏิบัติตามอย่างมีประสิทธิผลในทางปฏิบัติ องค์กรจำเป็นต้องมีการตรวจสอบอย่างสม่ำเสมอ ทั้งทางด้านกระบวนการทำงานรวมถึงด้านเทคนิค ทั้งนี้ การตรวจสอบมิได้จำกัดเฉพาะหน่วยงานตรวจสอบหรือคณะทำงานสอบทาน แต่ยังรวมถึงการตรวจสอบภายในโดยหน่วยงานของตนเอง

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. กองบริหารจัดการเรือประมงและการทำการประมง
3. ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)
4. ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวทางปฏิบัติในการสอบทาน

3.1 การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.1.1 กำหนดให้มีคณะทำงานสอบทาน ระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

3.1.2 ดำเนินการสอบทานระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติงาน ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศว่าสอดคล้องกับนโยบายหรือไม่ โดยรายงานสรุปผลเป็นรายไตรมาสหรืออย่างน้อยทุก 6 เดือน ให้ CIO ทราบพร้อมเสนอแนะแนวทางปรับปรุงแก้ไขในกรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีจุดบกพร่อง

3.1.3 หัวหน้างานในแต่ละหน่วยงานต้องรับผิดชอบในการสอบทานอย่างสม่ำเสมอ ถึงการปฏิบัติงานว่าสอดคล้องกับนโยบาย และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารรับผิดชอบในการสนับสนุนด้านการให้คำแนะนำในการปฏิบัติตามข้อกำหนดด้านความปลอดภัยสารสนเทศที่เกี่ยวข้องกับการปฏิบัติงานดังกล่าว

3.1.4 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายในหน่วยงานภาครัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ 1 ครั้ง

3.1.5 รายการที่สอบทาน

3.1.5.1 การป้องกันการบุกรุกระบบ

3.1.5.2 การสำรองข้อมูล

3.1.5.3 การควบคุมการเข้าห้องควบคุมระบบเครือข่าย

3.1.5.4 การควบคุมผู้เข้า - ออกอาคาร

3.1.5.5 การซ้อมรับสถานการณ์ฉุกเฉิน

3.2 การกำกับดูแลการปฏิบัติตามด้านเทคนิค

3.2.1 ผู้บริหารต้องกำกับดูแลเพื่อให้มั่นใจว่าเจ้าหน้าที่ทราบถึงความรับผิดชอบด้านการรักษาความปลอดภัยสารสนเทศและได้มีการปฏิบัติในทางที่เหมาะสม ซึ่งอาจรวมถึงการจัดให้มีมาตรการในการวัดผลการปฏิบัติงานของเจ้าหน้าที่จากการปฏิบัติตามมาตรฐานความปลอดภัยของสารสนเทศ

3.2.2 แผนกด้านตรวจสอบภายในหรือคณะทำงานสอบทานต้องตรวจสอบการควบคุมทางด้านเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอและเหมาะสมหรือไม่ รวมทั้งการปฏิบัติตามการควบคุมเหล่านั้น

3.2.3 ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบระดับมาตรฐานความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การทดสอบการเจาะระบบ เป็นต้น เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านความปลอดภัย

3.2.4 เครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ ระบบงาน และเอกสารที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้องจากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

หมวดที่ 4 การสร้างความตระหนักด้านความปลอดภัยสารสนเทศ

ส่วนที่ 20
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(Information Security Awareness Policy)

1. วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. กองบริหารทรัพยากรบุคคล
3. สำนักงานเลขานุการกรม
4. หน่วยงานที่ได้รับมอบหมายในการจัดฝึกอบรม
5. ผู้ดูแลระบบที่ได้รับมอบหมาย
6. เจ้าหน้าที่ที่ได้รับมอบหมาย

3. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.1 จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

3.2 จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

3.3 ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ โดยการติดประกาศ ประชาสัมพันธ์แผ่นพับ เผยแพร่ผ่านเว็บไซต์

3.4 สนับสนุนให้มีส่วนร่วมและนำสู่การปฏิบัติ ตลอดจนติดตามประเมินผลและสำรวจความต้องการของผู้ใช้บริการ

ส่วนที่ 21
นโยบายด้านการปฏิบัติตามข้อบังคับ
(Compliance Policy)

1. วัตถุประสงค์

การปฏิบัติตามข้อบังคับด้านกฎหมาย เพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมายที่เกี่ยวข้องกับการดำเนินงานขององค์กร การที่องค์กรทราบถึงข้อกำหนดต่าง ๆ ที่เกี่ยวข้องจะสามารถทำให้องค์กรตระหนักถึงความเสี่ยงที่เกิดขึ้น รวมทั้งวางมาตรการควบคุมที่เหมาะสมได้ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการละเมิดดังกล่าว

2. ผู้รับผิดชอบ

1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2. กองกฎหมาย
3. ผู้ดูแลระบบที่ได้รับมอบหมาย
4. เจ้าหน้าที่ที่ได้รับมอบหมาย
5. ผู้ใช้งาน

3. แนวปฏิบัติในการปฏิบัติตามข้อบังคับ

3.1 การปฏิบัติตามข้อบังคับด้านกฎหมาย

บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย ถือเป็นสิ่งสำคัญที่ผู้ใช้งานคอมพิวเตอร์จะต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานคอมพิวเตอร์กระทำผิดตามกฎหมายดังกล่าว องค์กรถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล

3.2 การปกป้องข้อมูลส่วนบุคคล

3.2.1 ข้อมูลรายละเอียดที่เกี่ยวกับการดำเนินงานขององค์กร ถือว่าเป็นข้อมูลที่มีความสำคัญ เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บริหารเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวได้

3.2.2 ข้อมูลส่วนตัวของเจ้าหน้าที่ถือว่าเป็นข้อมูลลับ และสามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ เช่น เจ้าหน้าที่เองหรือผู้ทำงานที่มีความเกี่ยวข้องเท่านั้น อย่างไรก็ดีองค์กรสงวนสิทธิ์ในการเข้าถึงข้อมูลทั้งหมดที่สร้างและเก็บอยู่ในระบบสารสนเทศขององค์กร

3.3 ลิขสิทธิ์ซอฟต์แวร์

3.3.1 ห้ามมิให้เจ้าหน้าที่นำซอฟต์แวร์ภายนอกมาใช้ในระบบประมวลผลขององค์กร โดยมิได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในหน่วยงาน โดยผู้บังคับบัญชาฯ ต้องสอบทานกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ในเรื่องลิขสิทธิ์ขององค์กรและความเสี่ยงด้านความปลอดภัยสารสนเทศในการนำซอฟต์แวร์ดังกล่าวมาใช้ตามลำดับ

3.3.2 เจ้าหน้าที่ต้องไม่ทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่องค์กรได้จัดซื้อลิขสิทธิ์เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

3.3.3 ซอฟต์แวร์ที่พัฒนาภายในองค์กร ทั้งโดยบุคคลอื่นหรือเจ้าหน้าที่ขององค์กรถือว่าเป็นทรัพย์สินขององค์กร องค์กรไม่อนุญาตให้เจ้าหน้าที่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินขององค์กร โดยไม่ได้รับการอนุญาตจากผู้บริหารเป็นลายลักษณ์อักษร

3.3.4 ผู้ที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศขององค์กรทั้งหมด ต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

3.3.5 ซอฟต์แวร์ที่ได้จัดซื้อจากภายนอกอาจมีเงื่อนไขในเรื่องลิขสิทธิ์ด้านการใช้งานที่แตกต่างกัน หน่วยงานที่รับผิดชอบด้านการจัดซื้อต้องรับผิดชอบในการศึกษาถึงเงื่อนไขดังกล่าว ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องสร้างความตระหนักถึงผู้ใช้งานซอฟต์แวร์ดังกล่าวได้ทราบถึงเงื่อนไขต่าง ๆ และข้อห้ามที่เกี่ยวข้อง

3.3.6 การจัดซื้อหรือใช้ซอฟต์แวร์ของบุคคลอื่นต้องปฏิบัติให้สอดคล้องกับข้อตกลงด้านลิขสิทธิ์ ห้ามนำซอฟต์แวร์ที่ซื้อไปติดตั้งที่คอมพิวเตอร์เครื่องอื่นนอกเหนือจากเครื่องที่ได้มีการติดตั้งแล้วตามข้อตกลงเรื่องลิขสิทธิ์ซอฟต์แวร์

3.3.7 ทำการตรวจสอบการใช้งานคอมพิวเตอร์ขององค์กรอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการใช้งานอุปกรณ์คอมพิวเตอร์ทุกชนิดเป็นไปตามข้อตกลงด้านลิขสิทธิ์ซอฟต์แวร์

3.3.8 เจ้าหน้าที่ที่ฝ่าฝืนละเมิดข้อตกลงด้านลิขสิทธิ์ของเจ้าของซอฟต์แวร์ถือว่าเป็นการละเมิดนโยบายความปลอดภัยสารสนเทศขององค์กร ถึงแม้การละเมิดนั้นจะเป็นไปเพื่อการปฏิบัติงานขององค์กรก็ตาม เจ้าหน้าที่ต้องรับผิดชอบผลเสียหายทั้งหมด

4. แนวปฏิบัติในการบังคับใช้สำหรับการฝ่าฝืนและบทลงโทษ

4.1 กรณีที่องค์กรตรวจสอบแล้วพบว่าบัญชีผู้ใช้งานระบบเครือข่ายใดมีพฤติกรรมสุ่มเสี่ยง ฝ่าฝืนนโยบาย หรือประพฤติโดยมิชอบ เช่น โหลดบิต การสร้างโปรเซสที่กินกำลังระบบ การขโมยข้อมูล การเจาะระบบการเข้าถึงระบบโดยปราศจากความยินยอมหรือการอนุญาตของผู้ดูแลระบบ เป็นต้น องค์กรขอสงวนสิทธิ์ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งานอินเทอร์เน็ต และ/หรือหยุดให้บริการแก่ผู้ใช้งานนั้นดังนี้

4.1.1 ละเมิดกฎครั้งแรก	ทำหนังสือตักเตือน
4.1.2 ละเมิดกฎครั้งที่ 2 ซ้ำโดยเจตนา	ทำหนังสือตักเตือน ระงับ User ชั่วคราว 1 เดือน
4.1.3 ละเมิดกฎครั้งที่ 3 ซ้ำโดยเจตนา	ทำหนังสือตักเตือน ระงับ User ชั่วคราว 2 เดือน
4.1.4 ละเมิดกฎซ้ำมากกว่า 3 ครั้งโดยเจตนา	ทำหนังสือตักเตือน ยกเลิก User ถาวร

4.2 องค์กรขอสงวนสิทธิ์ในการจัดสรรแบนด์วิดท์ (Bandwidth Quota) ของผู้ใช้งานแต่ละคนเพื่อการจัดการทรัพยากรแบนด์วิดท์ที่เหมาะสม

4.3 หากการกระทำอันฝ่าฝืนต่อนโยบายนี้เป็นความผิดตามกฎหมาย ให้องค์กรดำเนินคดีตามกฎหมายโดยลำดับต่อไปและองค์กรไม่รับผิดชอบต่อผลของการกระทำที่เกิดจากผู้ใช้งานและ/หรือบัญชีผู้ใช้งานที่ฝ่าฝืนต่อนโยบายนี้

ด่วนที่สุด บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร คปท. โทร. ๐ ๒๙๔๐ ๕๖๐๒ ต่อ ๔๐๔๐ - ๔๑

ที่ กษ ๐๕๒๓.๔/ ๖๘๒ **วันที่** ๑๘ สิงหาคม ๒๕๖๕

เรื่อง ลงนามประกาศกรมประมง เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕

เรียน อธิบดีกรมประมง

ตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้ดำเนินการทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี ๒๕๖๕ และได้จัดส่งแนวนโยบายและแนวปฏิบัติฯ พร้อมประกาศกรมประมงและแบบประเมินประกอบการพิจารณาการดำเนินงานตามนโยบายและแนวปฏิบัติฯ เพื่อขอความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตามความในมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ เมื่อวันที่ ๒๒ มิถุนายน ๒๕๖๕ รายละเอียดตามเอกสารแนบ ๑ นั้น

ในการนี้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ให้ความเห็นชอบต่อแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวน) ของกรมประมง เมื่อวันที่ ๑๗ สิงหาคม ๒๕๖๕ เป็นที่เรียบร้อยแล้ว และได้นำขึ้นประกาศในเว็บไซต์ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ปรากฏอยู่ในรายชื่อหน่วยงานผ่านความเห็นชอบการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ลำดับที่ ๖๓ รายละเอียดตามเอกสารแนบ ๒

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบโปรดลงนามในประกาศกรมประมง เพื่อกรมประมงจะได้ประกาศใช้แนวนโยบายและแนวปฏิบัติฯ ให้แก่เจ้าหน้าที่กรมประมงและผู้ที่เกี่ยวข้องทราบและนำไปปฏิบัติอย่างเคร่งครัดต่อไป

(นางสุนทรี แสงแสน)
หัวหน้าฝ่ายสารบรรณ
ปฏิบัติราชการแทนเลขานุการกรม
๑๙ ส.ค. ๒๕๖๕

(นายพลพิศิลป์ สุวรรณชัย)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ลงนามแล้ว

(นายเฉลิมชัย สุวรรณรักษ์)
อธิบดีกรมประมง

(นายถาวร ทันใจ)
รองอธิบดีกรมประมง

รายชื่อหน่วยงานผ่านความเห็นชอบการจัดทำนโยบายและแนวปฏิบัติฯ
(ปรับปรุง ณ วันที่ ๑๗ ส.ค. ๒๕๖๕)

เรียน ศกส
สุรัช
๒๓ สค ๖๕