ประกาศกรมการกงสุล
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓

เพื่อให้การดำเนินการด้านสารสนเทศ เป็นไปอย่างเหมาะสมมีมาตรฐานสอดคล้องกับระเบียบกฎหมายอาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีความมั่นคงปลอดภัยและเชื่อถือได้ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กรมการกงสุลจึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมการกงสุล เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓”

ข้อ ๒ ประกาศนี้ให้มีผลใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ดังต่อไปนี้

(๑) เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมการกงสุลจัดทำขึ้นเพื่อกำหนดวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้

(๓) เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ โดยอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

(๔) เพื่อกำหนดแนวทางและวิธีปฏิบัติสำหรับเจ้าหน้าที่หรือบุคคลที่ปฏิบัติงานให้กับกรมการกงสุลในการยืนยันตัวตน การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ

(๕) เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติ และให้สามารถกู้คืนข้อมูลได้ภายในระยะเวลาที่เหมาะสม

(๖) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอ

(๗) เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ และสร้างความเข้าใจเกี่ยวกับการเก็บข้อมูล การรักษาข้อมูล ระบบความมั่นคงปลอดภัยของระบบสารสนเทศให้แก่เจ้าหน้าที่และบุคคลที่ปฏิบัติงานให้กับกรมการกงสุล

(๘) เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมการกงสุล ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

ข้อ ๔ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการกงสุล ตามเอกสารแนบท้ายประกาศนี้ มี ๒ ส่วน ดังต่อไปนี้

(๑) การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๑.๑) จัดทำนโยบายและแนวปฏิบัติเป็นลายลักษณ์อักษร และประกาศให้ผู้ใช้งานได้ทราบ

(๑.๒) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติให้ชัดเจน

(๑.๓) มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติอย่างน้อยปีละ ๑ ครั้ง

(๒) รายละเอียดของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒.๑) การเข้าถึงและควบคุมการใช้งานสารสนเทศ

(๒.๒) การบริหารจัดการการเข้าถึงระบบของผู้ใช้งาน

(๒.๓) การกำหนดความรับผิดชอบของผู้ใช้งาน

(๒.๔) การควบคุมการเข้าถึงเครือข่าย

(๒.๕) การควบคุมการเข้าถึงระบบปฏิบัติการ

(๒.๖) การเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์

(๒.๗) การสำรองข้อมูลและระบบสารสนเทศ

(๒.๘) การตรวจสอบและการประเมินความเสี่ยงด้านสารสนเทศ

ข้อ ๕ ให้มีประกาศเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ผ่านช่องทางเว็บไซต์กรมการกงสุล เพื่อให้เจ้าหน้าที่ผู้เกี่ยวข้องและประชาชนทั่วไปทราบ พร้อมกำหนดให้ผู้รับผิดชอบตามนโยบายและแนวปฏิบัติต่าง ๆ ได้รับทราบเพื่อถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

ข้อ ๖ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

ข้อ ๗ กำหนดหน้าที่ผู้รับผิดชอบ

ระดับนโยบาย

(๑) กรณีข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดของกรมการกงสุลเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

(๒) ให้รองอธิบดีกรมการกงสุล ที่ได้รับมอบหมายในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ติดตาม กำกับ ควบคุม ดูแล ตรวจสอบ รวมทั้งให้ข้อเสนอแนะและให้คำปรึกษาแก่ผู้ใช้งานระบบสารสนเทศ

ระดับปฏิบัติ

(๓) ให้เจ้าหน้าที่กรมหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา มีหน้าที่รับผิดชอบในการวางแผน ติดตามการบริหารความเสี่ยง การควบคุม ดูแล รักษาความปลอดภัย บริหารจัดการ บำรุงรักษาระบบฐานข้อมูล ระบบสารสนเทศ ตรวจสอบการกำหนดสิทธิในการใช้งานระบบฐานข้อมูล ระบบสารสนเทศ วิเคราะห์ ออกแบบ พัฒนา ปรับปรุง ควบคุมและบำรุงรักษาระบบสารสนเทศที่สนับสนุนการตรวจลงตราและการปฏิบัติของเจ้าหน้าที่กรม ประเมินความเสี่ยง การควบคุมภายใน การรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ การจัดทำความตกลงและกำหนดมาตรฐานการเชื่อมโยงข้อมูลกับหน่วยงานภายนอก การดำเนินงานแผนการฝึกอบรมบุคลากรของกรมหรือสำนักงานในต่างประเทศ และเป็นผู้รับผิดชอบในการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๓๐ ธันวาคม พ.ศ. ๒๕๖๓

(นายชาตรี อรรจนานันท์)
อธิบดีกรมการกงสุล

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมการกงสุล

พ.ศ. ๒๕๖๓

คำนำ

ปัจจุบันกรมการกงสุลได้นำระบบสารสนเทศเข้ามาช่วยในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว มีประสิทธิภาพ และช่วยอำนวยความสะดวกในการดำเนินงานด้านต่าง ๆ ของหน่วยงาน เพื่อป้องกันความเสี่ยงที่อาจก่อให้เกิดภัยอันตรายต่อการปฏิบัติราชการ ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ และสร้างความเสียหายด้านระบบสารสนเทศของหน่วยงาน ดังนั้น ผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศ จึงมีความจำเป็นจะต้องตระหนักถึงการดูแล บำรุงรักษาและการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เกิดความปลอดภัยสูงสุด

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ของกรมการกงสุล ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

กรมการกงสุลจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

****

สารบัญ

****

ส่วนที่ ๑ คำนิยาม

(๑) **นโยบาย** หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(๒) **สำนักงานในต่างประเทศ** หมายความว่า สถานเอกอัครราชทูต สถานกงสุลใหญ่ สำนักงานการค้าและเศรษฐกิจไทย หรือองค์กร หน่วยงาน เอกชน ที่ได้รับมอบหมาย

(๓) **กรม** หมายความว่า กรมการกงสุล

(๔) **ผู้บังคับบัญชา** หมายความว่า อธิบดี รองอธิบดี หรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรม

(๕) **ผู้ใช้งาน** หมายความว่า

(๕.๑) **เจ้าหน้าที่กงสุล** หมายความว่า เจ้าหน้าที่กงสุลที่ประจำอยู่ที่กรมการกงสุล กระทรวงการต่างประเทศ และเจ้าหน้าที่กงสุลที่ปฏิบัติหน้าที่ด้านกงสุลในต่างประเทศ ซึ่งจะมีทั้งระดับผู้บังคับบัญชาเป็นผู้กำหนดผู้เข้าใช้งานและสร้าง User Staff เข้าใช้งานระบบ E-Back Office และมีระดับผู้ปฏิบัติงานผู้บังคับบัญชา หัวหน้าศูนย์ข้อมูลการตรวจลงตรา หรือผู้ได้รับมอบหมายจากผู้บังคับบัญชา ในการอนุมัติสิทธิต่าง ๆ ที่เกี่ยวข้องกับระบบงานใน Visa Data Center

(๕.๒) **ผู้ดูแลระบบ** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลระบบงานต่าง ๆ ที่มีความสำคัญใน Visa Data Center

(๕.๓) **ผู้ควบคุมดูแลห้อง** หมายความว่า เจ้าหน้าที่ที่ปฏิบัติงานอยู่ที่ Visa Data Center จะเกี่ยวข้องกับส่วนงาน Visa Data Center Operation

(๕.๔) **ผู้สนับสนุนและให้บริการ** หมายความว่า หน่วยงาน องค์กร เอกชน ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรมและงานบริการที่เกี่ยวข้อง

(๕.๕) **ผู้ใช้บริการ** หมายความว่า ผู้ที่มารับบริการจากกรมหรือสถานเอกอัครราชทูต สถานกงสุลใหญ่และสำนักงานการค้าและเศรษฐกิจไทย (สำนักงานในต่างประเทศ) ผ่านช่องทางการสื่อสารทางอิเล็กทรอนิกส์

(๖) **ผู้ใช้งานภายนอก** หมายความว่า บุคคลภายนอกซึ่งได้รับอนุญาตให้เข้าใช้งานระบบสารสนเทศของกรม

(๗) **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของกรม

(๘) **สินทรัพย์** หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่จับต้องได้และจับต้องไม่ได้อันมีมูลค่าหรือคุณค่าของกรม

(๙) **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การเข้าถึงสารสนเทศ ระบบสารสนเทศ ห้องเครื่องแม่ข่าย ระบบเครือข่าย อุปกรณ์เทคโนโลยีสารสนเทศ โดยสารสนเทศหมายรวมถึงสารสนเทศที่อยู่ในรูปแบบของอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์ และครอบคลุมถึงวิธีปฏิบัติการใช้งานสารสนเทศเกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามขอบเขตที่กำหนดไว้

(๑๐) **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

(๑๑) **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายความว่า กรณีที่เกิดเหตุการณ์บุกรุกสภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๒) **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของกรมถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๑๓) **ระบบป้องกันมัลแวร์** หมายความว่า โปรแกรมหรือแอปพลิเคชันที่สามารถป้องกันเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ จากโปรแกรมไม่ประสงค์ดีภายนอก

(๑๔) **ระบบปฏิบัติการ (Operating System)** หมายความว่า ซอฟต์แวร์ที่เอาไว้ใช้สำหรับควบคุมและประสานงานระหว่างอุปกรณ์ภายในคอมพิวเตอร์ทั้งหมด ตั้งแต่ซีพียู หน่วยความจำ ไปจนถึงส่วนนำเข้าและส่งออกผลลัพธ์ (input/output device) คอมพิวเตอร์จะทำงานได้จำเป็นต้องมีระบบปฏิบัติการติดตั้งอยู่ในเครื่องเสียก่อน

(๑๕) **อุปกรณ์จัดเส้นทาง** (Router) หมายความว่า อุปกรณ์ที่ใช้งานในการเชื่อมโยงเครือข่ายหลายเครือข่ายเข้าด้วยกัน หรือ เชื่อมโยงอุปกรณ์หลายอย่างเข้าด้วยกัน ดังนั้นจึงมีเส้นทางการเข้าออกของข้อมูลได้หลายเส้นทาง อุปกรณ์จัดเส้นทางจะหาเส้นทางที่เหมาะสมให้ เพื่อนำส่งข้อมูลผ่านเครือข่ายต่าง ๆ ไปยังอุปกรณ์ปลายทางตามที่ระบุไว้

(๑๖) **อุปกรณ์กระจายสัญญาณข้อมูล** (Switch) หมายความว่า อุปกรณ์ในระบบ computer network เช่นเดียวกับ Hub ทำหน้าที่เชื่อมต่ออุปกรณ์อื่น ๆ เข้าด้วยกันในระบบ โดยอาศัยการทำ packet switching ซึ่งจะรับประมวลผล และส่งข้อมูลต่อไปยังปลายทาง เพียงแค่หนึ่งหรือหลายพอร์ต

(๑๗) **VPN (Virtual Private Network)** หมายความว่า ฟังก์ชันหนึ่งในระบบเน็ตเวิร์ค สร้างขึ้นมาทำให้สามารถรับส่งข้อมูลได้ปลอดภัยมากขึ้น จะทำงานโดยใช้โครงสร้างของอินเทอร์เน็ต เป็นตัวส่งผ่านข้อมูล มีการเข้ารหัสข้อมูลทั้งหมดและจะมี Gateway เฉพาะในการส่งข้อมูลด้วย มีการ Login ผู้ใช้ รหัสผ่าน (Password) สำหรับบุคคลที่ได้รับอนุญาต

(๑๘) **Visa Data Center (VDC)** หมายความว่า ศูนย์ข้อมูลการตรวจลงตรา กรมการกงสุล

(๑๙) **Privileged Access Management (PAM)** หมายความว่า โปรแกรมสำหรับจัดการ และเป็นตัวกลางสำหรับการรีโมตไปยัง Server ต่าง ๆ รวมถึงการกำหนดสิทธิต่าง ๆ จัดการเพื่อให้สิทธิในการรีโมต

(๒๐) **Active Directory** หมายความว่า เครื่องมือที่มีมากับ Windows Server Operating System จัดการทรัพยากรในระบบ ด้วยเครื่องมือของ Server Domain Controller ถ้าองค์กรที่มี User จำนวนมาก ๆ สามารถนำ Active Directory มาใช้

(๒๑) **ช่องโหว่ทางเทคนิค** หมายความว่า ความอ่อนแอของระบบสารสนเทศหรือระบบเครือข่ายที่เปิดโอกาสให้สิ่งที่เป็นภัยคุกคามสามารถเข้าถึงสารสนทศในระบบได้ ซึ่งจะนำไปสู่ความเสียหายแก่สารสนเทศ หรือแม้แต่การทำงานของระบบ

****

ส่วนที่ ๒ ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

๒.๑ วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศและการสื่อสารของกรมและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก ที่จะสร้างความเสียหายแก่ข้อมูล ต้องตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของกรมได้อย่างถูกต้องเพื่อให้การดำเนินการตามข้อปฏิบัติการดูแลระบบสารสนเทศอย่างปลอดภัยนอกจากเป็นการสร้างความน่าเชื่อถือมั่นคงและปลอดภัย

๒.๒ แนวปฏิบัติ

(๑) กรมกำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่ผู้ใช้งานที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของกรมต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บังคับบัญชากรมหรือผู้ที่ได้รับมอบหมายให้มีอำนาจในการอนุญาต

(๒) ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับหน้าที่ความรับผิดชอบของเจ้าหน้าที่ผู้ใช้งานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบต้องติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

(๔) ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

(๕) บุคคลภายนอกที่ต้องการสิทธิเข้าใช้งานระบบสารสนเทศและการสื่อสารของกรมต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากกรม ในการอนุมัติ

(๖) หน่วยงานที่ทำงานให้กับกรมทุกหน่วยงานที่ต้องการเชื่อมต่อจากภายนอก ต้องแจ้งต่อกรม เป็นลายลักษณ์อักษรเพื่อขออนุมัติก่อนดำเนินการเชื่อมต่อ

(๗) กำหนดมาตรฐานในการเข้าใช้ข้อมูล หรือการเชื่อมโยงข้อมูลของหน่วยงานภาครัฐและภาคเอกชนที่ต้องการข้อมูลจากกรม

(๘) การควบคุมการเข้าถึงระบบสารสนเทศหลักของกรม

(๘.๑) การบริหารจัดการรหัสผู้ใช้งาน (User ID) และรหัสผ่าน (Password)

(ก) ผู้ใช้งานระบบสารสนเทศหลักของกรมต้องแจ้งให้กรมทราบเป็นหนังสือเพื่อดำเนินการกำหนดรหัสผู้ใช้และรหัสผ่าน

(ข) ช่องใส่รหัสผ่านต้องป้องกันไม่ให้แสดงข้อมูลรหัสผ่านที่ผู้ใช้งานพิมพ์ลงไป หรือทำให้ไม่เห็นข้อมูลรหัสผ่านที่แท้จริงได้

(ค) กรณีเจ้าหน้าที่ผู้ใช้งานระบบเปลี่ยนชื่อ นามสกุล ตำแหน่ง หรือ MAC Address ให้แจ้งกรมทราบเป็นหนังสือ เพื่อทำการปรับปรุงข้อมูลประวัติบุคคลของผู้ใช้งานระบบให้เป็นปัจจุบัน

(ง) กรณีกรมมีคำสั่งเลื่อนระดับหรือโยกย้ายเจ้าหน้าที่ผู้ใช้งานระบบไปปฏิบัติหน้าที่ในหน่วยงานอื่น กรมจะทำการปรับเปลี่ยนข้อมูลหน่วยงานของผู้ใช้งานระบบเพื่อให้ สามารถใช้งานระบบสารสนเทศที่หน่วยงานใหม่ได้ทันทีที่คำสั่งมีผลใช้บังคับ

(จ) กรมจะทำการยกเลิกรหัสผู้ใช้ รหัสผ่านและสิทธิในการเข้าถึงระบบฯ ของเจ้าหน้าที่ผู้ใช้งานระบบทันทีที่ทราบคำสั่งกรมให้เจ้าหน้าที่พ้นจากการปฏิบัติหน้าที่ เกษียณอายุ โอนย้ายไปหน่วยงานภาครัฐอื่น

(ฉ) ผู้ดูแลระบบ (Administrator) โยกย้ายไปปฏิบัติหน้าที่ที่หน่วยงานอื่น หน่วยงานต้องแจ้งรายชื่อเจ้าหน้าที่ที่ทำหน้าที่เป็นผู้ดูแลระบบใหม่ พร้อมแจ้งยกเลิกผู้ดูแลระบบสารสนเทศเดิม เพื่อให้กรมยกเลิกสิทธิในการกำหนดสิทธิการเข้าถึงระบบสารสนเทศให้กับผู้ใช้งานระบบ

(๘.๒) การใช้งานรหัสผู้ใช้งาน (User ID) และรหัสผ่าน (Password)

(ก) ผู้ใช้งานระบบต้องทำการเปลี่ยน/กำหนดรหัสผ่านของตนเองใหม่ทันทีหลังจากได้รับรหัสผ่านจากกรมที่กำหนดรหัสผู้ใช้และรหัสผ่านเป็นรหัสเดียวกันในครั้งแรก

(ข) ผู้ใช้งานระบบต้องทำการเปลี่ยน/กำหนดรหัสผ่านของตนเองใหม่ทุก ๓ เดือน

(ค) รหัสผ่านประกอบด้วยตัวอักษร อย่างน้อย ๘ หลัก ประกอบด้วย

- ตัวอักษรเล็กไม่น้อยกว่า ๑ ตัว ตัวอักษรใหญ่ไม่น้อยกว่า ๑ ตัว
- อักขระพิเศษ

(ง) รหัสผ่านเป็นช่องว่างไม่ได้

(จ) กำหนดรหัสผ่านซ้ำกับที่เคยกำหนดมาแล้ว ๓ ครั้งล่าสุดไม่ได้

(ฉ) ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่านของตนเอง

(ช) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๘.๓) การอนุญาตให้เข้าถึงระบบสารสนเทศหลัก

ผู้ดูแลระบบสารสนเทศของหน่วยงานมีหน้าที่กำหนดสิทธิการเข้าใช้งานระบบสารสนเทศให้กับเจ้าหน้าที่ผู้ใช้งานระบบของ หน่วยงาน โดยต้องกำหนดสิทธิในการเข้าถึงให้ตรงตามหน้าที่ ความรับผิดชอบของผู้ใช้งานระบบที่ได้รับมอบหมายจากผู้บังคับบัญชา สำหรับหน่วยงานที่ไม่มีผู้ดูแลระบบ กรณีต้องการเข้าใช้งานระบบสารสนเทศต้องแจ้งให้กรมทราบเป็นหนังสือ

(๘.๔) ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

(ก) ประเภทของข้อมูล แบ่งออกเป็น

- ข้อมูลสารสนเทศด้านการให้บริการ (ข้อมูลสถิติ)
- ข้อมูลสารสนเทศด้านการบริหารจัดการ

(a) ข้อมูลการดำเนินงานตามภารกิจของกรม

(b) ข้อมูลติดตามการดำเนินงานตามภารกิจของกรม

(c) ข้อมูลการติดต่อหน่วยงานภายใน

(d) ข้อมูลรายงานผลการปฏิบัติงาน

(e) ข้อมูลการติดต่อหน่วยงานภายนอก

(ข) การจัดแบ่งลำดับชั้นการเข้าถึงข้อมูล ได้แก่

- ระดับชั้นสำหรับผู้บังคับบัญชา คือ ระดับชั้นการเข้าถึงที่อนุญาตให้ผู้บริหาร หรือผู้ที่ได้รับมอบหมายเข้าถึงข้อมูลสารสนเทศ ด้านการบริหาร ด้านการจัดการและปฏิบัติงาน และด้านการ ให้บริการ โดยจะได้รับสิทธิตามความจำเป็นต่อการปฏิบัติหน้าที่ของผู้เข้าถึงในระดับนี้เท่านั้น

- ระดับชั้นสำหรับผู้ใช้งาน คือระดับชั้นการเข้าถึงที่อนุญาตให้เจ้าหน้าที่ที่ได้รับมอบหมายเข้าถึงข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงานและด้านการให้บริการ โดยจะได้รับสิทธิตามความจำเป็นต่อการปฏิบัติหน้าที่ของผู้เข้าถึงในระดับนี้เท่านั้น

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย คือ ระดับชั้นการเข้าถึงที่อนุญาตให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเข้าถึงข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน โดยจะได้รับสิทธิตามความจำเป็นต่อการดูและระบบหรือปฏิบัติหน้าที่ของผู้เข้าถึงในระดับนี้เท่านั้น

(ค) ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล กำหนดชั้นความลับของข้อมูลเป็น ๕ ระดับ ได้แก่

- ลับที่สุด ได้แก่ ข้อมูลที่มีความสำคัญที่สุดเกี่ยวกับข่าวสารวัตถุ หรือบุคคล ซึ่งถ้าหากข้อมูลดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหลไปถึงบุคคลผู้ไม่มีหน้าที่ได้รับทราบจะทำให้เกิดความเสียหายหรือเป็นภยันตรายต่อความมั่นคงปลอดภัย ของสาธารณชน หรือความสงบเรียบร้อยของประเทศชาติ หรือต่อธุรกิจหรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องอย่างร้ายแรงที่สุด

- ลับมาก ได้แก่ ข้อมูลที่มีความสำคัญมากเกี่ยวกับข่าวสารวัตถุหรือบุคคล ซึ่งถ้าหากข้อมูลดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหลไปถึงบุคคลที่ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายหรือเป็นภยันตรายต่อความมั่นคงปลอดภัยของสาธารณชน หรือความสงบเรียบร้อยของประเทศชาติ หรือต่อธุรกิจหรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องอย่างร้ายแรง

- ลับ ได้แก่ข้อมูลที่มีความสำคัญเกี่ยวกับข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากข้อมูลดังกล่าวทั้งหมด หรือเพียงบางส่วน รั่วไหลไปถึงบุคคลผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายต่อธุรกิจหรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้อง

- ปกปิด ได้แก่ ข้อมูลซึ่งไม่พึงเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบโดยสงวนไว้ให้ทราบเฉพาะบุคคลที่มีหน้าที่ต้องทราบเพื่อประโยชน์ในการปฏิบัติภารกิจขององค์กรหรือหน่วยงานที่เกี่ยวข้องเท่านั้น

- เปิดเผยได้ ได้แก่ ข้อมูลโดยทั่วไปที่สามารถเปิดเผยได้ เพื่อประโยชน์ในการปฏิบัติภารกิจขององค์กรหรือหน่วยงานที่เกี่ยวข้องเท่านั้น

(ง) เวลาการเข้าถึง

- การเข้าถึงสารสนเทศในเวลาราชการ (๐๘.๓๐-๑๖.๓๐ น.)

- การเข้าถึงสารสนเทศนอกเวลาราชการ (๑๖.๓๐ - ๐๘.๓๐ น.)

- การเข้าถึงสารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และ วันหยุดนักขัตฤกษ์)

(จ) ช่องทางการเข้าถึง

- ระบบอินเทอร์เน็ต (ทุกช่วงเวลา)
- ระบบอินทราเน็ต (ทุกช่วงเวลา)
- ระบบจดหมายอิเล็กทรอนิกส์ (ทุกช่วงเวลา)
- เว็บไซต์ (ทุกช่วงเวลาหรือในช่วงเวลาที่กำหนด)
- ระบบเครือข่าย LAN (ในและนอกเวลาราชการ)
- ระบบเครือข่ายไร้สาย (Wireless LAN) (ในช่วงเวลาที่กำหนด)
- การประชุมทางไกล (Video Conference) (ในเวลาราชการและในช่วงเวลาพิเศษเป็นรายครั้ง)
- โทรศัพท์หรือโทรสาร (ในเวลาราชการ)
- ติดต่อด้วยตัวเอง (ในเวลาราชการ)
- หนังสือหรือบันทึกข้อความ (ในเวลาราชการ)

(๙) ขั้นตอนการปฏิบัติการตรวจสอบระบบสารสนเทศ (IT Monitoring)

การตรวจสอบ Server และไฟสถานะอุปกรณ์สารสนเทศ ผู้ดูแลระบบจะต้องตรวจสอบ Server ประจำวัน สัปดาห์ และเดือนตามเอกสารแบบฟอร์มตรวจสอบการทำงานระบบห้อง Visa Data Center และเครื่องแม่ข่ายที่ได้รับมอบหมายจากหัวหน้าศูนย์ข้อมูลการตรวจลงตราสม่ำเสมอ

(๑๐) การบริหารจัดการการเข้าถึงระบบสารสนเทศ

(ก) การบริหารจัดการการเข้าถึงของผู้ใช้งาน

การลงทะเบียนเจ้าหน้าที่ใหม่

- จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบสารสนเทศขององค์กร
- ผู้ดูแลระบบต้องตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิหรืออนุมัติจากเจ้าของระบบอย่างถูกต้อง
- ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
- ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนหรือเพิ่มเติมสิทธิการเข้าถึงระบบสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน
- การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต การลงทะเบียนผู้ใช้งานระบบสารสนเทศ
- ยื่นคำขอกับผู้บังคับบัญชาหรือเจ้าหน้าที่ที่ได้รับมอบหมาย

(ข) กำหนดสิทธิการใช้ระบบสารสนเทศที่สำคัญโดยต้อง ให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอทุก ๆ ๓ เดือน

(ค) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

- สิทธิการเข้าถึงข้อมูลของผู้ใช้งานต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด และทุกครั้งที่มีการปรับเปลี่ยนการย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบหรือการยกเลิก การจ้างแล้วแต่กรณี

- ต้องทำการทบทวนสิทธิการเข้าถึงของผู้ใช้งานทุก ๆ ๓ เดือน สิทธิในระดับผู้ดูแลระบบต้องทบทวนสิทธิสำหรับผู้มีสิทธิในระดับสูงอย่างน้อยทุก ๆ ๓ เดือน

(ง) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

- ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศที่ใช้งานโดยทันทีเมื่อเสร็จสิ้นงาน ผู้ใช้งานต้องล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

- ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อกหน้าจอเมื่อไม่ใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

- ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(จ) ระบบเครือข่ายทั้งหมดของกรมที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกกรมต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

(ฉ) การเข้าสู่ระบบงานเครือข่ายของผู้ใช้งานภายในกรมผ่านทางอินเทอร์เน็ตต้อง Login และพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องก่อนทุกครั้ง

(ช) ต้องทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๑๑) การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

(ก) ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ต้องกำหนดรับผิดชอบในการดูแลและในกรณีที่ต้องทำการแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของระบบ (System configuration)

(ข) การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย (Server) ต้องควบคุมดูแลและได้รับอนุญาตโดยผู้ดูแลระบบเท่านั้น

(๑๒) การควบคุมการเข้าใช้งานระบบจากภายนอก

การเข้าสู่ระบบจากระยะไกล (Remote access) การควบคุมบุคคลที่เข้าสู่ระบบของกรมจากระยะไกลต้องกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน โดยต้องกระทำผ่าน VPN เท่านั้น

(๑๓) การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก

ผู้ใช้งานทุกคนเมื่อจะเข้าใช้งานระบบ ไม่ว่าจะเป็นการเข้าสู่ระบบสารสนเทศทางอินเทอร์เน็ต การเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร โดยต้องทำเรื่อง

ขออนุญาตเป็น ลายลักษณ์อักษรเพื่อขออนุมัติจากผู้มีบังคับบัญชาในการอนุมัติ และปฏิบัติตามวิธีการที่กรมกำหนด ดังนี้

(ก) การติดต่อเข้าใช้งานระบบต่าง ๆ ของกรมผ่านระบบอินเทอร์เน็ต (Internet) จากภายนอกต้องทำการเชื่อมต่อผ่าน VPN ของกรม และป้อน Username และ Password ก่อนใช้งานทุกครั้ง

(ข) กรอกข้อมูลผู้ใช้งานตามที่กำหนด และเมื่อปฏิบัติตามขั้นตอนต่าง ๆ และได้รับการอนุญาตจากระบบของกรม โดยระบุดังนี้ Username : ที่ผู้บังคับบัญชากำหนดน้อยจำนวน ๖ หลัก Password : อย่างน้อย ๘ หลัก ประกอบด้วย (a) ตัวอักษรเล็กไม่น้อยกว่า ๑ ตัว ตัวอักษรใหญ่ไม่น้อยกว่า ๑ ตัว และ (b) อักขระพิเศษ

****

ส่วนที่ ๓ ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

๓.๑ วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานสารสนเทศของกรมการกงสุล รวมทั้งสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานสารสนเทศขององค์กรได้อย่างถูกต้อง และเพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓.๒ แนวปฏิบัติ

ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ

๓.๒.๑ การควบคุมการเข้าถึงสารสนเทศ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ ให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต และรวมความถึงการกำหนดหน้าที่ของผู้ใช้งาน การเข้าถึงเครือข่าย การใช้งานระบบสารสนเทศ การเฝ้าดูการใช้งาน ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ นโยบายควบคุมการเข้าถึงต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๓.๒.๒ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย

(๑) มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(ก) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(ข) มีการปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

(๒) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

(๓) การบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการได้ลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิเท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศและต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิการใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

(๔) การเข้าถึงข้อมูลตามระดับชั้นความลับ ต้องมีการจัดลำดับชั้นความลับ มีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการจำหน่ายหรือการนำอุปกรณ์กลับมาใช้ใหม่

****

ส่วนที่ ๔ การบริหารจัดการการเข้าถึงระบบของผู้ใช้งาน

ขั้นตอนการปฏิบัติการลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration)

๔.๑ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมจะต้องสร้างความรู้ความเข้าใจให้กับผู้ใช้งานของกรมและผู้รับบริการระบบสารสนเทศ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงผลกระทบอันเกิดจากการใช้งานในระบบสารสนเทศโดยไม่ระมัดระวัง และส่งเสริมให้ความรู้ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้งาน เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับการอนุญาต และให้ถือปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓ อย่างเคร่งครัด ดังนี้

(๑) จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง

(๒) จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร อย่างน้อยปีละ ๑ ครั้ง

(๓) ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๔.๒ การลงทะเบียนสิทธิผู้ใช้งาน

(๑) ผู้ดูแลระบบ จะต้องได้รับการอนุญาตจากผู้บังคับบัญชา ตามความจำเป็นต่อการใช้งาน เพื่อลงทะเบียนสิทธิผู้ใช้งานใหม่เพื่อเข้าถึงสารสนเทศและระบบสารสนเทศ โดยกระบวนการลงทะเบียนสิทธิผู้ใช้งานจะต้องผ่านการอนุมัติตามกระบวนการ Change Process ก่อนเท่านั้น ซึ่งต้องมีการกำหนดขั้นตอนในการขออนุญาตเข้าถึงประกอบรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ใช้งาน (ภาษาอังกฤษ) รหัสพนักงาน เหตุผลในการขอใช้งาน ระยะเวลาในการใช้งาน และ MAC Address ของเครื่องคอมพิวเตอร์ที่จะใช้งาน ระบบงานที่เกี่ยวข้องมีดังนี้ Active Directory , PAM, VPN

(๒) ผู้ใช้งาน จะต้องได้รับการอนุญาตจาก ผู้บังคับบัญชาเจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้นเพื่อลงทะเบียนสิทธิผู้ใช้งานใหม่ เพื่อเข้าถึงสารสนเทศ และระบบสารสนเทศ โดยกระบวนการลงทะเบียนสิทธิผู้ใช้งานจะต้องส่งอีเมล์รายละเอียดขอลงทะเบียนสิทธิผู้ใช้งานใหม่มายังผู้ที่ดูแลระบบ และผู้ดูแลระบบจะขออนุมัติตามกระบวนการ Change Process ซึ่งต้องมีการกำหนดขั้นตอนในการขออนุญาตเข้าถึงประกอบรายละเอียดอย่างน้อยดังนี้ ชื่อผู้ใช้งาน(ภาษาอังกฤษ) รหัสพนักงาน เหตุผลในการขอใช้งานระยะเวลาในการใช้งาน และ MAC Address ของเครื่องคอมพิวเตอร์ที่จะใช้งาน ระบบงานที่เกี่ยวข้องมีดังนี้ Active Directory (สร้างเพื่อใช้เป็น User สำหรับ Logon Domain เท่านั้น), VPN

๔.๓ การถอดถอนสิทธิ

การถอดถอนสิทธิผู้ใช้งานเนื่องจากผู้ใช้งาน ลาออก หรือโยกย้ายหน้าที่ผู้ใช้งานความรับผิดชอบงาน

(๑) กรณีผู้ใช้งานลาออก ผู้บังคับบัญชาจะต้องแจ้งให้ทางผู้ดูแลระบบเพื่อทำการ Disable User ผู้ใช้งานทันที และจะขออนุมัติตามกระบวนการ Change Process เพื่อ Delete User ผู้ใช้งานออกจากระบบตามรอบทบทวนการใช้งานของ User ทุก ๆ ๓ เดือน

(๒) การทบทวน User ใช้งานตามรอบทุก ๆ ๓ เดือนโดยผู้ดูแลระบบจะ List User จากระบบต่าง ๆ และส่งข้อมูลให้กับผู้บังคับบัญชาเจ้าของข้อมูล/เจ้าของระบบ เพื่อยืนยันการใช้งานแต่ละ User กลับมา หากพบ User ที่ไม่ได้ใช้งานแล้วจะดำเนินการตามข้อ ๗.๒ (๑) ต่อไป

๔.๔ การบริหารสิทธิการเข้าถึงระบบของผู้ใช้งานระบบ (Privilege Management)

กำหนดสิทธิการใช้ข้อมูลและระบบสารสนเทศแก่ผู้ใช้งาน และงาน Operation กลุ่มงานนี้จะถูกการกำหนดสิทธิการเข้าถึงข้อมูล และระบบสารสนเทศไว้ ดังนี้

(๑) กลุ่มผู้ใช้งานที่เป็นเจ้าหน้าที่กงสุล และเจ้าหน้าที่ทดสอบระบบ เพื่อเข้าไปทดสอบเพื่อปรับปรุงพัฒนา Application ให้ใช้งานได้อย่างเหมาะสม และมีคุณภาพ โดยจะกำหนดให้มีการเข้ามาใช้งาน Application E-Back Office ผ่านการ VPN เท่านั้น

(๒) กลุ่มผู้ใช้งานที่เป็นผู้ดูแลระบบจะได้รับการอนุมัติจากผู้บังคับบัญชาเพื่อกำหนดสิทธิการเข้าถึงระบบสารสนเทศสำหรับงาน Operation เท่านั้น เช่น

- การ Monitoring (System, Network, Service, Server, Firewall และ Data Center and Facility)
- การ Query Data เพื่อนำข้อมูลมาวิเคราะห์ปัญหาในกรณีที่เกิด Incident
- การกำหนดสิทธิการใช้งาน User ให้กับเจ้าของระบบงาน E-Back Office เป็น Approve โดยจะได้รับสิทธิพิเศษระดับ Admin ที่มีสิทธิสร้าง User ที่เป็น staff ให้กับหน่วยงานที่รับผิดชอบ เข้าใช้งาน E-Back Office (Consular)

๔.๕ การกำหนดสิทธิสำหรับสิทธิพิเศษแก่ผู้ดูแลระบบ

สิทธิพิเศษของระบบงานต่าง ๆ เช่น Active Directory, PAM, VPN, Firewall, Network, Storage, vCenter, E-BackOffice, กล้องวงจรปิด CCTV, ระบบ Access Control (สแกนนิ้วเปิดประตู) และ Database

(๑) ผู้บังคับบัญชาจะเปลี่ยน Password และเก็บเข้าซองปิดผนึกไว้

(๒) กรณีที่ผู้ดูแลระบบจำเป็นต้องเบิก Password มาใช้งานงานจะต้องส่งเมล์แจ้งผู้บังคับบัญชาพร้อมระบุเหตุผล อ้างอิง Change Request หรือ Incident เท่านั้น และ ห้ามผู้ดูแลระบบ ใช้ชื่อผู้ใช้งานที่มีสิทธิระดับสูงในการปฏิบัติงานทั่วไป หลังใช้งานเสร็จจะต้องส่งเมล์แจ้งผู้บังคับบัญชา

(๓) ผู้บังคับบัญชาต้องเข้ามาเปลี่ยนรหัสผ่านโดยทันที หากมีความจำเป็นต้องใช้งานให้ส่งเมล์แจ้งขอใช้งานโดยจะเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน

๔.๖ การบริหารจัดการรหัสผ่านผู้ใช้งาน (User Password Management)

การกำหนดรหัสผ่าน

(๑) ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราวให้กับผู้ใช้งาน ที่มีความชั่วคราว และจัดส่งยากต่อการคาดเดาโดยผู้อื่น และกำหนดรหัสผ่านที่แตกต่างกัน โดยใช้รหัสผ่านการ Password Generator

(๒) ใส่ซองปิดผนึกส่งให้กับผู้ใช้งาน (เจ้าหน้าที่กงสุล) และโทรแจ้งเฉพาะบุคคลที่ใช้งาน เจ้าหน้าที่ทดสอบระบบ

การเปลี่ยนรหัสผ่าน

ผู้ใช้งานหลังจากได้รหัสผ่านชั่วคราว จะต้องเปลี่ยนรหัสผ่านทันที และควรเปลี่ยนรหัสผ่านให้มีความยากต่อการคาดเดาโดยผู้อื่น

๔.๗ การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

ตรวจสอบรายชื่อผู้ใช้งานระบบ

ผู้ดูแลระบบต้องดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของบุคลากรที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) หรือได้รับแจ้งจากผู้ใช้งานทางอีเมล์ หนังสือ โดยตรวจสอบทุก ๆ ๓ เดือน

ระงับการใช้งาน

ผู้ดูแลระบบต้องดำเนินการโดยทันทีเมื่อตรวจพบความผิดปกติในการเข้าถึงระบบสารสนเทศ ได้แก่ การระงับ (Disable) การใช้งาน เปลี่ยนรหัสผ่าน และ ลบออกจากระบบ ตามรอบทุก ๆ ๓ เดือนตามกระบวนการ Change Process

****

ส่วนที่ ๕ การรับผิดชอบหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๕.๑ การใช้งานรหัสผ่าน (Password Use)

การใช้รหัสผ่านของผู้ใช้งานระบบ และผู้ดูแลระบบ

(๑) ต้องเก็บรหัสผ่านไว้เป็นความลับ และไม่ใช้รหัสผ่านร่วมกับผู้อื่น

(๒) หลีกเลี่ยงการบันทึกรหัสผ่าน (เช่น บันทึกลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่าง ๆ) นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยมีการเข้ารหัสลับ (Encryption) เพื่อป้องกัน หรือวิธีในการบันทึกนั้นได้รับการอนุมัติแล้ว

(๓) กำหนดรหัสผ่านที่มีคุณภาพ โดยให้สอดคล้องกับข้อกำหนดเรื่องการตั้งและเปลี่ยนหัสผ่านที่มีความมั่นคงปลอดภัยของ Visa Data Center

(๔) เปลี่ยนรหัสผ่านทุกครั้ง ในทันทีที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

(๕) เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนดหรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้งานที่ได้สิทธิพิเศษควรได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) โดยให้สอดคล้องกับข้อกำหนดเรื่องการตั้งและเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยของ Visa Data Center

(๖) เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

(๗) ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการเข้าสู่ระบบอัตโนมัติ (Auto Login)

(๘) ไม่ใช้รหัสผ่านที่ใช้ในระบบงานของ Visa Data Center ไปตั้งเป็นค่ารหัสผ่านของระบบงานส่วนตัว

(๙) ต้องตรวจสอบว่ามีการกำหนดรหัสผ่านที่รัดกุมตามแนวทางปฏิบัติดังกล่าว สำหรับบัญชีผู้ใช้งานทั้งหมดบนทุกอุปกรณ์เทคโนโลยีสารสนเทศ

๕.๒ การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended User Equipment)

การป้องกันอุปกรณ์ของผู้ดูแลระบบ

(๑) ผู้ดูแลระบบต้องออกจากระบบสารสนเทศของ Visa Data Center โดยทันที เมื่อเสร็จสิ้นการใช้งาน เช่น ออกจากระบบงาน ออกจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้งาน (Logout)

(๒) ผู้ดูแลระบบต้องล็อก (Lock) อุปกรณ์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว เช่น การล็อกหน้าจอด้วยรหัสผ่านและการล็อกคอมพิวเตอร์แบบพกพาเข้ากับสายล็อกเพื่อป้องกันการถูกขโมยเครื่อง

(๓) ผู้ดูแลระบบต้องป้องกันไม่ให้ผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบสารสนเทศ โดยการกำหนดให้ต้องใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

(๔) ผู้ดูแลระบบต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอ หลังจากที่ไม่ได้ใช้งานมาช่วงระยะเวลาหนึ่งโดยอัตโนมัติ ๑๕ นาที หลังจากที่มีการล็อกหน้าจอแล้วนั้น ต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้

(๕) ผู้ดูแลระบบต้องปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือไม่มีการใช้งานนานเกินกว่า ๑ ชั่วโมง เว้นแต่ เครื่องคอมพิวเตอร์นั้นเป็น

เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ซึ่งต้องใช้งานตลอด ๒๔ ชั่วโมง ให้ผู้ดูแลระบบออกจากระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายหรือล็อกหน้าจอ

๕.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

(๑) ผู้ดูแลระบบต้องจัดให้มีการควบคุมสินทรัพย์สารสนเทศ และการใช้งานระบบคอมพิวเตอร์ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๒) เมื่อสินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือข้อมูลอิเล็กทรอนิกส์ไม่สามารถใช้งานได้แล้ว ให้ผู้ดูแลระบบทำลายสินทรัพย์สารสนเทศ ดำเนินการโดยมีข้อปฏิบัติ ดังนี้

- กระดาษ ให้ทำลายด้วยการหั่นด้วยเครื่องหั่นทำลายเอกสาร
- ซีดีหรือดีวีดี ให้ทำลายด้วยการหั่นด้วยเครื่องหั่นทำลายเอกสาร
- เทป ให้ทำลายด้วยการทุบหรือบดให้เสียหาย หรือเผาทำลาย
- ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ต่าง ๆ ให้ทำลายด้วยการเขียนทับข้อมูลซ้ำหลายรอบหรือทำให้เสียหายทางกายภาพ โดยวิธีการทำลาย ทุบ บดหรือเจาะให้เสียหาย

(๓) ผู้ใช้งานทุกคนต้องป้องกันทรัพย์สินอย่างเคร่งครัด

(๔) ผู้ใช้งานทุกคนต้องออกจากระบบที่ใช้งานทันที เมื่อจำเป็นต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแล

(๕) ผู้ใช้งานทุกคนต้องจัดเก็บข้อมูลสารสนเทศที่มีความสำคัญของกรมการกงสุลไว้ในที่ปลอดภัย เช่น เก็บไว้ในตู้เก็บเอกสารที่มีระบบล็อก และมีกุญแจเปิดปิด

๕.๔ การนำเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ

ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ดังต่อไปนี้

- ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- ต้องกำหนดรายชื่อผู้ใช้ และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลแต่ละชั้นความลับของข้อมูล
- ต้องกำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องมีการเข้ารหัส ที่เป็นมาตรฐานสากล อาทิ SSL VPN
- กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

****

ส่วนที่ ๖ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๖.๑ การปฏิบัติในการยืนยันตัวบุคคล (User Identification and Authentication)

(๑) ผู้บังคับบัญชาต้องออกแบบการตั้งชื่อบัญชีผู้ใช้งานในระบบงานที่แตกต่างกันตามหน้าที่เพื่อใช้ในการแสดงตัวตน เช่น บัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบ บัญชีของผู้ดูแล ฐานข้อมูล บัญชีของผู้พัฒนาระบบ บัญชีของผู้ใช้งานทางเทคนิคอื่น ๆ

(๒) ตั้งชื่อผู้ใช้งานแต่ละบุคคลให้แยกออกจากกันเพื่อใช้ในการแสดงตัวตนและพิสูจน์ตัวตนที่แตกต่างกัน

(๓) แสดงตัวตนและพิสูจน์ตัวตนทุกครั้ง ก่อนใช้ระบบสารสนเทศ โดยใช้ชื่อบัญชีผู้ใช้งาน (User account) และรหัสผ่าน (Password) เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งเปิดตาม Incident Process เพื่อให้ผู้ดูแลระบบแก้ไข

(๔) กำหนดให้ผู้ใช้งานที่เป็นเจ้าของชื่อบัญชีผู้ใช้งาน ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น โดยไม่ได้เกิดจากความประมาทเลินเล่อของผู้ใช้งาน

(๕) กำหนดให้ผู้ใช้งานต้องเก็บรักษารหัสผ่านของบัญชีผู้ใช้งาน ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

(๖) กำหนดให้ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อบัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

(๗) กำหนดให้ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานเข้ามาปฏิบัติงานที่ห้องปฏิบัติการครือข่าย ต้องแจ้งให้ผู้ดูแลระบบรับทราบทุกครั้ง (เฉพาะกรณีที่ต้องมาแก้ไข Incident หรือการเข้าบำรุงรักษาเครื่อง เท่านั้น)

(๘) กำหนดให้ผู้ใช้งานที่ต้องการเข้าถึงระบบสารสนเทศ จากภายนอก ต้องได้รับอนุญาตจากผู้มีอำนาจก่อน และเป็นผู้ที่ได้รับสิทธิในการเข้าใช้บริการแล้วเท่านั้น และต้องเชื่อมต่อตามแนวทางปฏิบัติงานจากภายนอก

๖.๒ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

(๑) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งการเข้าถึงทางกายภาพ และเข้าถึงการควบคุมพอร์ตผ่านทางระบบเครือข่าย เช่น การยืนยันตัวตนก่อนการเข้าปฏิบัติงาน

(๒) ควบคุมสถานที่ติดตั้งอุปกรณ์เครือข่ายที่เป็นช่องทางที่สามารถใช้สำหรับการปรับแต่งการกำหนดค่าการทำงานของระบบเครือข่าย เพื่อป้องกันการเข้าถึงทางกายภาพด้วยการต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(๓) ยกเลิกหรือปิดหมายเลขพอร์ตที่ไม่มีความจำเป็นในการใช้งานบนอุปกรณ์ที่ติดตั้งอยู่ร่วมกับระบบเครือข่าย รวมถึงมีการตรวจสอบและปิดช่องทางเข้าถึงพอร์ตทางกายภาพ ของระบบหรืออุปกรณ์อย่างสม่ำเสมอ โดยมีการตรวจสอบ ๓ เดือนครั้งสำหรับระบบที่มีผลกระทบและมีความสำคัญสูง และปีละ ๑ ครั้งสำหรับระบบทั่วไป

(๔) ต้องเปลี่ยนหัสผ่านเริ่มต้นที่ติดมากับระบบ (Default Password) โดยทันที

(๕) ติดตั้งอุปกรณ์ป้องกันพอร์ต เพื่อป้องกันการบุกรุกโดยผู้ไม่ประสงค์ดี หรือใช้งานผิดวัตถุประสงค์ของการบริการใด ๆ

(๖) กำหนดให้มีการเปิด - ปิดช่องทางติดต่อสื่อสารของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงของอุปกรณ์เครือข่ายต่าง ๆ โดยปิดช่องทางติดต่อสื่อสารที่มีความเสี่ยง ไม่ปลอดภัย หรืออาจก่อให้เกิดความเสียหายต่อระบบเครือข่าย

(๗) กำหนดให้บุคคลภายนอกที่เข้าดำเนินการบำรุงรักษา บริหารจัดการช่องทางติดต่อสื่อสารของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องแจ้งให้ผู้ดูแลระบบรับทราบก่อนทุกครั้ง

๖.๓ การควบคุมผู้ใช้งานในการใช้งานเครือข่าย (Network Connection Control)

(๑) ต้องทำการป้องกันเลขที่อยู่ไอพี (IP Address) ภายในของระบบในการใช้งานเครือข่ายมิให้หน่วยงานภายนอกสามารถมองเห็นและเชื่อมต่อได้โดยตรง

(๒) ต้องทำการติดตั้งซอฟต์แวร์หรือฮาร์ดแวร์ที่สามารถบันทึกการทำงานของระบบเครือข่าย การปฏิบัติงานของผู้ใช้งาน การบุกรุก การเข้าออกระบบ การใช้งานและข้อมูลจราจรคอมพิวเตอร์ และต้องมีการจัดเก็บข้อมูลเหล่านี้ไว้ไม่ต่ำกว่า ๙๐ วัน

(๓) ต้องทำการควบคุมและจำกัดสิทธิการเชื่อมต่อทางระบบเครือข่ายของผู้ใช้งานต่อระบบงานและการโอนย้ายไฟล์ ดังนี้

- ต้องมีการลงทะเบียนผู้ใช้งานเพื่อระบุตัวตนในการเข้าใช้งานระบบ
- ต้องมีการจำกัดสิทธิให้เข้าใช้งานได้เฉพาะระบบงานที่ได้รับอนุญาตเท่านั้น
- ต้องมีการจำกัดสิทธิให้สามารถโอนย้ายไฟล์ได้เฉพาะไฟล์ที่รับอนุญาตเท่านั้น
- ต้องทำการควบคุมบุคคลหรือหน่วยงานภายนอกที่ทำการเข้าใช้หรือเชื่อมต่อกับระบบเครือข่าย
- บุคคลหรือหน่วยงานภายนอกที่ต้องการเชื่อมต่อกับระบบเครือข่ายต้องมีการร้องขอเข้าใช้งานพร้อมระบุเหตุผลในการเข้าใช้งาน
- การร้องขอเข้าใช้งานต้องได้รับอนุญาตจากผู้บริหารที่มีอำนาจของฝ่ายเทคโนโลยีสารสนเทศ
- ต้องมีการควบคุมช่องทางพอร์ตที่เข้ามาใช้งานอย่างรอบคอบรัดกุม
- ต้องมีการกำหนดระยะเวลาในเชื่อมต่อและต้องทำการปิดการเชื่อมต่อทันทีที่ถึงกำหนดเวลา
- ต้องมีการจำกัดเส้นทางในการเชื่อมต่อรวมถึงควบคุมซอฟต์แวร์หรือฮาร์ดแวร์ที่นำมาใช้ในการเชื่อมต่อให้เป็นไปตามที่ฝ่ายเทคโนโลยีสารสนเทศ กำหนดไว้เท่านั้น

(๔) ต้องทำการควบคุมการเชื่อมต่ออินเทอร์เน็ตและระบบงานต่าง ๆ ดังนี้

- ต้องจัดให้มีการลงทะเบียนเพื่อระบุตัวตนในการเข้าใช้งาน
- การลงทะเบียนต้องทำเฉพาะบุคคลเท่านั้น โดยห้ามกระทำการโอนสิทธินี้แก่ผู้อื่น
- ต้องมีการจำกัดสิทธิเพื่อควบคุมผู้ใช้งานให้สามารถเข้าใช้งานได้เฉพาะระบบเครือข่ายและระบบงานที่ได้รับอนุญาตเท่านั้น

- ต้องมีการตรวจสอบและทบทวนสิทธิอย่างสม่ำเสมอทุก ๆ ๓ เดือน

๖.๔ การจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน (Network Routing Control)

(๑) กำหนดไม่ให้มีการเปิดเผยแผนการใช้งานเลขที่อยู่ไอพี (IP Address)

(๒) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์หนึ่งเครื่องใด ไปยังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่าย โดยไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

(๓) ไม่อนุญาตให้บุคคลใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใด ๆ ต่ออุปกรณ์เครือข่ายส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

(๔) ไม่อนุญาตผู้ใช้งานทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) หรือกำหนดค่าเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์ภายในหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

(๕) ต้องดำเนินการใด ๆ เพื่อยุติการกระทำของผู้ใช้งานที่ไม่เป็นไปตามแนวปฏิบัตินี้ และในกรณีที่จำเป็นให้ระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าว เพื่อป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นแก่
Visa Data Center

(๖) ผู้ดูแลระบบต้องดูแลรักษาและปรับปรุงระบบควบคุมการจัดเส้นทางบนเครือข่ายให้สามารถใช้งานได้ดีอยู่เสมอ

(๗) ผู้ดูแลระบบต้องดูแลการใช้งานระบบควบคุมการจัดเส้นทางบนเครือข่ายให้เป็นไปตามแนวทางนี้ กรณีที่พบว่ามีการกระทำหรือการใช้งานที่ไม่ถูกต้องให้รายงานต่อผู้บังคับบัญชาทราบโดยเร็ว และหากมีความจำเป็นเพื่อป้องกันความเสียหาย หรือ ผลกระทบที่อาจเกิดขึ้นต่อผู้อื่นหรือต่อการใช้งานระบบสารสนเทศโดยส่วนรวม ให้ผู้ดูแลระบบระงับการใช้งานดังกล่าว

(๘) ผู้ดูแลระบบต้องจัดทำบัญชีอุปกรณ์เครือข่าย บัญชีเครื่องคอมพิวเตอร์แม่ข่าย ที่ระบุถึงการเชื่อมโยง การจัดสรรหมายเลขที่อยู่ไอพี (IP Address) และ MAC Address และผู้มีสิทธิใช้งาน พร้อมปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ

(๙) ผู้ดูแลระบบต้องทบทวนและตรวจสอบเส้นทางบนเครือข่ายให้เป็นไปตามที่กำหนดปีละ ๑ ครั้งและปรับปรุงแก้ไขหรือยกเลิกเส้นทางที่ไม่มีความจำเป็นต้องใช้งาน

๖.๕ การแบ่งแยกเครือข่าย

ผู้ดูแลระบบต้องมีการออกแบบและทำการแบ่งแยกเครือข่าย (segregation in networks) โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายในและเครือข่ายสำหรับผู้ใช้งานภายนอก เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

****

ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๗.๑ วัตถุประสงค์

(๑) เพื่อกำหนด แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ Visa Data Center ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และปฏิบัติตามอย่างเหมาะสม

(๒) เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของ Visa Data Center ว่า สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีความพร้อมใช้งาน (Availability)

(๓) เพื่อให้ผู้ใช้งานและผู้ดูแลระบบได้มีแนวปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการเข้าถึงข้อมูลและการใช้งานสารสนเทศ โดยต้องมีการป้องกันและควบคุมการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศจากผู้ไม่มีสิทธิ ทั้งนี้เพื่อให้เกิดความมั่นคงปลอดภัยทั้งต่อข้อมูลและระบบสารสนเทศ

(๔) เพื่อเผยแพร่ให้เจ้าหน้าที่และผู้ใช้งานสารสนเทศของ Visa Data Center ได้รับทราบและถือปฏิบัติตามอย่างเคร่งครัด

(๕) เพื่อเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยสารสนเทศในการดำเนินกิจกรรมอันเกี่ยวข้องกับระบบสารสนเทศ

๗.๒ แนวปฏิบัติ

(๑) ผู้ใช้งานต้องระบุ ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ทุกครั้งก่อนการเข้าใช้ระบบปฏิบัติการ

(๒) การควบคุมการแก้ไขหรือปรับแต่งค่าในระบบปฏิบัติการ ต้องผ่านการอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมรักษาหน้าจอ (Screen saver) ทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หรือลงบันทึกออก (Logout) จากระบบปฏิบัติการทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน หลังจากนั้นเมื่อต้องการใช้งานระบบปฏิบัติการอีก ต้องใส่รหัสผ่านอีกครั้งเพื่อเข้าใช้งาน

(๔) จำกัดระยะเวลาและจำนวนครั้งในการป้อนรหัสผ่านเพื่อเข้าถึงระบบปฏิบัติการ หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนที่กำหนดไว้ ให้ทำการล็อกสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีก จนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อกให้

(๕) ผู้ดูแลระบบต้องออกแบบการตั้งชื่อบัญชีผู้ใช้งานในระบบงานที่แตกต่างกันตามหน้าที่เพื่อใช้ในการแสดงตัวตน เช่น บัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบ บัญชีของผู้ดูแลฐานข้อมูล บัญชีของผู้พัฒนาระบบ บัญชีของผู้ใช้งานทางเทคนิคอื่น ๆ

(๖) ตั้งชื่อผู้ใช้งานแต่ละบุคคลให้แยกออกจากกันเพื่อใช้ในการแสดงตัวตนและพิสูจน์ตัวตนที่แตกต่างกัน

(๗) กำหนดให้ผู้ใช้งานที่เป็นเจ้าของชื่อบัญชีผู้ใช้งาน ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น โดยไม่ได้เกิดจากความประมาทเลินเล่อของผู้ใช้งาน

(๘) กำหนดให้ผู้ใช้งานต้องเก็บรักษารหัสผ่านของบัญชีผู้ใช้งาน ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

(๙) กำหนดให้ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อบัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

(๑๐) ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราวให้กับผู้ใช้งาน ที่มีความยากต่อการคาดเดาโดยผู้อื่น และกำหนดรหัสผ่านที่แตกต่างกัน โดยใช้การ Password Generator

(๑๑) ผู้ดูแลระบบต้องออกจากระบบสารสนเทศของ Visa Data Center โดยทันที เมื่อเสร็จสิ้นการใช้งานอาทิ ออกจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้งาน (Logout)

(๑๒) ผู้ดูแลระบบต้องล็อก (Lock) อุปกรณ์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว เช่น การล็อกหน้าจอด้วยรหัสผ่าน และการล็อกคอมพิวเตอร์แบบพกพาเข้ากับสายล็อกเพื่อป้องกันการถูกขโมยเครื่อง

(๑๓) ผู้ดูแลระบบต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอ หลังจากที่ไม่ได้ใช้งานมาช่วงระยะเวลาหนึ่งโดยอัตโนมัติ ๑๕ นาที หลังจากที่มีการล็อกหน้าจอแล้วนั้น ต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้

(๑๔) ผู้ดูแลระบบต้องปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือไม่มีการใช้งานนานเกินกว่า ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ซึ่งต้องใช้งานตลอด ๒๔ ชั่วโมง ให้ผู้ดูแลระบบออกจากระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายหรือล็อกหน้าจอ

(๑๕) เมื่อผู้ใช้งานลาออก โยกย้ายหน้าที่ หรือพ้นจากตำแหน่ง จะต้องการถอดถอนสิทธิผู้ใช้งานออกจากระบบ

(๑๖) การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้นตามระยะเวลาที่กำหนด ดังนี้

- ต้องกำหนดให้ระบบสารสนเทศ ได้แก่ ระบบงานต่าง ๆ ของกรม อุปกรณ์เครือข่าย มีการตัดและหมดเวลาการใช้งาน รวมถึงการปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๑๐ นาที
- ต้องกำหนดให้ระบบสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ
- ต้องกำหนดให้ระบบสารสนเทศที่มีความสำคัญและมีความเสี่ยงสูง มีการตัดและหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๑๗) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ดังนี้

- ต้องกำหนดให้ระบบสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้นโดยกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาทำงานราชการตามปกติเท่านั้น

- ต้องกำหนดให้ระบบสารสนเทศที่ความสำคัญและมีความเสี่ยงสูง กำหนดให้ใช้งานได้ ๒ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง มีการตัดและหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- ต้องกำหนดให้ระบบสารสนเทศที่ต้องมีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานตามระยะเวลาที่กำหนดไว้ข้างต้น

(๑๘) การบริหารจัดการรหัสผ่าน (Password Management System) เชิงโต้ตอบ

- ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย โดยกำหนดให้รหัสผ่านมีความยาวอย่างน้อย ๘ หลัก ประกอบด้วย (a) ตัวอักษรเล็กไม่น้อยกว่า ๑ ตัว ตัวอักษรใหญ่ไม่น้อยกว่า ๑ ตัว และ (b) อักขระพิเศษ

- รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก โดยเลือกรหัสผ่านที่ปลอดภัย และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้ (ทุก ๆ ๓ เดือน หรือเมื่อระบบแจ้งเตือนให้เปลี่ยนรหัสผ่าน)

- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๓ เดือน

- ในการเปลี่ยนรหัสผ่านแต่ละครั้งจะกำหนดรหัสผ่านซ้ำกับที่เคยกำหนดมาแล้ว ๓ ครั้งล่าสุดไม่ได้

- ระบบบริหารจัดการรหัสผ่านต้องป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ หรือที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

- ผู้ใช้งานใส่รหัสผ่านผิดเกิน ๕ ครั้ง ระบบจะต้องทำการยึดชื่อผู้ใช้ (Lock Username) ไม่ให้ทำการล็อกอิน (Login) จนกว่าจะครบ ๑๕ นาที หรือ ติดต่อผู้ดูแลระบบ เพื่อปลดล็อก

- กรณีมีการแจ้งเตือนให้เปลี่ยนรหัสผ่านล่วงหน้าอย่างน้อย ๑ สัปดาห์ ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ทันที

(๑๙) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

ผู้ดูแลระบบต้องกำหนดให้ควบคุมการใช้โปรแกรมอรรถประโยชน์สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- จำกัดการใช้งานโปรแกรมอรรถประโยชน์ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

- ให้แยกโปรแกรมอรรถประโยชน์ออกจากโปรแกรมระบบงาน

- โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

****

ส่วนที่ ๘ แนวทางปฏิบัติในการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์
(Application and Information Technology Access Control)

๘.๑ วิธีปฏิบัติการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์

(๑) กำหนดให้ผู้ดูแลระบบต้องควบคุม จำกัด หรือให้สิทธิการเข้าถึงสารสนเทศและสารสนเทศ ข้อมูล และฟังก์ชันต่าง ๆ ของระบบสารสนเทศและโปรแกรมประยุกต์ ดังนี้

- ต้องลงทะเบียนการเข้าใช้งานเพื่อทำการระบุตัวตน
- ให้เข้าถึงได้เฉพาะส่วนระบบงานและฟังก์ชันที่จำเป็นต่อการทำงานและที่ได้รับอนุญาตเท่านั้น
- ให้เข้าถึงได้เฉพาะข้อมูลที่จำเป็นต่อการใช้งานและที่ได้รับอนุญาตเท่านั้น
- ห้ามไม่ให้กระทำการโอนย้ายสิทธิแก่ผู้อื่น โดยสิทธิการเข้าใช้งานให้เป็นสิทธิเฉพาะบุคคลเท่านั้น
- ให้ทำการยกเลิกสิทธิการเข้าใช้งานทันทีที่ผู้ได้รับสิทธินั้น ไม่ได้รับสิทธิการเข้าใช้งานอีกต่อไป
- กำหนดให้มีข้อความแสดงเตือนถึงผู้ไม่มีสิทธิเข้าถึงหรือใช้งานสารสนเทศ ระบบงาน ข้อมูลและฟังก์ชันต่าง ๆ ของระบบงาน

(๒) กำหนดให้ผู้ดูแลระบบต้องทำการควบคุมหรือจำกัดสิทธิการเข้าถึงระบบงานซึ่งถูกเข้าถึงจากอีกระบบงานหนึ่ง ดังนี้

- ให้เข้าถึงได้เฉพาะส่วนฟังก์ชันที่จำเป็นต่อการใช้งานและที่ได้รับอนุญาตเท่านั้น
- ให้เข้าถึงได้เฉพาะข้อมูลที่จำเป็นต่อการใช้งานและที่ได้รับอนุญาตเท่านั้น
- กำหนดให้มีการพิสูจน์ตัวตน (Authentication) ก่อนการเข้าถึงระบบงานทุกครั้ง
- กำหนดให้มีการจำกัดเส้นทางและวิธีการในการเข้าถึงระบบงานจากอีกระบบงานหนึ่ง
- กำหนดให้มีการทบทวนสิทธิในการเข้าถึงทุก ๆ ๓ เดือน

(๓) กำหนดให้ผู้ดูแลระบบต้องทำการควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงานหนึ่ง โดยให้นำข้อมูลออกได้เฉพาะที่เกี่ยวข้องและจำเป็นสำหรับการนำไปใช้งานเท่านั้น

(๔) กำหนดให้ระบบที่ใช้งานต้องมีการแสดงเฉพาะข้อมูลพื้นฐานเพื่อให้ผู้ใช้งานได้รับทราบข้อมูลเฉพาะที่จำเป็น และตามสิทธิการใช้งานเท่านั้น

(๕) กำหนดให้ระบบที่ใช้งานต้องมีข้อจำกัดไม่ให้ระบบแสดงความช่วยเหลือใด ๆ กรณีที่มีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นในระบบ

(๖) กำหนดให้ระบบที่ใช้งานต้องมีฟังก์ชันที่สามารถทำการตรวจสอบและควบคุมการลงบันทึกเข้า (Login) ดังนี้

- แสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ลงบันทึกเข้า (Login) เสร็จแล้ว
- ตรวจสอบข้อมูลการลงบันทึกเข้า (Login) หลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว
- จำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการลงบันทึกเข้า (Login) ผิด
- กำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบงานได้ภายหลังจากที่ใส่ข้อมูลการลงบันทึกเข้า (Login) ผิดเกินกว่าจำนวนครั้งที่กำหนด

- กำหนดให้มีฟังก์ชันที่สามารถส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามลงบันทึกเข้า (Login) แต่ผิดพลาดเป็นจำนวนหลายครั้ง

- กำหนดให้มีการบันทึกข้อมูลลงบันทึกเข้า (Login) ทั้งที่สำเร็จและไม่สำเร็จ

- จำกัดช่วงเวลาที่นานที่สุดที่ผู้ใช้งานจะลงบันทึกเข้า (Login) ให้สำเร็จ

- แสดงวันที่/เวลาที่ลงบันทึกเข้า (Login) ครั้งที่แล้ว (ทั้งที่สำเร็จและไม่สำเร็จ)

๘.๒ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๑) กำหนดให้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ผู้บังคับบัญชา อนุญาตให้บุคคลใดนำไปใช้งานเป็นทรัพย์สิน ดังนั้นผู้ใช้งานต้องใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่อย่างมีประสิทธิภาพเพื่องานของ Visa Data Center

(๒) มีการวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เพื่อนำมาทบทวนและปรับปรุงการใช้งาน

(๓) มีระบบควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อบริหารจัดการและควบคุมการใช้งานที่ส่วนกลางและบริหารจัดการการควบคุม กำหนดสิทธิการใช้งาน จัดการกับข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ผ่านเครือข่ายอินเทอร์เน็ต

(๔) มีมาตรการในการตรวจจับและป้องกันโปรแกรมไม่พึงประสงค์ต่าง ๆ (Anti-malware)

(๕) ควบคุมการเข้าถึงระบบงานของ Visa Data Center จากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ซึ่งเชื่อมต่อผ่านทางเครือข่ายอื่น ๆ เช่น อินเทอร์เน็ตสาธารณะ โดยให้ปฏิบัติตามแนวทางปฏิบัติในการปฏิบัติงานจากภายนอก

(๖) ควบคุมการติดตั้งซอฟต์แวร์หรือโปรแกรมประยุกต์ ในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยให้ปฏิบัติตามแนวทางปฏิบัติในการเข้าถึงระบบปฏิบัติการ

(๗) ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ให้เป็นไปตามแนวทางปฏิบัติ กรณีที่พบว่ามีการกระทำหรือการใช้งานที่ไม่ถูกต้อง ให้รายงานต่อผู้บังคับบัญชาทราบโดยเร็ว

(๘) ต้องเก็บรักษาความลับของข้อมูลอันเนื่องมาจากการปฏิบัติหน้าที่

(๙) ต้องไม่ใช้อำนาจหน้าที่ในการเข้าถึงข้อมูลใดที่ตนไม่มีสิทธิเข้าถึงนอกจากงานในหน้าที่

๘.๓ การควบคุมการจ้างเหมาพัฒนา ตรวจสอบ ดูแลและบำรุงรักษาระบบ (Outsource)

ในการจ้างเหมาพัฒนา ตรวจสอบ ดูแลและบำรุงรักษาระบบ ผู้ใช้งานภายนอกที่เข้าถึงระบบสารสนเทศต้องดำเนินการ ดังต่อไปนี้

- ผู้ใช้งานภายนอกมีสิทธิในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ และระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งานเท่านั้น

- ผู้ใช้งานภายนอกต้องพิสูจน์ตัวตนก่อนที่เข้ามาใช้งานระบบสารสนเทศ ได้แก่ ชื่อผู้ใช้งานและรหัสผ่านสำหรับเข้าใช้งานระบบสารสนเทศ โดยผู้ดูแลระบบต้องตั้งชื่อผู้ใช้งานแต่ละบุคคลให้แยกออกจากกันเพื่อใช้ในการแสดงตัวตนและพิสูจน์ตัวตนที่แตกต่างกัน

- ในระบบที่มีความสำคัญสูงต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากผู้บริหารก่อน

๘.๔ การจัดการกับระบบซึ่งไวต่อการรบกวน

ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องมีการควบคุมสภาพแวดล้อมของตนเอง โดยเฉพาะการเข้า-ออก ห้องเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ซึ่งเป็นห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิให้เฉพาะผู้มีสิทธิใช้ระบบเท่านั้นที่สามารถเข้าไปปฏิบัติงานได้ และมีการจัดให้มีการบริหารจัดการสภาพแวดล้อมในส่วนของพื้นที่ห้องเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ดังนี้

- กำหนดระเบียบและแนวทางปฏิบัติในการเข้า-ออก พื้นที่ห้องเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย
- ควบคุมการเข้า-ออก ด้วยระบบ Access Card หรือระบบ Biometrics พร้อมระบบ CCTV
- ติดตั้งระบบปรับอากาศควบคุมความชื้นอัตโนมัติ
- ติดตั้งระบบป้องกันสัญญาณรบกวนไฟฟ้าและอิเล็กทรอนิกส์
- ติดตั้งระบบเครื่องกำเนิดไฟฟ้าและระบบเครื่องสำรองไฟฟ้า
- ติดตั้งระบบตรวจจับการรั่วซึมของน้ำ
- ติดตั้งระบบดับเพลิงอัตโนมัติและระบบตรวจสอบควันไฟ
- ติดตั้งระบบไฟส่องสว่างฉุกเฉิน

****

ส่วนที่ ๙ แนวปฏิบัติในการสำรองข้อมูลและระบบสารสนเทศ

๙.๑ วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติในการสำรองและกู้คืนข้อมูล ให้ผู้ดูแลระบบสารสนเทศและระบบเครือข่ายสามารถดำเนินการได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น โดยนโยบายแนวปฏิบัติต้องมีการดำเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้ง ต่อปี

๙.๒ แนวปฏิบัติ

การสำรองข้อมูล

(๑) พิจารณาคัดเลือกและทบทวนระบบสารสนเทศที่มีความสำคัญ กำหนดประเภทของข้อมูลและกำหนดความถี่ในการจัดทำระบบสำรองที่เหมาะสมอย่างน้อยปีละ ๑ ครั้ง โดยทำการประเมินความเสี่ยงที่มีผลทำให้ระบบสารสนเทศที่มีความสำคัญสูงไม่สามารถทำงานได้อันเป็นผลมาจากภัยพิบัติอันอาจมีผลกระทบต่อระบบสารสนเทศ

(๒) การจัดทำบันทึกการสำรองข้อมูล ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ วันที่เวลาเริ่มต้นและสิ้นสุด ชนิดของข้อมูลที่บันทึก เป็นต้น

(๓) ให้ผู้ดูแลระบบมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรอง ในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

(๔) ให้ผู้ดูแลระบบกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งสื่อที่ใช้เก็บข้อมูล

(๕) ผู้ดูแลระบบต้องพิจารณาคัดเลือกจัดทำระบบสำรองหรือทำการสำรองข้อมูลที่เหมาะสมเพื่อให้อยู่ในสภาพที่พร้อมใช้งาน ตามแผนการสำรองข้อมูลที่กำหนด

(๖) ผู้ดูแลระบบ ต้องตรวจสอบผลการสำรองข้อมูลด้วยว่าการสำรองข้อมูลถูกต้องสมบูรณ์หรือไม่

(๗) ผู้ดูแลระบบ ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขรายงานต่อผู้บังคับบัญชา

(๘) มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

(๙) ต้องบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรองสำเร็จ/ไม่สำเร็จ เป็นต้น

(๑๐) มีการจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ในการสำรองข้อมูลไว้อย่างชัดเจน และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

(๑๑) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

แผนการสำรองข้อมูล

ที่	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Web Servers Application Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	Full backup แบบ Daily weekly และ Monthly
๒	Database Server	ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	Full backup แบบ Daily weekly และ Monthly
๓	vCenter	ข้อมูลสำคัญสำหรับจัดการควบคุม VMWare	Full backup แบบ Daily weekly และ Monthly
๔	System และ Components	ข้อมูลสำคัญของระบบ รวมถึง Components บนเครื่อง Server ต่าง ๆ	Full backup แบบ Daily weekly และ Monthly
๕	Server อื่น ๆ	ค่า Configure	Full backup แบบ Daily weekly และ Monthly

การกู้คืนข้อมูล

(๑) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบสารสนเทศและ/หรือระบบเครือข่ายจนเป็นเหตุให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งรายงานสรุปผลการปฏิบัติการ ต่อผู้บังคับบัญชา

(๒) ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม สำหรับการกู้คืนระบบ

(๓) หากการเสียหายที่เกิดขึ้นกับระบบสารสนเทศ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ที่เกี่ยวข้องรับทราบทันที

(๔) มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์โดยผู้บังคับบัญชาเป็นผู้กำกับดูแลการปฏิบัติงาน ความถี่อย่างน้อยปีละ ๑ ครั้ง

(๕) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

(๖) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบสารสนเทศหรือระบบเครือข่าย จนเป็นเหตุต้องมีการดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบ (System Administrator) ดำเนินการแก้ไข และรายงานปัญหาดังกล่าวต่อผู้บังคับบัญชา ทราบโดยด่วน

(๗) กรณีความเสียหายที่เกิดขึ้นกับระบบสารสนเทศหรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้รีบแจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบ เมื่อการดำเนินการกู้คืนระบบเสร็จสิ้นสมบูรณ์

แผนการกู้คืนข้อมูล

สาเหตุ	วิธีการ	ผู้รับผิดชอบ
กรณีที่ ๑ เกิดความเสียหายขึ้นกับโปรแกรมต้นฉบับ (Source Code)	ดำเนินการติดตั้งโปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด	- ผู้อำนวยการกอง สำนัก หรือผู้ดูแลระบบของกรม ที่ได้รับมอบหมาย หรือ - ศูนย์บริหารข้อมูลการกงสุลและสารสนเทศ และ - ผู้สนับสนุนและให้บริการของกรม
กรณีที่ ๒ เกิดความเสียหายขึ้นกับฐานข้อมูล	ดำเนินการกู้คืนฐานข้อมูลที่เก็บไว้ล่าสุด เพื่อให้ใช้งานได้ต่อเนื่องและข้อมูลสูญหายน้อยที่สุด	- ผู้อำนวยการกอง สำนัก หรือผู้ดูแลระบบของกรม ที่ได้รับมอบหมาย หรือ - ศูนย์บริหารข้อมูลการกงสุลและสารสนเทศ และ - ผู้สนับสนุนและให้บริการของกรม
กรณีที่ ๓ เกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดย Hardware ยังคงทำงานได้ปกติ	จะทำการติดตั้งระบบปฏิบัติการใหม่และติดตั้ง ระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด รวมทั้งทำการกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุดหรือตามความเหมาะสม	- ผู้อำนวยการกอง สำนัก หรือผู้ดูแลระบบของกรม ที่ได้รับมอบหมาย หรือ - ศูนย์บริหารข้อมูลการกงสุลและสารสนเทศ และ - ผู้สนับสนุนและให้บริการของกรม
กรณีที่ ๔ เกิดความเสียหายขึ้นกับ Hardware	ให้บริษัทผู้ดูแลทำการแก้ไขเบื้องต้นให้ Hardware สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับ OS และระบบงาน จะทำการติดตั้ง ระบบปฏิบัติการใหม่และติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมทั้ง ทำการกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุดหรือตามความเหมาะสม	- ผู้อำนวยการกอง สำนัก หรือผู้ดูแลระบบของกรม ที่ได้รับมอบหมาย หรือ - ศูนย์บริหารข้อมูลการกงสุลและสารสนเทศ และ - ผู้สนับสนุนและให้บริการของกรม

****

ส่วนที่ ๑๐ แนวปฏิบัติการตรวจสอบและการประเมินความเสี่ยงด้านสารสนเทศ

๑๐.๑ วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคง ปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๑๐.๒ แนวทางปฏิบัติ

(๑) หน่วยงานจะต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกอย่างน้อยปีละ ๑ ครั้ง

(๒) ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานเพื่อการประเมินความเสียงนั้น ๆ

(๓) กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยง

(๔) ติดตามการดำเนินการตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานที่ได้กำหนดไว้

(๕) ทบทวนและปรับปรุงแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานในด้านต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง ให้สอดคล้องกับสถานการณ์

****

ส่วนที่ ๑๑ การกำหนดหน้าที่ความรับผิดชอบ

๑๑.๑ วัตถุประสงค์

เพื่อเป็นการกำหนดหน้าที่ความรับผิดชอบ มีวัตถุประสงค์เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งมีแนวทางปฏิบัติต้องกำหนดบุคลากรที่ปฏิบัติหน้าที่ที่รับผิดชอบ ในส่วนนโยบายและผู้ปฏิบัติงานระบบสารสนเทศ โดยกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบสารสนเทศ รายละเอียดดังนี้

๑๑.๒ ระดับนโยบาย

อธิบดีกรมการกงสุล ในฐานะผู้บริหารระดับสูงสุดของกรม (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศหรือข้อมูลสารสนเทศของกรมหรือสำนักงานในต่างประเทศ

รองอธิบดีกรมการกงสุล ที่ได้รับมอบหมายในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ติดตาม กำกับ ควบคุม ดูแล ตรวจสอบ รวมทั้งให้ข้อเสนอแนะและให้คำปรึกษาแก่ผู้ใช้งาน

๑๑.๓ ระดับปฏิบัติ

เจ้าหน้าที่กรมหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา มีหน้าที่รับผิดชอบ ดังนี้

(๑) รับผิดชอบในการทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย บริหารจัดการ และบำรุงรักษาระบบฐานข้อมูล ระบบสารสนเทศและระบบการเชื่อมโยงข้อมูลการตรวจลงตรา ตรวจสอบการกำหนดสิทธิในการใช้งานระบบฐานข้อมูล ระบบสารสนเทศ

(๓) รับผิดชอบในการศึกษา วิเคราะห์ ออกแบบ พัฒนา ปรับปรุง ควบคุมและบำรุงรักษาระบบสารสนเทศที่สนับสนุนการการตรวจลงตรา และการปฏิบัติของเจ้าหน้าที่กรม

(๔) รับผิดชอบในการศึกษา วิเคราะห์ และจัดทำแผนในการพัฒนา ปรับปรุง บำรุงรักษา และจัดทำแผนในการนำเทคโนโลยีสารสนเทศ นำเสนอข้อมูลการดำเนินงานผ่านระบบสารสนเทศ เพื่อส่งเสริมให้บริการการตรวจลงตราเป็นไปอย่างมีประสิทธิภาพ

(๕) รับผิดชอบในการประเมินความเสี่ยง การควบคุมภายใน การรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ การจัดทำความตกลงและกำหนดมาตรฐานการเชื่อมโยง ข้อมูลกับหน่วยงานภายนอก การดำเนินงานแผนการฝึกอบรมบุคลากรของกรมหรือสำนักงานในต่างประเทศ

(๖) รับผิดชอบในการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอย่างน้อยปีละ ๑ ครั้ง

****