คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่าง ต่อเนื่อง ส่งเสริมการดำเนินงานอันเกี่ยวข้องกับกิจการของกรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร ในขณะเดียวกันลดความเสียงทางอิเล็กทรอนิกส์ อันเกิดมาจากการดำเนินการใด ๆ ด้วย วิธีการทางอิเล็กทรอนิกส์ ซึ่งอาจก่อให้เกิดความเสียหายหน่วยงานจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร พ.ศ.๒๕๖๐ โดยให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ และสอดคล้องตามพระราชกฤษฎีกาและประกาศ ฯ ดังกล่าวข้างต้น เพื่อให้เจ้าหน้าที่และผู้ที่เกี่ยวข้องรับทราบและนำไปปฏิบัติต่อไป

สารบัญ

เรื่อง **หน้า**

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร พ.ศ. ๒๕๖๐

หลักการและเหตุผล

โดยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ ดังนั้น กรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร จึงได้จัดทำนโยบายและแนว ปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องนำไปปฏิบัติอย่าง เคร่งครัด

วัตถุประสงค์

๑. เพื่อให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒. เพื่อกำหนดมาตรฐาน ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมการอุตสาหกรรมทหาร ในการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

๓. เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติ ให้มีระบบสำรองสามารถทำงานได้อย่างต่อเนื่องและ สามารถกู้ระบบคืนมาได้ภายในระยะเวลาที่เหมาะสม

๔. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่าสม่ำเสมอ

๕. เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจและการให้การอบรมด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๖. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมการอุตสาหกรรมทหาร ได้รับทราบและเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด เพื่อให้การดำเนินการที่เกี่ยวข้องเป็นไปโดยเรียบร้อย ต่อเนื่อง ปลอดภัย และเชื่อถือได้

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหารจัดทำขึ้นเพื่อกำหนดวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งออกเป็นส่วน ๆ ดังต่อไปนี้

ส่วนที่ ๑ แนวปฏิบัติการควบคุมการเข้าออกห้องศูนย์ปฏิบัติการและเครือข่าย

ส่วนที่ ๒ แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๓ แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

ส่วนที่ ๔ แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ ๕ แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ส่วนที่ ๖ แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน

ส่วนที่ ๗ แนวปฏิบัติการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ ๘ แนวปฏิบัติการจัดทำระบบการสำรองและการกู้คืนข้อมูล

ส่วนที่ ๙ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

ส่วนที่ ๑๐ แนวปฏิบัติความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต

ส่วนที่ ๑๑ แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

ส่วนที่ ๑๒ แนวปฏิบัติการฝึกอบรม

แนวปฏิบัติการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของกรมการอุตสาหกรรมทหารนี้ จัดเป็นมาตรฐานความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมการอุตสาหกรรมทหาร ฯ เจ้าหน้าที่ของกรมการอุตสาหกรรมทหาร ฯ และหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด ทั้งนี้ ต้องมีการทบทวนแนวนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อย ปีละ ๑ ครั้ง

คำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัตินี้ ประกอบด้วย

กรมการอุตสาหกรรมทหาร หมายถึง กรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมการอุตสาหกรรมทหารศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร

เจ้ากรมการอุตสาหกรรมทหาร หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของกรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร และมีอำนาจตัดสินใจเกี่ยวกับ ระบบเทคโนโลยีสารสนเทศภายในกรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร

หน่วยบริการเทคโนโลยีสารสนเทศ หมายถึง หน่วยงานระดับงานและ/หรือ ระดับฝ่ายหรือเทียบเท่าของกรมการอุตสาหกรรมทหาร ที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบชุดคำสั่งชุดคำสั่งโปรแกรม และเครือข่ายในกรมการอุตสาหกรรมทหาร

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของกรมการอุตสาหกรรมทหาร

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

วิธีการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของกรมการอุตสาหกรรมทหาร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาทตามทีกรมการอุตสาหกรรมทหารกำหนดไว้ ดังนี้

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของกรมการอุตสาหกรรมทหาร หรือผู้ที่ได้รับมอบหมาย

ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บริหารให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำและเจ้าหน้าที่ประจำโครงการของกรมการอุตสาหกรรมทหาร ฯ

ผู้ใช้งานทั่วไป หมายถึง ประชาชน หรือผู้รับบริการทั่วไปที่ไม่ใช่เจ้าหน้าที่ของกรมการอุตสาหกรรมทหาร

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับระบบสารสนเทศของกรมการอุตสาหกรรมทหาร

สินทรัพย์ (Asset) หมายถึง สินทรัพย์ด้านสารสนเทศ และระบบสารสนเทศของกรมการอุตสาหกรรมทหาร

สารสนเทศ หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจจะอยู่ในรูปแบบของข้อความ ตัวเลข หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธ ความรับผิด (Non - Repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือสภาพของเครือข่าย ที่แสดงให้เห็นว่าเป็นไปได้ที่จะมีการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือสภาพของมาตรการป้องกันที่ล้มเหลว และรวมถึงเหตุการณ์อันอาจเกี่ยวข้องกับความมั่นคงปลอดภัยด้วย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดซึ่งอาจทำให้ระบบสารสนเทศถูกบุกรุกหรือโจมตีและคุกคามความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ระบบคอมพิวเตอร์ หมายถึงอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของกรมการอุตสาหกรรมทหารได้ เช่น ระบบแลน (Lan) ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต(Internet)

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหารการสนับสนุนการให้บริการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบเช่น ระบบคอมพิวเตอร์ ระบบเครือข่ายโปรแกรมข้อมูลและสารสนเทศ เป็นต้น

ข้อมูลลับ หมายถึง สารสนเทศและระบบสารสนเทศที่มีความสำคัญซึ่งจำเป็นต้องได้รับการธำรงไว้ซึ่งความลับ (Confidentiality) ซึ่งหากข้อมูลดังกล่าวทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคลผู้ไม่มีหน้าที่เกี่ยวข้องได้รับทราบ จะทำให้เกิดความเสียหายต่อสำนักงาน และ/หรือบุคคลอื่น

ข้อมูลลับที่กำหนดชั้นความลับ (Confidential Data and Information) หมายถึง สารสนเทศและระบบสารสนเทศที่มีความสำคัญ และเป็นความลับในการดำเนินการของสำนักงานซึ่งหากถูกเปิดเผยออกไปอาจก่อให้เกิดความเสียหายหรือผลเสียอื่น ๆ โดย สำนักงานได้กำหนดชั้นความลับตามความสำคัญของเนื้อหาแหล่งที่มาของข้อมูล วิธีการนำไปใช้ประโยชน์ จำนวนบุคคลที่ต้องรับทราบ ผลกระทบและระดับความร้ายแรงหากมีการเปิดเผยหรือมีการรั่วไหลของข้อมูลนั้น หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติ โดยกำหนดชั้นความลับของสารสนเทศไว้ ๔ ระดับ คือ ลับที่สุด ลับมาก ลับ และใช้ภายใน

ลับที่สุด หมายถึง ความลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดผลเสียหายต่อสานักงาน และ/หรือเจ้าของข้อมูลที่เกี่ยวข้องอย่างร้ายแรงที่สุด และจาเป็นต้องมีการจากัดการเข้าถึงสารสนเทศแก่บุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น โดยจัดทารายชื่อผู้ได้รับอนุญาตให้เข้าถึงอย่างรอบคอบ

ลับมาก หมายถึง ความลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดผลเสียหายต่อสานักงาน และ/หรือเจ้าของข้อมูลที่เกี่ยวข้องอย่างร้ายแรง และจาเป็นต้องมีการจากัดการเข้าถึงสารสนเทศแก่บุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

ลับมาก หมายถึง ความลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดผลเสียหายต่อสานักงาน และ/หรือเจ้าของข้อมูลที่เกี่ยวข้อง และจาเป็นต้องมีการจากัดการเข้าถึงสารสนเทศแก่บุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

ใช้ภายใน หมายถึง ความลับซึ่งใช้ประโยชน์ภายในสานักงาน ฯ เท่านั้น ซึ่งจาเป็นต้องได้รับการป้องกันการเข้าถึงจากบุคคลภายนอก

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งออกเป็น

พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล
พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)
พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

เจ้าของข้อมูล หมายถึง ผู้ที่ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดการสูญหาย

จดหมายอิเล็กทรอนิกส์ (e-Mail) หมายถึง ระบบที่บุคคลใช้การรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายเชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถ

ส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนได้

รหัสผ่าน (Password) หมายถึง ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัว บุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิด ความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงกับคำสั่งที่กำหนดไว้

ส่วนที่ ๑
แนวปฏิบัติการควบคุมการเข้าออกห้องศูนย์ปฏิบัติการและเครือข่าย

<u>วัตถุประสงค์</u>

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้ งานหรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจต้องรักษาความลับโดย มาตรการนี้ จะมีผลบังคับใช้กับผู้ใช้งานที่มีส่วนเกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการอุตสาหกรรมทหาร โดยแนวปฏิบัตินี้ต้องมีการดาเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้งต่อปี

<u>ผู้รับผิดชอบ</u>

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

<u>แนวปฏิบัติการควบคุมการเข้าออกห้องศูนย์ปฏิบัติการและเครือข่าย</u>

ภายในกรมการอุตสาหกรรมทหารมีการจำแนกและกำหนดพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่ายอุปกรณ์เครือข่าย ระบบเทคโนโลยีสารสนเทศต่าง ๆ เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ไม่ได้รับการอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้

๑. ให้ผู้ดูแลระบบกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งที่ใช้งานและประกาศให้รับทราบโดยทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกเป็นพื้นที่ทำงานทั่วไป(General Working Area) พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) เป็นต้น

๒. ให้ผู้ดูแลระบบกำหนดสิทธิ์ให้กับเจ้าหน้าที่ในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

๓. ให้หน่วยบริการเทคโนโลยีสารสนเทศกำหนดมาตรการการควบคุมการเข้า - ออกห้องศูนย์ปฏิบัติการเครือข่าย

๔. จัดทำทะเบียนผู้มีสิทธิเข้าออกพื้นที่ เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

๕. กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสารบันทึกการเข้าออกพื้นที่

๖. จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นประจำ และมีการปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารปีละ ๑ ครั้งเป็นอย่างน้อย

๗. บุคคลภายนอกที่เข้ามาติดต่อจะต้องขออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้องและต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๘. บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและ ความจำเป็นก่อนที่จะอนุญาต

ส่วนที่ ๒
แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสาหรับการควบคุมการเข้าถึงและการใช้งานสารสนเทศของกรมการอุตสาหกรรมทหาร ป้องกันการบุกรุกผ่านระบบเครือข่าย ป้องกันการเข้าถึงและควบคุมการใช้งานสารสนเทศและระบบสารสนเทศโดยไม่ได้รับอนุญาต โดยเจ้าหน้าที่หรือพนักงานโครงการ ผู้บริหารและผู้ที่เกี่ยวข้องทุกฝ่ายอย่างเหมาะสม หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศและระบบเครือข่าย รวมทั้งสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานสารสนเทศขององค์กรได้อย่างถูกต้อง

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๑.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานเท่านั้น

๑.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งต้องทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้เจ้าหน้าที่ผู้ใช้ระบบต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นของการใช้งาน

๑.๓ ผู้ดูแลระบบหรือผู้ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๑.๔ ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการอุตสาหกรรมทหาร ฯ และตรวจตราการละเมิดความปลอดภัยที่มีต่อข้อมูลสำคัญ

๑.๕ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๒. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๑ ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ซึ่งในการขออนุญาตเข้าระบบงานนั้นจะต้องมีการทำเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวและจัดเก็บไว้เป็นหลักฐาน

๒.๒ ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำ เท่านั้น

๒.๓ เจ้าหน้าที่ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๔ เจ้าหน้าที่ผู้ใช้งานต้องไม่ดาวน์โหลดหรือติดตั้งโปรแกรม หรือผู้อื่นผู้ใดติดตั้งโปรแกรมที่ไม่ถูกต้องตามลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของหน่วยงาน หากฝ่าฝืนกรมการอุตสาหกรรมทหาร ฯ จะถือเป็นความรับผิดชอบของผู้ใช้งานเครื่องคอมพิวเตอร์เครื่องนั้น

๒.๕ เจ้าหน้าที่ใช้งานต้องไม่นำทรัพย์สินของทางราชการไปใช้ในทางเสื่อมเสีย ผิดกฎหมาย หรือทำให้ผู้อื่นได้รับความเดือดร้อน

๒.๖ เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์ชนิดพกพา ก่อนการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์ ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนการเข้าถึง

๒.๗ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๒.๘ เจ้าหน้าที่ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเคร่งครัด

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน

๓.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ของกรมการอุตสาหกรรมทหาร ฯ ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน ได้แก่ เมื่อลาออกต้องไปทำการยกเลิกภายใน ๒๔ ชั่วโมงหรือเมื่อเปลี่ยนตำแหน่งภายในต้องทำภายใน ๒ วัน

๓.๒ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๓ เจ้าหน้าที่ผู้ใช้ต้องลงนามรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๓.๔ การบริหารจัดการบัญชีรายชื่อ และรหัสผ่านของเจ้าหน้าที่

๓.๔.๑ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ความรับผิดชอบ

๓.๔.๒ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับเจ้าหน้าที่ผู้ใช้งาน หมายถึง เจ้าหน้าที่ผู้ใช้งานที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้สิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ในการพิจารณา

- ต้องได้รับความเห็นชอบจากผู้บริหาร หรือผู้ดูแลระบบงานนั้นๆ
- ต้องควบคุมการใช้งานอย่างเข้มงวด ได้แก่ กำหนดให้ใช้งานได้เฉพาะกรณีที่จำเป็นเท่านั้น
- ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

- ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด ได้แก่ ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน และจะต้องกำหนดให้มีการเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๓.๔.๓ การบริหารการเข้าถึงข้อมูลลับที่กำหนดชั้นความลับ แบ่งออกเป็นดังนี้

(๑) ข้อมูลลับรูปแบบเอกสารตีพิมพ์ ให้ปฏิบัติดังนี้

ลับที่สุด	**ลับมาก**	**ลับ**	**ใช้ภายใน**
การระบุชั้นความลับของสารสนเทศ			
ระบุคำว่า **"ลับที่สุด"** และ ชื่อผู้เป็นเจ้าของข้อมูลทุกหน้าเอกสารสำหรับเอกสารแยกแผ่นและระบุ บนปก หรือหน้าแรกของ เอกสาร หากเอกสารได้รับ การเข้าเล่ม	ระบุคำว่า **"ลับมาก"** และ ชื่อผู้เป็นเจ้าของข้อมูลทุกหน้าเอกสารสำหรับเอกสารแยกแผ่น และระบุบนปก หรือหน้าแรกของเอกสาร หากเอกสารได้รับการเข้าเล่ม	ระบุคำว่า **"ลับ"** และ ชื่อผู้เป็นเจ้าของข้อมูลทุกหน้าเอกสารสำหรับเอกสารแยกแผ่น และระบุบนปก หรือหน้าแรกของเอกสาร หากเอกสารได้รับการเข้าเล่ม	ระบุคำว่า**"เอกสารปกปิด"**สำหรับเผยเท่านั้น"
การเข้าถึงเอกสาร			
บุคคลทีมีหน้าทีเกียวข้องตามรายชือผู้ได้รับอนุญาต ให้เข้าถึงสารสนเทศ	บุคคลทีมีหน้าทีเกียวข้องและได้รับอนุญาตจากผู้บังคับบัญชา ตั้งแต่ระดับผู้อำนวยการฝ่ายขึ้นไปที่เป็นเจ้าของข้อมูล	บุคคลทีมีหน้าทีเกียวข้องและเป็นไปตามหลักการ Need – to - Know	ใช้งานได้ภายในศูนย์ข้อมูลสำนักงาน หรือภายในฝ่ายงานที่เป็นเจ้าของข้อมูลเท่านั้น
การเก็บรักษาเอกสาร			
เก็บรักษาในตู้เอกสารที่ ปิดล็อคเมื่อไม่ได้ใช้งาน	เก็บรักษาในตู้เอกสารที่ ปิดล็อคเมื่อไม่ได้ใช้งาน	เก็บรักษาในตู้เอกสารที่ปิดล็อคเมื่อไม่ได้ใช้งาน	เอกสารต้นฉบับต้องได้รับ การเก็บรักษาอย่างดีไม่ให้ เกิดความเสียหาย
การทำเนาเอกสาร			
ต้องขออนุญาตจากเจ้าของข้อมูลก่อนเสมอและสำเนาต้องได้รับการระบุชือผู้ทีได้รับอนุญาตให้ใช้งาน	ต้องขออนุญาตจากเจ้าของข้อมูลก่อนเสมอและสำเนาต้องได้รับการ ระบุชื่อผู้ที่ได้รับอนุญาตให้ ใช้งาน	ต้องขออนุญาตจากเจ้าของข้อมูลก่อนเสมอและสำเนาต้องได้รับการระบุชือผู้ทีได้รับอนุญาตให้ใช้งาน	อนุญาตให้ทำสำเนาได้ เพือใช้ในการปฏิบัติงาน เท่านั้น
การส่งเอกสารภายในสำนักงาน			
สอดในซองปิดผนึกและระบุคำว่า **"ลับที่สุด"**และ ชื่อ-ที่อยู่ผู้รับ บนหน้าซอง	สอดในซองปิดผนึกและระบุคำว่า **"ลับมาก"**และ ชื่อ-ที่อยู่ผู้รับ บนหน้าซอง	สอดในซองปิดผนึกแลระบุคำว่า **"ลับ"** และ ชื่อ-ทีอยู่ผู้รับบนหน้าซอง	มีปกเอกสารเพือปกปิด ข้อมูลอย่างมิดชิด
การส่งเอกสารภายนอก สำนักงาน			

สอดในซอง ๒ ชั้น ปิดผนึก ชั้นนอกและชั้นในด้วยวัสดุ ที่ป้องกันการลักลอบเปิดอ่านได้ ซองชั้นในระบุคำว่า **“ลับที่สุด”** และใช้บริการไปรษณีย์ ลงทะเบียนหรือบริษัทขนส่งที เชือถือได้ระบุชื่อ - ที่อยู่ของผู้รับ และผู้ส่ง	สอดในซอง ๒ ชั้น ปิดผนึก ชั้นนอกและชั้นในด้วยวัสดุที่ ป้องกันการลักลอบเปิดอ่าน ได้ซองชั้นในระบุคำว่า“**ลับมาก**”และใช้บริการ ไปรษณีย์ลงทะเบียนหรือ บริษัทขนส่งทีเชือถือได้ระบุ ชื่อ - ที่อยู่ของผู้รับ และผู้ส่ง	สอดในซอง ๒ ชั้น ปิดผนึก ชั้นนอกและชั้นในด้วยวัสดุ ที่ป้องกันการลักลอบเปิด อ่านได้ซองชั้นในระบุคำ ว่า“**ลับ**”และใช้บริการ ไปรษณีย์ลงทะเบียน หรือ บริษัทขนส่งทีเชือถือได้ ระบุชื่อ - ที่อยู่ของผู้รับ และผู้ส่ง	สอดซองปิดผนึก และ ระบุชื่อ - ทีอยู่ของผู้รับ และผู้ส่ง และใช้บริการ ไปรษณีย์ลงทะเบียน หรือบริษัทขนส่งที่ เชื่อถือได้
การส่งโทรสาร			
ตรวจสอบหมายเลขปลายทางให้ ถูกต้องโทรศัพท์แจ้งให้ผู้รับทราบ ถึงการส่งเอกสารและขอให้ผู้รับ แจ้งยืนยัน เมื่อได้รับเอกสารแล้ว รอรับเอกสาร ที่เครื่องโทรสารทุก ครั้ง	ตรวจสอบหมายเลขปลายทาง ให้ถูกต้องโทรศัพท์แจ้งให้ผู้รับ ทราบถึงการส่งเอกสารและ ขอให้ผู้รับแจ้งยืนยันเมื่อได้รับ เอกสารแล้วรอรับเอกสารที่ เครื่องโทรสารทุกครั้ง	ตรวจสอบหมายเลข ปลายทางให้ถูกต้อง โทรศัพท์แจ้งให้ผู้รับทราบ ถึงการส่งเอกสารและขอให้ ผู้รับแจ้งยืนยันเมื่อได้รับ เอกสารแล้วรอรับเอกสาร ที่เครื่องโทรสารทุกครั้ง	ตรวจสอบหมายเลข ปลายทางให้ถูกต้อง โทรศัพท์แจ้งให้ผู้รับ ทราบถึงการส่งเอกสาร และขอให้ผู้รับแจ้ง ยืนยันเมื่อได้รับเอกสาร แล้วรอรับเอกสารที่ เครื่องโทรสารทุกครั้ง
การทำลายเอกสาร			
ใช้เครื่องทำลายเอกสาร	ใช้เครื่องทำลายเอกสาร	ใช้เครื่องทำลายเอกสาร	ใช้เครื่องทำลายเอกสาร
การนำกระดาษกลับมาใช้ซ้ำ			
ห้ามนำกระดาษกลับมาใช้ซ้ำ	ห้ามนำกระดาษกลับมาใช้ซ้ำ	ห้ามนำกระดาษกลับมา ใช้ซ้ำ	สามารถนำกระดาษ กลับมาใช้ซ้ำได้ โดยให้ ใช้เฉพาะเอกสารทีใช้ ภายใน *** เท่านั้น

(๒) ข้อมูลลับในรูปแบบอิเล็กทรอนิกส์ ให้ปฏิบัติดังนี้

ลับที่สุด	**ลับมาก**	**ลับ**	**ใช้ภายใน**
การระบุชั้นความลับของข้อมูลบนจอแสดงผล			
ต้องระบุคำว่า **“ลับที่สุด”** บนหน้าจอ และระบุชือผู้ เป็นเจ้าของข้อมูล	ต้องระบุคำว่า **“ลับมาก”** บนหน้าจอ และระบุชือผู้ เป็นเจ้าของข้อมูล	ต้องระบุคำว่า **“ลับ”** บนหน้าจอ	ไม่จำเป็นต้องระบุ
การเข้าถึงและการทำสำเนาสารสนเทศ			
บุคคลทีมีหน้าทีเกียวข้อง ตามรายชื่อผู้ได้รับอนุญาต	บุคคลทีมีหน้าทีเกียวข้อง และได้รับอนุญาตจาก	บุคคลที่มีหน้าที่เกี่ยวข้อง และเป็นไปตามหลักการ	ใช้งานได้ภายในศูนย์ ข้อมูล สำนักงาน หรือ

ให้เข้าถึงข้อมูล	ผู้บังคับบัญชา ตั้งแต่ระดับผู้อำนวยการฝ่ายขึ้นไปที่เป็นเจ้าของข้อมูล	Need – to - know	ภายในฝ่ายงานที่เป็นเจ้าของข้อมูลเท่านั้น
การเก็บรักษาบนสื่อที่ไม่สามารถเคลื่อนย้ายได้ (ที่ได้ควบคุมการเข้าถึง)			
ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล
การเก็บรักษาบนสื่อที่ไม่สามารถเคลื่อนย้ายได้ (ที่ไม่ได้ควบคุมการเข้าถึง)			
เข้ารหัสข้อมูล	เข้ารหัสข้อมูล	เข้ารหัสข้อมูล	เข้ารหัสข้อมูล
การสั่งพิมพ์สารสนเทศ			
ต้องมีผู้รอรับเอกสาร ที่เครื่องทุกครั้ง	ต้องมีผู้รอรับเอกสาร ที่เครื่องทุกครั้ง	ต้องมีผู้รอรับเอกสาร ที่เครื่องทุกครั้ง	มีผู้รอรับเอกสาร ที่เครื่องทุกครั้ง
การส่งสารสนเทศผ่านเครือข่ายสาธารณะ			
ต้องเข้ารหัสข้อมูล	ต้องเข้ารหัสข้อมูล	ต้องเข้ารหัสข้อมูล	ต้องเข้ารหัสข้อมูล
การทำลายสารสนเทศ			
ต้องทำลายด้วยวิธี Secure Delete	ต้องทำลายด้วยวิธี Secure Delete	ต้องทำลายด้วยวิธี Secure Delete	ลบไฟล์ด้วยวิธีปกติ โดยการกดแป้น Delete หรือ Shift + Delete
การทำลายสื่อบันทึกข้อมูล			
เจ้าของข้อมูลต้องเลือกใช้วิธีทำลายที่มั่นใจว่าสื่อบันทึกข้อมูลถูกทำลายจนไม่สามารถกู้ข้อมูลกลับคืนมาได้ ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม	เจ้าของข้อมูลต้องเลือกใช้วิธีทำลายที่มั่นใจว่าสื่อบันทึกข้อมูลถูกทำลายจนไม่สามารถกู้ข้อมูลกลับคืนมาได้ ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม	เจ้าของข้อมูลต้องเลือกใช้วิธีทำลายที่มั่นใจว่าสื่อบันทึกข้อมูลถูกทำลายจนไม่สามารถกู้ข้อมูลกลับคืนมาได้ ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม	ทำลายด้วยวิธีปกติ โดยการกดแป้น Delete หรือ Shift + Delete

(๓) ข้อมูลลับที่ส่งผ่านทางวาจา ให้ปฏิบัติตามดังนี้

ลับที่สุด	ลับมาก	ลับ	ใช้ภายใน
การเข้าถึงสารสนเทศ			
บุคคลทีมีหน้าทีเกียวข้องตามรายชือผู้ได้รับอนุญาตให้เข้าถึงข้อมูล	บุคคลทีมีหน้าทีเกียวข้องและได้รับอนุญาตจากผู้บังคับบัญชา ตั้งแต่ระดับผู้อำนวยการฝ่ายขึ้นไปที่เป็นเจ้าของข้อมูล	บุคคลที่มีหน้าที่เกี่ยวข้องและเป็นไปตามหลักการ Need – to - know	ใช้งานได้ภายในศูนย์ข้อมูลสำนักงาน หรือภายในฝ่ายงานที่เป็นเจ้าของข้อมูลเท่านั้น
การสนทนาทางโทรศัพท์			

ตรวจสอบคู่สนทนาทางโทรศัพท์ทุกครั้ง ว่าเป็นผู้ที่ต้องการสนทนาด้วย	ตรวจสอบคู่สนทนาทางโทรศัพท์ทุกครั้ง ว่าเป็นผู้ ที่ต้องการสนทนาด้วย	ตรวจสอบคู่สนทนาทางโทรศัพท์ทุกครั้ง ว่าเป็นผู้ ที่ต้องการสนทนาด้วย	ตรวจสอบคู่สนทนาทางโทรศัพท์ทุกครั้ง ว่าเป็นผู้ ที่ต้องการสนทนาด้วย
การฝากข้อความทางโทรศัพท์			
ห้ามฝากข้อความที่มีเนื้อหาข้อมูลไว้ในเครื่องตอบรับอัตโนมัติหรือระบบวอยซ์เมล์	ห้ามฝากข้อความที่มีเนื้อหาข้อมูลไว้ในหรือระบบวอยซ์เมล์	ห้ามฝากข้อความที่มีเนื้อหาข้อมูลไว้ในหรือระบบวอยซ์เมล์	หลีกเลี่ยงการฝากข้อความที่มีเนื้อหาข้อมูลไว้ในเครื่องตอบรับอัตโนมัติหรือระบบวอยซ์เมล์

๔. การบริหารจัดการการเข้าถึงระบบเครือข่าย

๔.๑ ผู้ดูแลระบบต้องออกแบบและแบ่งแยกระบบเครือข่าย ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ เพื่อให้การควบคุมเป็นระบบและป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

๔.๒ ผู้ดูแลระบบต้องจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้ใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๔.๓ ผู้ดูแลระบบต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งาน

๔.๔ ผู้ดูแลระบบต้องจำกัดเส้นทางบนเครือข่าย จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้งานใช้เส้นทางอื่น ๆ ได้ และกำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบ

๕. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๕.๑ ต้องกำหนดบุคคลที่รับผิดชอบการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบอย่างชัดเจน

๕.๒ ต้องเปิดใช้บริการเท่าที่จาเป็นเท่านั้น เช่น Telnet FTP หรือ Ping เป็นต้น หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

๕.๓ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย ต้องจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มระบบเครือข่ายและคอมพิวเตอร์ของกรมการอุตสาหกรรมทหาร ฯ

๖. การบริหารจัดการการบันทึกและตรวจสอบ

๖.๑ ต้องกำหนดให้มีการบันทึกการทางานของระบบคอมพิวเตอร์ บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Log) และเก็บไว้อย่างน้อย 3 เดือน

๖.๒ ต้องมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๗. การพิสูจน์ตัวตนสำหรับผู้ใช้งาน

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของกรมการอุตสาหกรรมทหาร ฯ ดังนี้

๗.๑ แสดงชื่อผู้ใช้งาน (Username)

๗.๒ ใส่รหัสผ่าน (Password)

ส่วนที่ ๓
แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทาให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมการอุตสาหกรรมทหาร

<u>ผู้รับผิดชอบ</u>

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

<u>แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการเครือข่าย</u>

๑. การใช้งานบริการเครือข่าย

๑.๑ ห้ามเจ้าหน้าที่ผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่ขัดต่อกฎหมาย หรือศีลธรรมอันดีต่อสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกความรับผิดชอบของกรมการอุตสาหกรรมทหาร ฯ

๑.๒ ไม่อนุญาตให้เจ้าหน้าที่ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหากำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเตอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๑.๓ เจ้าหน้าที่ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น คือผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขข้อมูลใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก(Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น เจ้าหน้าที่ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว กรมการอุตสาหกรรมทหาร ฯ ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๑.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยามรุกล้าเขตหวงห้ามของทางราชการ

๑.๕ ผู้ใช้งานต้องใช้งานระบบเครือข่ายทั้งแบบมีสายและไร้สายของกรมการอุตสาหกรรมทหาร ฯ ภายใต้วัตถุประสงค์เพื่อการปฏิบัติงานและสนับสนุนการดำเนินงานของกรมการอุตสาหกรรมทหาร ฯ เท่านั้น

๑.๖ ห้ามมิให้เจ้าหน้าที่ผู้ใช้งานทำการแก้ไขเปลี่ยนแปลงการตั้งค่าพารามิเตอร์ต่างๆ เช่น Computer Name, System Configuration และ Program Configuration เว้นแต่ผู้มีหน้าที่ดูแลระบบเครือข่ายคอมพิวเตอร์

๑.๗ เจ้าหน้าที่ผู้ใช้งานทั้งที่อยู่ภายในและภายนอกกรมการอุตสาหกรรมทหาร ฯ ต้องทำการยืนยันตัวบุคคลผ่าน User Account ที่ได้รับซึ่งประกอบด้วย Username และ Password

๑.๘ บัญชีผู้ใช้งาน (User Account) เป็นเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายสิทธินี้ให้กับผู้อื่นไม่ได้

๑.๙ บัญชีผู้ใช้งาน (User Account) ที่กรมการอุตสาหกรรมทหารให้กับเจ้าหน้าที่ผู้ใช้งานนั้น เจ้าหน้าที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆอันอาจจะเกิดขึ้น รวมทั้งผลเสียหายต่างๆที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดการกระทำของผู้อื่น

๑.๑๐ เจ้าหน้าที่ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศผ่านทางเครือข่ายได้เพียงบริการที่ได้รับอนุญาตให้เข้าเท่านั้น โดยแบ่งเป็นสิทธิของผู้ใช้งาน สิทธิของผู้ดูแลระบบ และแบ่งสิทธิตามการใช้งานภายใน/ภายนอกระบบเครือข่าย

คอมพิวเตอร์ นอกจากนี้ให้ดำเนินการควบคุมการเชื่อมต่อกับอุปกรณ์ระบบเครือข่ายที่ไม่มีหน้าที่เกี่ยวข้อง ได้แก่ การป้องกันการนำอุปกรณ์กระจายสัญญาณไร้สายมาเชื่อมต่อเข้ากับระบบเครือข่ายคอมพิวเตอร์โดนพลการ รวมทั้งดำเนินการและมีการเก็บบันทึกการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ที่แสดงหมายเลขไอพีแอดเดรสทั้งเครื่องคอมพิวเตอร์ต้นทางและปลายทาง นอกจากนี้ให้มีการควบคุมและบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่ายทั้งโดยผู้ดูแลระบบและผู้ให้บริการภายนอก โดนหากเป็นผู้ให้บริการภายนอก ที่จะมาให้บริการที่ห้องเครื่องคอมพิวเตอร์แม่ข่ายต้องแจ้งรายละเอียดและนัดหมายกับกรมการอุตสาหกรรมทหาร ฯ ล่วงหน้า เมื่อมาถึงต้องแลกบัตรประจำตัวประชาชนหรือใบขับขี่เพื่อให้ได้รับบัตรอนุญาตเข้าพื้นที่ชั่วคราว และแจ้งให้ผู้ดูแลระบบนำพาไปลงบันทึกการเข้าปฏิบัติงานในห้องคอมพิวเตอร์แม่ข่าย ชี้แจงการนำอุปกรณ์หรือวัสดุใด ๆ เข้าออก และให้ผู้ดูแลระบบควบคุมการปฏิบัติของผู้ให้บริการ

๑.๑๑ หลังการใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น เจ้าหน้าที่ผู้ใช้งานต้องไม่เข้าเว็บลามก อนาจาร หรือเว็บในลักษณะเดียวกัน และ/หรือ ไม่ส่งรูปภาพลามกอนาจารผ่านระบบเครือข่ายของกรมการอุตสาหกรรมทหาร ฯ เป็นอันขาด

๑.๑๒. เจ้าหน้าที่ผู้ใช้งานที่ต้องการยืมวัสดุอุปกรณ์ต่าง ๆ ไปใช้งานภายนอกหน่วยงานหรือไปใช้งานต่างหน่วยงาน ต้องเป็นข้าราชการของกรมการอุตสาหกรรมทหาร ฯ เท่านั้น โดยต้องทำเอกสารหลักฐานแสดงการยืมวัสดุอุปกรณ์หรือครุภัณฑ์คอมพิวเตอร์ในเอกสารหลักฐานต้องประกอบด้วย ชื่อสกุล หน่วยงานที่สังกัด ระยะเวลาการยืม - คืน รายการอุปกรณ์ จำนวนอุปกรณ์ เป็นอย่างน้อย ทั้งนี้ ผู้มีอำนาจในการให้ยืมต้องอยู่ในระดับผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรมหาร กรมการอุตสาหกรรมทหาร ฯ เท่านั้น โดยความเสียหายต่อทรัพย์สินต่าง ๆ ที่ยืมไป ผู้ใช้บริการและหน่วยงานที่ยืมต้องเป็นผู้รับผิดชอบต่อค่าเสียหายที่เกิดขึ้น

๒. การบริหารความมั่นคงของระบบเครือข่าย

๒.๑ จัดให้มีอุปกรณ์รักษาความมั่นคงปลอดภัยทางเครือข่าย ได้แก่ Firewall, Proxy, IPS ฯลฯ และตั้งค่าอุปกรณ์ดังกล่าวด้วย ACL (Access Control List), Firewall Rules เพื่อควบคุมการเชื่อมต่อ เข้าถึง หรือกำหนดเส้นทางของระบบเครือข่ายตามความเหมาะสม

๒.๒ จัดเก็บ Log ของระบบเครือข่าย รวมถึง Security Log ที่จำเป็นตามที่กำหนด โดยกฎหมายและความต้องการด้านการบริหารความมั่นคงของสานักงาน

๒.๓ ผู้ดูแลระบบต้องเฝ้าติดตามตรวจสอบ สถานะของระบบเครือข่าย การใช้งานบริการระบบเครือข่าย และ Security Log ที่เกี่ยวข้อง รวมถึงการเฝ้าระวังความผิดปกติต่าง ๆ ได้แก่ การพยายามบุกรุกเข้าระบบ การปฏิเสธการให้บริการ หรือการทำให้ประสิทธิภาพในการทำงานของระบบสารสนเทศลดลง

๒.๔ การเข้าถึงระบบบริหารจัดการระบบเครือข่าย ต้องผ่านช่องทางโปรโตคอล ซึ่งในระบบ Internet จะใช้ภาษาสื่อสารมาตรฐานที่ชื่อว่า TCP/IP เป็นภาษาหลัก

๒.๕ ใช้กระบวนการพิสูจน์ตัวตน (Authentication) และการกำหนดขอบเขตความรับผิดชอบในการบริหารจัดการอุปกรณ์ระบบเครือข่าย

๒.๖ สำรองข้อมูลค่าการปรับแต่ง (Configuration) ของอุปกรณ์ระบบเครือข่าย อย่างสม่ำเสมอ หรือทุกครั้งที่มีการเปลี่ยนแปลง

๒.๗ การติดตั้งระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสม เพื่อรักษาความมั่นคงให้แก่สารสนเทศ และระบบสารสนเทศของกรมการอุตสาหกรรมทหาร ประกอบด้วย

๒.๗.๑ ฮาร์ดแวร์ (Hardware) ที่เชื่อมต่อกับระบบเครือข่ายทั้งหมด ต้องได้รับการตั้งค่าสนับสนุนการบริหารจัดการ และการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย

๒.๗.๒ สายเคเบิ้ลของระบบเครือข่าย ต้องได้มาตรฐานสากล หรือมาตรฐานผลิตภัณฑ์อุตสาหกรรม (มอก.)

๒.๗.๓ ระบบป้องกันผู้บุกรุกจากภายนอก ต้องได้รับการตั้งค่าตามคำแนะนำของผู้ผลิต และ/หรือ หน่วยงานด้านความมั่นคงปลอดภัยต่าง ๆ ได้แก่ SANS Institute หรือ NSA

๒.๗.๔ Network Address ของระบบเครือข่ายต่าง ๆ ต้องได้รับการลงทะเบียน แจกจ่าย และบริหารจัดการ โดยผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมายให้รับผิดชอบ และต้องไม่ถูกเปิดเผยต่อระบบเครือข่ายภายนอก

๒.๗.๕ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

๒.๗.๕.๑ ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยการล๊อกอินเข้ามาใช้งาน

๒.๗.๕.๒ ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันไว้ในห้องคอมพิวเตอร์แม่ข่ายที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

๒.๗.๕.๓ ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

๒.๗.๕.๔ เปิดพอร์ตที่มีความจำเป็นในการใช้งาน และยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๒.๗.๕.๕ ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

๒.๗.๕.๖ กำหนดสิทธิบุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

๒.๗.๕.๗ บันทึกการเข้า - ออกพื้นที่บริเวณห้องคอมพิวเตอร์แม่ข่ายกลาง ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และ ผู้ดูแลระบบ เป็นต้น

๒.๗.๕.๘ ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้ผู้ดูแลระบบ เป็นผู้รับผิดชอบนำพาเข้าไป

๒.๗.๖ อุปกรณ์ของระบบเครือข่ายที่สำคัญของสำนักงาน ต้องใช้ระบบไฟฟ้าสำรอง (UPS) เสมอ

๒.๗.๗ อุปกรณ์ของระบบเครือข่ายที่สำคัญของสำนักงานต้องมีการจัดทำทะเบียน

๒.๗.๘ ห้ามติดตั้งอุปกรณ์ใดเข้ากับระบบเครือข่ายของสำนักงาน โดยไม่ได้รับอนุญาต

๒.๗.๙ ระบบเครือข่ายต้องได้รับการตั้งค่าให้สามารถป้องกันการเชื่อมต่อในลักษณะ (Bridge) ผ่านไปยังช่องทางการสื่อสารอื่น

๒.๗.๑๐ ทำการแบ่งแยกเครือข่าย (segregation in networks) สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

๒.๘ การใช้บริการระบบเครือข่ายภายนอก ต้องจัดทำเอกสารข้อตกลงของระดับ การบริการกับผู้ให้บริการ พร้อมติดตาม ตรวจสอบ และประเมินผลการให้บริการให้เป็นไปตามข้อตกลง

๒.๙ ให้หน่วยประสานงานเครือข่ายไร้สาย ซึ่งมอบหมายโดย เจ้ากรมการอุตสาหกรรมทหาร ฯ ให้เป็นผู้บริหารจัดการและให้บริการระบบเครือข่ายไร้สายของกรมการอุตสาหกรรมทหาร

๒.๑๐ การระบุอุปกรณ์บนเครือข่าย (equipments identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

๒.๑๐.๑ การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ หรือผู้ดูแลระบบก่อนจึงจะสามารถดำเนินการได้

๒.๑๐.๒ ผู้ดูแลระบบเครือข่ายมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ กำหนด และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

๒.๑๐.๓ จะต้องมีการจำกัดสิทธิการเข้าใช้อุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

๒.๑๐.๔ มีการจัดทำทะเบียนบัญชีอุปกรณ์ที่ใช้บนเครือข่าย

๒.๑๑ มีการควบคุมการเชื่อมโยงเครือข่าย (network connection control) ผู้ดูแลระบบต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมโยงระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติอย่างน้อย ดังนี้

๒.๑๑.๑ การจำกัดสิทธิ การเข้าถึงเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

๒.๑๑.๒ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๒.๑๑.๓ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๒.๑๑.๔ การเข้าใช้งานเชื่อมต่อเครือข่ายต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

๒.๑๑.๕ ควบคุมไม่ให้เปิดเผยข้อมูลระบบเครือข่ายที่สำคัญในการเชื่อมต่อเข้าสู่ระบบได้แก่ หมายเลข IP Address Username และ Password เป็นต้น

๒.๑๑.๖ ผู้ใช้งานห้ามนำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

๒.๑๒ มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย ดังนี้

๒.๑๒.๑ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) ของหน่วยงาน

๒.๑๒.๒ กำหนดให้มีการแปลงหมายเลขเครือข่ายย่อย

๒.๑๒.๓ กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย หรือจำกัดสิทธิในการใช้บริการเครือข่ายของหน่วยงาน

๒.๑๒.๔ ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย ที่เชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบสารสนเทศที่มีการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ และควบคุมการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆได้

๓. ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่กรมการอุตสาหกรรมทหารมีแนวทางปฏิบัติดังนี้

๓.๑ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมบุคคลในการเข้าออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก ทะเบียนผู้มีสิทธิเข้าออกพื้นที่ เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๓.๒ สิทธิในการเข้าออกพื้นที่ต่างๆภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่ต้องเป็นเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

๓.๓ ต้องจัดทำระบบเก็บบันทึกการเข้าออกกรมการอุตสาหกรรมทหารตามกระบวนการที่ระบุไว้ในเอกสารบันทึกการเข้าออกพื้นที่

๓.๔ เจ้าหน้าที่ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก เป็นประจำทุกเดือน

ส่วนที่ ๔
แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

วัตถุประสงค์

เพื่อผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจ ตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมในการใช้งาน โดยแนวปฏิบัติต้องมีการดำเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้ง ต่อปี

ผู้รับผิดชอบ

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๑. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๑.๑ เจ้าหน้าที่ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๑.๒ เจ้าหน้าที่ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) ล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อเจ้าหน้าที่ต้องการใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๑.๓ ก่อนการเข้าใช้ระบบปฏิบัติการเจ้าหน้าที่ต้องใส่ User name และ Password ทุกครั้ง

๑.๔ เจ้าหน้าที่ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๑.๕ เจ้าหน้าที่ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๑.๖ การบริหารจัดการรหัสผ่าน (password management system) ต้องแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะเชิงโต้ตอบ (interactive) หรือต้องทำงานในลักษณะอัตโนมัติเพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๑.๖.๑ เปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้บริการลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๑.๖.๒ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายทางอิเล็กทรอนิกส์ ที่ไม่มีการป้องกันในการส่งรหัสผ่าน และเมื่อผู้ใช้บริการได้รับรหัสผ่านต้องตอบยืนยันการได้รับรหัสผ่าน

๑.๖.๓ กำหนดชื่อผู้ใช้บริการ และรหัสผ่าน ต้องไม่ซ้ำกัน

๑.๗ ต้องจำกัดการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความ มั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้ให้ดำเนินการดังนี้

๑.๗.๑ ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาตและยังไม่ผ่านการตรวจสอบ

๑.๗.๒ ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

๑.๗.๒ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๑.๗.๓ ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๑.๗.๔ กำหนดให้ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน

๒.๑ เจ้าหน้าที่ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อปองกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาดต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข เมื่อยืนยันผิดครบ ๓ ครั้ง ระบบจะทำการล็อค

๒.๒ เจ้าหน้าที่ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๓ เจ้าหน้าที่ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อผู้อื่นห้ามโอนจำหน่าย หรือแจกจ่ายให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๒.๔ เจ้าหน้าที่ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเองและทำการบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

ส่วนที่ ๕
แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศของกรมการอุตสาหกรรมทหารและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการท างานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบและติดตามพิสูจน์บุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการอุตสาหกรรมทหาร ฯ ได้อย่างถูกต้องโดยนโยบายแนวปฏิบัติต้องมีการดำเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้ง ต่อปี

ผู้รับผิดชอบ

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๑. แนวปฏิบัติการจำกัดการเข้าถึงระบบสารสนเทศ

๑.๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กร และต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๑.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเตอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๑.๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของ บุคลากรดังต่อไปนี้

๑.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อเจ้าหน้าที่ผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๑.๓.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย และต้องหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๑.๓.๓ กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๑.๓.๔ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๑.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๑.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับเจ้าหน้าที่ผู้ใช้งานที่มีสิทธิสูงสุด เจ้าหน้าที่ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้น ระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสเจ้าหน้าที่ผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๑.๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๑.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๑.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๑.๔.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว โดยมี Timeout

๑.๔.๔ การรับ - ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๑.๔.๕ ต้องกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๑.๔.๖ ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑.๕ ระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

๑.๕.๑ การแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษ จากผู้ดูแลระบบ ฯ ที่ได้รับมอบหมายจากผู้บริหาร โดยจะต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ ให้ทำงานอยู่บนเครื่องเซิร์ฟเวอร์ หรือคอมพิวเตอร์ไม่ใช้ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดตั้งห้องเครื่องคอมพิวเตอร์แม่ข่ายกลางที่มีสภาพแวดล้อมเหมาะสม

๑.๕.๒ ให้มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ห้องคอมพิวเตอร์แม่ข่ายกลาง ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่ายกลาง และอื่นๆ เป็นต้น เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

๑.๕.๓ ควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกกำหนดสิทธิการเข้าใช้งานโดยกำหนดค่าที่ Firewall

๑.๕.๔ มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๑.๖ ควบคุมผู้ใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

๑.๖.๑ ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ ได้แก่ ให้เจ้าหน้าที่บริษัทควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่บริษัทหลักทรัพย์ (onsite service) และให้เจ้าหน้าที่บริษัทตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ remote access และปิด modem ทันทีที่การให้บริการเสร็จสิ้น เป็นต้น

๑.๖.๒ ดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๑.๖.๓ กำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข

๑.๖.๔ มีขั้นตอนในการตรวจรับงานของผู้ให้บริการ

๒. แนวปฏิบัติการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๒.๑ ผู้ดูแลระบบต้องตั้งค่าของเครื่องคอมพิวเตอร์ที่ใช้ในกิจการของกรมการอุตสาหกรรมทหาร ฯ ซึ่งรวมถึงเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา เครื่องบริการ หรือเครื่องคอมพิวเตอร์ประเภทอื่นใด ดังนี้

๒.๑.๑ ให้ใช้รหัสผ่านบนระบบปฏิบัติการในการเข้าถึงทุกครั้ง

๒.๑.๒ ตั้งค่าเริ่มต้นให้เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา และอุปกรณ์สื่อสารพกพาใช้ Screen Saver ที่ต้องปลดล็อคด้วยรหัสผ่านอัตโนมัติ

๒.๑.๓ ตั้งค่าการยุติการใช้งาน สำหรับระบบสารสนเทศ (Session Timeout) เพื่อป้องกันการเข้าถึงสารสนเทศ เมื่อผู้ใช้งานว่างเว้นจากการใช้งาน เป็นระยะเวลา ๑๕ นาที

๒.๑.๔ จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ไว้ที่ ๓ ชั่วโมง สำหรับระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูง

๒.๑.๕ ผู้ดูแลระบบต้องให้เจ้าหน้าที่ผู้ใช้งานสามารถเข้าถึงได้ โดยผ่านช่องทางระบบเครือข่ายที่มีการเข้ารหัสลับเสมอ ได้แก่ สายสัญญาณระบบเครือข่ายที่มีการจัดเตรียมไว้ หรือ VPN หรือช่องทางสื่อสารอื่น ๆ ของกรมการอุตสาหกรรมทหาร ทีมีการเข้ารหัสลับข้อมูลในการสื่อสารเพื่อความมั่นคงปลอดภัยแล้ว ยกเว้นการให้บริการข้อมูลเว็บสาธารณะส่วนที่มีคนอ่านอย่างเดียว

๒.๑.๖ ผู้ดูแลระบบต้องปกป้องระบบสารสนเทศของสำนักงานด้วยความเอาใจใส่ ความระมัดระวังตามวิชาชีพของตน โดยการติดตั้งซอฟต์แวร์ Anti – Virus ซอฟต์แวร์ Anti – Spyware ซอฟต์แวร์ Anti – Malware ซอฟต์แวร์ Firewall ปรับปรุง Security Patch ของระบบปฏิบัติการคอมพิวเตอร์ ติดตั้งระบบ การป้องกัน และตรวจจับการบุกรุกลงบนเครื่องคอมพิวเตอร์

๓. แนวปฏิบัติการปฏิบัติงานจากภายนอกกรมการอุตสาหกรรมทหาร

๓.๑ ผู้ดูแลระบบต้องจัดการให้การเข้าถึงระบบเครือข่ายของกรมการอุตสาหกรรมทหารจากระยะไกลมีกลไกในการพิสูจน์ตัวตนผู้ใช้งานอย่างเหมาะสม โดยการตรวจสอบจาก หมายเลข IP Address เฉพาะที่กำหนดให้สามารถเข้าถึงได้เท่านั้น เพื่อให้ผู้ดูแลระบบสามารถตรวจจับการเข้าถึงที่ไม่ได้รับอนุญาตได้

๓.๒ ห้ามผู้ดูแลระบบอนุญาตให้บุคคลภายนอกพยายามล่วงละเมิดความมั่นคงปลอดภัยหรือรบกวนการทำงานของระบบเครือข่ายของสำนักงาน ได้แก่ การเข้าถึงสารสนเทศหรือเครื่องบริการ (Server) ที่ตนไม่ได้รับอนุญาตการทำ Sniffing, การทำPinged Floods, การทำPacket Spoofing, การโจมตีแบบ Denial of Service หรือการทำ Forged Routing Information เป็นต้น เว้นแต่เพื่อเป็นการปฏิบัติหน้าที่ในการค้นหาจุดบกพร่องของระบบสารสนเทศและได้รับอนุญาตจากผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม กรมการอุตสาหกรรมทหาร ฯ แล้ว

๓.๓ การเข้าถึงระบบเครือข่ายหรือระบบสารสนเทศภายในของสำนักงานด้วยการเชื่อมต่อกับระบบ เครือข่ายภายนอก ได้แก่ จากบ้าน จากโรงแรม จากอุปกรณ์ไร้สาย ฯลฯ ต้องถูกจำกัดให้ดำเนินการเฉพาะเท่าที่จำเป็นเท่านั้น และต้องได้รับการควบคุมดังนี้

๓.๓.๑ อนุญาตให้ทำการเข้าถึงระบบจากระยะไกลได้เฉพาะกับบริการที่มีความจำเป็นเท่านั้น

๓.๓.๒ ทำการเข้าถึงระบบจากระยะไกลเมื่อมีความจำเป็นเท่านั้น

๓.๓.๓ ผู้ใช้งานที่ได้รับอนุญาตเท่านั้นที่มีสิทธิดำเนินการเข้าถึงระบบจากระยะไกล

๓.๓.๔ การเข้าถึงระบบสำคัญ หรือระบบทีเกี่ยวข้องกับสารสนเทศสำคัญจากระยะไกลต้องการพิสูจน์ตัวตนผู้ใช้งานด้วยวิธีที่มีความมั่นคง

๓.๓.๕ ห้ามใช้บริการระบบเครือข่าย หรือ Protocol ที่ไม่มั่นคงปลอดภัย ในการเข้าถึงระบบสารสนเทศจากระยะไกล

๓.๓.๖ ห้ามทำการเชื่อมต่อเพื่อเข้าถึงระบบเครือข่ายภายในสำนักงาน จากระยะไกลด้วยเครื่องคอมพิวเตอร์สาธารณะ ได้แก่ เครื่องคอมพิวเตอร์ในร้านอินเทอร์เน็ต เครื่องคอมพิวเตอร์ที่ให้บริการฟรีในร้านอาหารเป็นต้น

๓.๓.๗ การเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในของสำนักงานด้วยวิธีการแบบ Phone - Line - Dial -Up ต้องดำเนินการผ่านโมเด็มพูของส่วนกลาง ที่ได้รับการตรวจสอบเท่านั้น

๓.๓.๘ ระบบทั้งหมดที่ผู้ใช้งานสามารถเข้าถึงจากระยะไกล ผ่านระบบเครือข่ายสาธารณะได้นั้น ต้องได้รับการกำหนดระยะเวลาการเข้าใช้งาน โดยระบบต้องตัดการเชื่อมต่อที่ไม่มีการใช้งานใด ๆ เป็นระยะเวลาติดต่อกันเกิน ๓๐ นาที และตัดการเชื่อมต่อใด ๆ ที่ใช้งานติดต่อกันเกิน ๖ ชั่วโมง ทั้งนี้ การเชื่อมต่อเข้าสู่ระบบภายในอีกครั้ง ต้องได้รับการพิสูจน์ตัวตนด้วยเสมอ

๓.๔ ผู้ใช้งานที่ปฏิบัติงานอยู่ภายนอกสำนักงาน มีขั้นตอนปฏิบัติดังนี้

๓.๔.๑ แสดงตนด้วยบัญชีผู้ใช้งานและรหัสผ่านที่เป็นมาตรฐานของสำนักงานก่อนการเข้าถึงระบบสารสนเทศของสำนักงานทุกครั้ง

๓.๔.๒ ใช้งานซอฟต์แวร์ (Software) ป้องกันไวรัสที่ได้รับการอัพเดทอยู่เสมอ

๓.๔.๓ ใช้งานซอฟต์แวร์ไฟร์วอลล์ส่วนบุคคล (Personal Firewall)

๓.๔.๔ ใช้งานซอฟต์แวร์หรืออุปกรณ์ ประเภท Virtual Private Networking หรือใช้เทคโนโลยีอื่น ๆ เพื่อปกป้องการเชื่อมต่อระหว่างสถานที่ปฏิบัติงานภายนอก และระบบเครือข่ายภายในของกรมการอุตสาหกรรมทหาร

๓.๔.๕ ต้องใช้ความระมัดระวังมากเป็นพิเศษ เพื่อปกป้องอุปกรณ์คอมพิวเตอร์พกพา รวมถึงสารสนเทศที่อยู่ในอุปกรณ์เหล่านั้น มิให้ถูกล่วงละเมิดโดยบุคคลที่ไม่ได้รับอนุญาต ซึ่งรวมถึงสมาชิกในครอบครัวของผู้บริหาร ผู้ดูแลระบบ และเจ้าหน้าที่

ส่วนที่ ๖
แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน

<u>วัตถุประสงค์</u>

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน ไม่ให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องในการทางานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจากัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการอุตสาหกรรมทหาร โดยแนวปฏิบัติต้องมีการดาเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้ง ต่อปี

<u>ผู้รับผิดชอบ</u>

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

<u>แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน</u>

๑. การลงทะเบียนผู้ใช้งาน

๑.๑ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเทคโนโลยีสารสนเทศของกรมการอุตสาหกรรมทหาร

๑.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานที่ยังไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๑.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๑.๔ ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศทันทีเมื่อผู้ใช้งานนั้นมีการลาออกหรือเปลี่ยนตำแหน่งงาน

๒. การบริหารจัดการสิทธิของผู้ใช้งาน

๒.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๒ ผู้ดูแลระบบต้องมอบหมายสิทธิที่มีความสอดคล้องกับนโยบายการควบคุมการเข้าถึง

๒.๓ ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๔ ในกรณีมีความจาเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓. การบริหารจัดการรหัสผ่านสาหรับผู้ใช้งาน

๓.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสาหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๓.๒ ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราวและต้องเปลี่ยนรหัสผ่านที่มีการยากต่อการคาดเดาโดยผู้อื่น

๓.๓ ผู้ดูแลระบบต้องกาหนดรหัสผ่านชั่วคราว โดยกาหนดรหัสผ่านให้มีความยากต่อการคาดเดาโดยผู้อื่นและต้องกาหนดรหัสผ่านที่แตกต่างกัน

๓.๔ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยจัดส่งเป็นเอกสารลับหรือผ่านช่องทางระบบอัตโนมัติที่มั่นใจว่ามีความปลอดภัย และต้องกำหนดให้ผู้ใช้งานยืนยันการได้รับรหัสผ่านแล้ว

๔. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

๔.๑ ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๔.๒ ผู้ดูแลระบบ ต้องทบทวนสิทธิสาหรับผู้ที่มีสิทธิในระดับสูง ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๔.๓ ผู้ดูแลระบบ ต้องทบทวนสิทธิตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงใดๆ ได้แก่ การเลื่อนตำแหน่ง การย้ายหน่วยงาน

ส่วนที่ ๗
แนวปฏิบัติการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่ เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมการอุตสาหกรรมทหารเพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยต้องมีการดำเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้ง ต่อปี

ผู้รับผิดชอบ

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

แนวปฏิบัติการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

๑. การใช้งานรหัสผ่าน (Password Usage) ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ต้องปฏิบัติตามข้อกำหนดในการใช้รหัสผ่านดังนี้

๑.๑ ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการคาดเดาของผู้อื่น

๑.๒ ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

๑.๓ ผู้ใช้งานต้องเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๑.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้จากผู้อื่น

๑.๕ ผู้ใช้งานต้องตั้งรหัสผ่านที่มีความยาวเกินกว่าความยาวขั้นต่ำที่กำหนดไว้

๑.๖ ผู้ใช้งานไม่ต้องตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

๑.๗ ผู้ใช้งานต้องหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระเรียงกัน ได้แก่ abcd , ๑๒๓๔ หรือกลุ่มตัวอักขระที่เหมือนกันเช่น aaaa , ๑๑๑๑ เป็นต้น

๑.๘ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

๑.๙ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๑.๑๐ ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป ได้แก่ ทุกๆ ๓ เดือน สำหรับผู้ดูแลและทุก ๆ ๖ เดือน สำหรับผู้ใช้งานระบบ

๑.๑๑ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

๑.๑๒ ผู้ใช้งานไม่ต้องกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้เพื่อสะดวกต่อตนเองเมื่อทำการล็อกอินในภายหลัง

๑.๑๓ ผู้ใช้งานไม่ต้องใช้รหัสผ่านของตนร่วมกับผู้อื่น

๑.๑๔ ผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่ สำคัญหรือข้อมูลที่เป็นความลับ ผ่านเครือข่ายสาธารณะ

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๒.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน ได้แก่ ระบบงานเครื่องคอมพิวเตอร์ที่ใช้งาน

๒.๒ เจ้าหน้าที่ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๒.๓ ผู้ดูแลระบบต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๓. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

๓.๑ ผู้ดูแลระบบต้องจัดให้มีการควบคุมสินทรัพย์สารสนเทศ และการใช้งานระบบคอมพิวเตอร์ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๓.๒ ผู้ใช้งานทุกคนต้องปฏิบัติการป้องกันทรัพย์สิน

๓.๓ ผู้ใช้งานทุกคนต้องออกจากระบบที่ใช้งานทันที เมื่อจำเป็นต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแล

๓.๔ ผู้ใช้งานทุกคนต้องจัดเก็บข้อมูลสารสนเทศที่มีความสำคัญของกรมการอุตสาหกรรมทหารไว้ในที่ ปลอดภัย เช่น เก็บไว้ในตู้เก็บเอกสารที่มีระบบล็อค และมีกุญแจเปิดปิด

๓.๕ เมื่อสินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือข้อมูลอิเล็กทรอนิกส์ไม่สามารถใช้งานได้แล้วให้ผู้ดูแลระบบทำลายสินทรัพย์สารสนเทศ โดยมีข้อปฏิบัติดังนี้

๓.๕.๑ กระดาษ ให้ทำลายด้วยการหั่นด้วยเครื่องหั่นทำลายเอกสาร

๓.๕.๒ ซีดีหรือดีวีดี ให้ทำลายด้วยการหั่นด้วยเครื่องหั่นทำลายเอกสาร

๓.๕.๓ เทป ให้ทำลายด้วยการทุบหรือบดให้เสียหาย หรือเผาทำลาย

๓.๕.๔ ทัมป์ไดรฟ์หรือแฟลชไดรฟ์ ให้ทำลายด้วยการทุบหรือบดให้เสียหาย

๓.๕.๕ ฮาร์ดดิสก์ ให้ทำลายด้วยการเขียนทับข้อมูลซ้ำหลายรอบและทำให้เสียหายทางกายภาพ

๓.๕.๖ การทำลายข้อมูลจากฮาร์ดดิสก์ หรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ต่างๆด้วยวิธีการทำลายใช้สนามแม่เหล็กในการทำลาย ซึ่งสอดคล้องกับมาตรฐานของ The US Department of Defense (DOD) และ The National Security Agency (NSA)

๔. กำหนดให้เข้ารหัสกับข้อมูลที่เป็นความลับ การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ โดยให้เข้ารหัสข้อมูลที่มีชั้นความลับลับที่สุด ลับมาก และลับ รวมทั้งรหัสผ่านที่ผู้ใช้งานใช้ในการเข้าถึงระบบสารสนเทศ ได้แก่ รหัสผ่านของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ รหัสผ่านของผู้ใช้งานระบบเครือข่ายคอมพิวเตอร์โดยเมื่อเข้ารหัสข้อมูลรหัสผ่านแล้วจะต้องมีรูปแบบที่ไม่สามารถอ่านเข้าใจได้ หรือง่ายต่อการคาดเดา แม้ว่ามีผู้ใช้งานที่ตั้งรหัสผ่านเหมือนกัน เมื่อเข้ารหัสแล้วต้องมีรูปแบบที่แตกต่างกันเพื่อป้องกันไม่ให้ทราบได้ว่ามีผู้ใช้ที่ตั้งรหัสผ่านเหมือนกัน ทั้งนี้ หากผู้ใช้งานลืมหรือทำรหัสผ่านสูญหาย ต้องติดต่อโดยตรงด้วยตนเอง ณ แผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กรมการอุตสาหกรรมทหารเพื่อขอให้กำหนดรหัสผ่านให้ใหม่

ส่วนที่ ๘
แนวปฏิบัติการจัดทำระบบสำรองและการกู้คืนข้อมูล

วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติในการสำรองและกู้คืนข้อมูล ให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น โดยนโยบายแนวปฏิบัติต้องมีการดำเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้ง ต่อปี

ผู้รับผิดชอบ

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

แนวปฏิบัติในการสำรองข้อมูลและระบบคอมพิวเตอร์

๑. พิจารณาคัดเลือกและทบทวนระบบสารสนเทศที่มีความสำคัญ กำหนดประเภทของข้อมูลและกำหนดความถี่ในการจัดทำระบบสำรองที่เหมาะสมอย่างน้อยปีละ 1 ครั้ง โดยทำการประเมินความเสี่ยงที่มีผลทำให้ระบบสารสนเทศที่มีความสำคัญสูงไม่สามารถทำงานได้อันเป็นผลมาจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ

๒. การจัดทำบันทึกการสำรองข้อมูล ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ วันที่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก เป็นต้น

๓. ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรอง ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

๔. ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งสื่อที่ใช้เก็บข้อมูล

๕. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่าย ต้องพิจารณาคัดเลือกจัดทำระบบสำรองหรือทำการสำรองข้อมูลที่เหมาะสมเพื่อให้อยู่ในสภาพที่พร้อมใช้งาน ตามแผนการสำรองข้อมูลที่กำหนด

๖. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องตรวจสอบผลการสำรองข้อมูลด้วยว่าการสำรองข้อมูลถูกต้องสมบูรณ์หรือไม่

๗. ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขรายงานต่อ ผอ.กองควบคุมยุทธภัณฑ์หรือผู้ที่ได้รับมอบหมาย

๘. ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญ และจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความสำคัญของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานมากไปหาน้อย

๙. มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

๑๐. ต้องบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๑๑. มีการจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่าสม่ำเสมอ

๑๒. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม สำหรับการกู้คืนระบบ

๑๓. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

๑๔. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

๑๕. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนเป็นเหตุต้องมีการดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบ (System Administrator) ดำเนินการแก้ไข และรายงานปัญหาดังกล่าวต่อผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ หรือผู้ที่ได้รับมอบจากผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ ทราบโดยด่วน

๑๖. กรณีความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้รีบแจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบ เมื่อการดำเนินการกู้คืนระบบเสร็จสิ้นสมบูรณ์

๑๗. กำหนดให้ผู้ดูแลระบบ ต้องสำรองข้อมูลที่สำคัญของระบบงาน National Single Window (NSW) ได้แก่ ข้อมูลและค่า Configure ของ Database Server, Web Server, Mail Server และ Firewall Server เป็นประจำอย่างน้อย ๑ เดือนครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๑๘. จัดทำระบบสำรองและกู้คืนข้อมูลโดยมีแนวปฏิบัติตามประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์มาตรการกำกับดูแลความปลอดภัยต่อสุขภาพของมนุษย์จากการใช้เครื่องวิทยุโทรคมนาคม ข้อ ๑๒.๕

<u>แผนการสำรองข้อมูล</u>

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑. Mail Server	ค่า Configuration	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลใน Mail Box	๑ ครั้งต่อเดือน
๒. Web Server	ค่า Configuration	ก่อนและหลงการเปลี่ยนแปลง
	ข้อมูลเผยแพร่ในเว็บไซต์	๑ ครั้งต่อเดือน
๓. Database Server	ค่า Configuration	ก่อนและหลงการเปลี่ยนแปลง
	ข้อมูลในฐานข้อมูลระบบที่สำคัญ	๑ ครั้งต่อสัปดาห์
๔. Firewall Server	ค่า Configuration	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูล Rule ของ Firewall	๑ ครั้งต่อเดือน
๕. Server อื่นๆ ได้แก่ระบบงานต่างๆ	ค่า Configuration	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลบน Server อื่นๆ	๑ ครั้งต่อเดือน

<u>การกู้คืนข้อมูล</u>

๑. ในกรณีทีพบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งรายงานสรุปผลการปฏิบัติการ ต่อผอ.กองควบคุมยุทธภัณฑ์หรือผู้ที่ได้รับมอบหมายให้มีหน้าที่กำกับดูแลด้านสารสนเทศของกรมการอุตสาหกรรมทหาร

๒. ให้ใช้ข้อมูลทันสมัยที่สุดที่ได้ทำการสำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๓. หากการเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ที่เกี่ยวข้องรับทราบทันที

๔. มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์เป็นลำดับขั้น โดยผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ หรือผู้ที่ได้รับมอบหมายเป็นผู้กำกับดูแลการปฏิบัติงานความถี่อย่างน้อยปีละ ๑ ครั้ง

<u>แผนการกู้คืนข้อมูล</u>

สาเหตุ	วิธีการ
กรณีที่ ๑ เกิดความเสียหายต่อระบบงาน	จะทำการติดตั้งระบบงานจาก Source Code ทีมีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด
กรณีที่ ๒ เกิดความเสียหายขึ้นกับฐานข้อมูล	จะนำฐานข้อมูลที่เก็บไว้ล่าสุดกู้คืนเพื่อให้ใช้งานได้ต่อเนื่องและข้อมูลสูญหายน้อยที่สุด
กรณีที่ ๓ เกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS)SKDGDBF โดย Hardware ยังคงทำงานได้ปกติ	จะทำการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมทั้งทำการกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุดหรือตามความเหมาะสม
กรณีที่ ๔ เกิดความเสียหายขึ้นกับ Hardware	ให้บริษัทผู้ดูแลทำการแก้ไขเบื้องต้นให้ Hardware สามารถทำงานได้ตามปกติ และหากเกิดความเสียหาย กับ OS และระบบงาน จะทำการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมทั้งทำการกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุดหรือตามความเหมาะสม

การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ ต้องมอบหมายให้บุคลากรที่เกียวข้องดำเนินการดังต่อไปนี้

๑. กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๒. กำหนดชนิดของภัยพิบัติที่มีผลกระทบต่อระบบที่มีความสำคัญสูง

๓. ประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดไม่สามารถใช้งานได้อันเป็นผลมาจากภัย พิบัติที่กำหนดไว้

๔. จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๕. ต้องมีการทดสอบสภาพการพร้อมใช้ระบบสารสนเทศ ระบบสำรอง อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๖. มีการประเมินและปรับปรุงแผนรับมือกับภัยพิบัติสาหรับระบบที่มีความสำคัญสูง อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๙
แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของกรมการอุตสาหกรรมทหาร เพื่อให้มั่นใจว่านโยบายและมาตรฐานต่างๆ ด้านความมั่นคงปลอดภัยสารสนเทศได้มีการปฏิบัติตามอย่างมีประสิทธิผล โดยแนวปฏิบัติต้องมีการดาเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้ง ต่อปี

ผู้รับผิดชอบ

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

แนวปฏิบัติการตรวจสอบและประมินความเสี่ยง

๑. ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามเอกสาร การบริหารจัดการความเสี่ยงด้านสารสนเทศ การระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการอุตสาหกรรมทหารฯ ได้พิจารณาใช้วิธีการตั้งคำถามและหาคำตอบว่า มีปัจจัยใดที่เป็นความเสี่ยงต่อระบบเทคโนโลยีสารสนเทศในลักษณะว่า หากเกิดเหตุการณ์หนึ่งขึ้นจะส่งผลกระทบอย่างไร เพื่อนำไปสู่การพิจารณามาตรการป้องกันแก้ไข โดยพิจารณาในสองปัจจัย ได้แก่ ปัจจัยภายนอกองค์กรได้แก่ ภัยพิบัติ เหตุการณ์ความไม่สงบ และปัจจัยภายใน ได้แก่ ความไม่ปกติที่เกิดขึ้นกับระบบสารสนเทศและผู้ใช้งาน

๒. กำหนดวิธีการในการตรวจสอบและประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยง ผลลัพธ์ที่ได้จากขั้นตอนการระบุปัจจับที่ก่อให้เกิดความเสี่ยงจะทำให้เกิดปัจจัยเสี่ยงจำนวนมาก ดังนั้นเพื่อที่จะช่วยให้สามารถตัดสินใจใช้กลยุทธ์ที่เหมาะสมเป็นแนวทางในการจัดการความเสี่ยง จะต้องพิจารณาความเสี่ยงตามลำดับความสำคัญ โดยกำหนดเกณฑ์ในการประเมินความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงว่ามีโอกาสมากน้อยเพียงใด และความรุนแรงของผลกระทบที่จะเกิดขึ้นว่ามีมากน้อยเพียงใด การกำหนดหลักเกณฑ์ของโอกาสที่เกิดความเสี่ยงแบ่งเป็น ๕ ระดับ ดังนี้

ระดับ	การประเมิน
๑	มีโอกาสเกิดน้อยมาก
๒	มีโอกาสเกิดน้อย
๓	มีโอกาสเกิดปานกลาง
๔	มีโอกาสเกิดสูง
๕	มีโอกาสเกิดสูงมาก

การกำหนดหลักเกณฑ์ความรุนแรงของผลกระทบที่จะเกิดขึ้นแบ่งเป็น ๕ ระดับ ดังนี้

ระดับ	การประเมิน
๑	มีผลกระทบน้อยมาก
๒	มีผลกระทบน้อย
๓	มีผลกระทบปานกลาง
๔	มีผลกระทบมาก
๕	มีผลกระทบสูงมาก

การวิเคราะห์ความเสี่ยงพิจารณาจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยง โดยใช้ตารางประเมินระดับความเสี่ยง ดังต่อไปนี้

ตารางประเมินความเสี่ยง

ผลกระทบของความเสี่ยง						
	๕	๕	๑๐	๑๕	๒๐	๒๕
	๔	๔	๘	๑๒	๑๖	๒๐
	๓	๓	๖	๙	๑๒	๑๕
	๒	๒	๔	๖	๘	๑๐
	๑	๑	๒	๓	๔	๕
		๑	๒	๓	๔	๕

โอกาสที่จะเกิดความเสี่ยง

ระดับความเสี่ยง = โอกาสที่จะเกิดความเสี่ยง x ผลกระทบของความเสี่ยง

ตารางจัดระดับความเสี่ยง

ระดับความเสี่ยง	การจัดระดับ	ความหมาย
๑ - ๓	ต่ำ	ระดับที่ยอมรับได้โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องจัดการเพิ่มเติม
๔ - ๙	ปานกลาง	ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายยังระดับที่ยอมรับไม่ได้
๑๐ - ๑๖	สูง	ระดับที่ไม่สามารถยอมรับได้ ต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้
๑๗ - ๒๕	สูงมาก	ระดับที่มาสามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระที่ยอมรับได้ทันที

เมื่อจัดระดับของความเสี่ยงในแต่ละปัจจัยความเสี่ยงได้แล้ว จึงนำปัจจับความเสี่ยงนั้น ๆ มาจัดลำดับความสำคัญจากระดับความเสี่ยงสูงมากไปจนถึงระดับความเสี่ยงต่ำ เพื่อเลือกกลยุทธ์ในการจัดการที่เหมาะสม

๓. กำหนดมาตรการจัดการความเสี่ยง

๓.๑ ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ฉุกเฉินและภัยพิบัติต่างๆ

๓.๒ จัดทำหลักเกณฑ์กฎระเบียบในการใช้เครื่องคอมพิวเตอร์และเครือข่ายของกรมการอุตสาหกรรมทหาร

๔. จัดให้มีการตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายในองค์กร (Internal Auditor) และโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)) ได้แก่ สำนักงานตรวจสอบภายในกลาโหม และกรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม โดยพิจารณาตามความเหมาะสม อย่างน้อยปีละ ๑ ครั้ง เพื่อให้ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๕. ต้องมีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันที่เหมาะสม ตามแผนการฝึกอบรมเรื่อง “ความเสี่ยงและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ”

๖. ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆแก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารสูงสุด ซึ่งหมายถึง เจ้ากรมการอุตสาหกรรมทหารฯ ซึ่งมีหน้าที่กำกับดูแลด้านสารสนเทศของกรมการอุตสาหกรรมทหาร เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นโดยตรง รวมถึงที่มีการร้องเรียนและการฟ้องร้องภายใต้กฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ส่วนที่ ๑๐
แนวปฏิบัติความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต

<u>วัตถุประสงค์</u>

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ตอย่างปลอดภัยและป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เช่นการส่งข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรืออื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของกรมการอุตสาหกรรมทหารถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้ โดยแนวปฏิบัติต้องมีการดำเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้ง ต่อปี

<u>ผู้รับผิดชอบ</u>

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

<u>แนวปฏิบัติในการใช้งานอินเตอร์เน็ต</u>

๑. ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบความปลอดภัยทีกรมการอุตสาหกรรมทหารจัดสรรไว้เท่านั้นเช่น Firewall, Proxy, IPS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุความจำเป็นและทำการขออนุญาตจากกลุ่มระบบเครือข่ายและคอมพิวเตอร์เป็นลายลักษณ์อักษร

๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์ ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

๓. ผู้ใช้ต้องไม่ใช้เครือข่ายของกรมการอุตสาหกรรมทหารเพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บที่ไม่เหมาะสม เช่นเว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือ เว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๔. ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกรมการอุตสาหกรรมทหาร

๕. ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ขัดต่อศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจจะก่อให้เกิดความเสียหานแก่กรมการอุตสาหกรรมทหาร

๖. ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมการอุตสาหกรรมทหารที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเตอร์เน็ต

๗. หลังการใช้งานอินเตอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการใช้งานโดยบุคคลอื่น

ส่วนที่ ๑๑
แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรมการอุตสาหกรรมทหารสามารถสนับสนุนการปฏิบัติการและการบริหารของกรมการอุตสาหกรรมทหารให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล และเพื่อให้การรับส่งจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรมการอุตสาหกรรมทหารเป็นมาตรฐานและอยู่ในกรอบของกฎหมาย ระเบียบคำสั่ง ข้อบังคับของกรมการอุตสาหกรรมทหาร โดยแนวปฏิบัติต้องมีการดำเนินการตรวจสอบและประเมินตามระยะเวลา ๑ ครั้ง ต่อปี

ผู้รับผิดชอบ

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

แนวทางปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์

๑. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมการอุตสาหกรรมทหาร ฯ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่นการลาออก การเลื่อนตำแหน่ง

๒. ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่านสำหรับการเข้าใช้งานครั้งแรกเพื่อตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมการอุตสาหกรรมทหาร

๓. ผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรก ระบบต้องบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๔. ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๕. ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ต้องมีการล็อกเอาท์จากหน้าจอตัดการใช้งานเมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

๖. ผู้ใช้จะต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลโดยอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๗. ผู้ใช้ต้องมีการเปลี่ยนรหัสผ่านทุก ๓ – ๖ เดือน

๘. ผู้ใช้ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายแก่กรมการอุตสาหกรรมทหาร ฯ หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมาย หรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรมการอุตสาหกรรมทหาร ฯ

๙. ผู้ใช้ไม่ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์(e-Mail Address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นจะได้รับการยินยอมจากเจ้าของผู้ใช้และถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๑๐. ผู้ใช้ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของกรมการอุตสาหกรรมทหารเพื่องานของกรมการอุตสาหกรรมทหาร ฯ เท่านั้น

๑๑. ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๒. ผู้ใช้ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ ของตนเองทุกวันและต้องจัดเก็บจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๑๓. ผู้ใช้ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๑๔. หลังการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จแล้วให้ทำการล็อกเอาส์ออกจากระบบเพื่อป้องกันการใช้งานโดยบุคคลอื่น

ส่วนที่ ๑๒
แนวปฏิบัติการฝึกอบรม

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการฝึกอบรมบุคลากร และเจ้าหน้าที่ในการปฏิบัติงานของกรมการอุตสาหกรรมทหาร เพื่อให้บุคลากร และเจ้าหน้าที่มีความเข้าใจ และยึดถือปฏิบัติในแนวนโยบายและแนวทางการปฏิบัติ ด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างมีประสิทธิผล

ผู้รับผิดชอบ

๑. ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๒. หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ
๓. ประจำแผนกกรรมวิธีข้อมูลยุทธภัณฑ์ กองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ

แนวปฏิบัติการฝึกอบรม

๑. การฝึกอบรม

๑.๑ มีการฝึกอบรมถ่ายทอดความรู้ด้านการควบคุม ดูแลรับผิดชอบในการปฏิบัติสำหรับการเข้าออกห้องควบคุมเครือข่าย, การเข้าถึงระบบสารสนเทศ, การเข้าถึงและใช้บริการระบบเครือข่าย, การเข้าถึงระบบปฏิบัติการ, การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ, การเข้าถึงของผู้ใช้งาน, หน้าที่ความรับผิดชอบของผู้ใช้งาน, การสำรองและการกู้คืนข้อมูล, การตรวจสอบและประเมินความเสี่ยง, ความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต, การใช้งานจดหมายอิเล็กทรอนิกส์ ให้กับผู้บริหารหรือผู้ที่มีหน้าที่เกี่ยวข้องในการดูแลระบบ ของกรมการอุตสาหกรรมทหาร ฯ ที่มีหน้าที่เกี่ยวข้องในส่วนต่าง ๆ ของระบบสารสนเทศ ทั้งนี้ มีจุดมุ่งหมายเพื่อให้เจ้าหน้าที่สามารถใช้งานระบบได้อย่างถูกต้อง มีประสิทธิภาพ และมีความปลอดภัย โดยต้องมีการฝึกอบรมอย่างน้อยปีละ ๒ ครั้ง หรือเมื่อมีการปรับปรุงแก้ไขนโยบายและการปฏิบัติ

๑.๒ มีการฝึกอบรมถ่ายทอดความรู้ด้านการปฏิบัติต่าง ๆ รวมถึงด้านความปลอดภัยในการใช้งานระบบสารสนเทศของกรมการอุตสาหกรรมทหาร ฯ เพื่อให้ผู้ใช้บริการสามารถปฏิบัติงานได้อย่างถูกต้อง มีประสิทธิภาพ และตระหนักถึงความปลอดภัยในการใช้งานหรือการปฏิบัติอยู่เสมอ โดยต้องมีการฝึกอบรมอย่างน้อยปีละ ๒ ครั้ง หรือเมื่อมีการปรับปรุงแก้ไขนโยบายและการปฏิบัติ

๑.๓ จัดทำแผนฝึกอบรมโดยมีรายละเอียดไม่น้อยกว่าที่กำหนดดังนี้

๑.๓.๑ ชื่อวิชา (Title)
๑.๓.๒ เนื้อหา (Content)
๑.๓.๓ กลุ่มผู้อบรม (Target Group)
๑.๓.๔ กำหนดวันที่จะฝึกอบรม (Timing)
๑.๓.๕ ระยะเวลาที่จะต้องใช้ (Duration)
๑.๓.๖ วิธีการอบรม (Workshop)
๑.๓.๗ สถานที่ทำการอบรม (Location)
๑.๓.๘ จำนวนผู้เข้าอบรม (Class Size)
๑.๓.๙ Training Course Material

๒. เอกสารและคู่มือต่าง ๆ

๒.๑ ผู้จัดฝึกอบรมต้องจัดทำคู่มือหรือเอกสารการฝึกอบรม สำหรับผู้เข้าอบรมท่านละ ๑ ชุด

๒.๒ ผู้จัดฝึกอบรมจะต้องมีคู่มือหรือเอกสารด้านแนวนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยที่เป็นภาษาไทย แจกจ่ายให้แต่ละแผนกในกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม กรมการอุตสาหกรรมทหาร ฯ

แผนการฝึกอบรม “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร พ.ศ. ๒๕๕๙

ลำดับที่	หลักสูตรการฝึกอบรม	ผู้เข้ารับการฝึกอบรม	ปี ๒๕๖๐			ปี ๒๕๖๑											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
๑	การเข้าถึงระบบสารสนเทศ	เจ้าหน้าที่ทุกระดับ ผู้ใช้บริการ	•		•					•		•					
๒	การเข้าถึงและใช้บริการระบบเครือข่าย	เจ้าหน้าที่ทุกระดับ ผู้ใช้บริการ	•		•					•		•					
๓	การเข้าถึงโปรแกรมประยุกต์	เจ้าหน้าที่ทุกระดับ	•							•							
๔	การเข้าถึงระบบปฏิบัติการ	เจ้าหน้าที่ที่มีส่วนเกี่ยวข้อง		•							•						
๕	การสำรองและการกู้คืนข้อมูล	เจ้าหน้าที่ที่มีส่วนเกี่ยวข้อง		•							•						
๖	การตรวจสอบและประเมินความเสี่ยง	เจ้าหน้าที่ที่มีส่วนเกี่ยวข้อง		•							•						
๗	การเข้าถึงของผู้ใช้งาน และหน้าที่ความรับผิดชอบของผู้ใช้งาน	ผู้ใช้บริการ			•							•					
๘	ความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต	เจ้าหน้าที่ทุกระดับ ผู้ใช้บริการ	•		•					•		•					
๙	หลักสูตรความปลอดภัยในการใช้งานระบบสารสนเทศ	เจ้าหน้าที่ทุกระดับ ผู้ใช้บริการ	•		•					•		•					
	หมายเหตุ : ถ้ามีการปรับปรุงแก้ไขนโยบายและการปฏิบัติ จะต้องมีการฝึกอบรมในเดือนต่อไป																

ผนวก ก
แผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของ
ฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

หลักการและเหตุผล

ระบบข้อมูลและสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถไปใช้ประโยชน์ต่อการบริหารราชการได้อย่างมีประสิทธิภาพ

กรมการอุตสาหกรรมทหาร ฯ ได้นำเอาฐานข้อมูลและสารสนเทศ เข้ามาใช้เพื่อเพิ่มประสิทธิภาพในการดำเนินงาน และให้บริการหน่วยงานทั้งภาครัฐและเอกชนให้ได้รับความสะดวก ขณะเดียวกันระบบฐานข้อมูลและสารสนเทศ อาจได้รับความเสียหายจากการโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ทำความเสียหายต่อระบบฐานข้อมูลและสารสนเทศ ส่งผลกระทบต่อการดำเนินงานของหน่วยงาน เพื่อป้องกันและแก้ไขปัญหาดังกล่าว กรมการอุตสาหกรรมทหาร ฯ ได้เล็งเห็นความจำเป็นต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบฐานข้อมูลและสารสนเทศ จึงได้กำหนดแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) โดยการวิเคราะห์ปัจจัย ข้อเสนอแนะ แนวทางในการดำเนินงาน และแผนการดำเนินงาน เพื่อใช้เป็นแนวทางในการป้องกันผลกระทบที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ ให้กลับคืนสู่สภาวะปกติ และสามารถปฏิบัติงานได้อย่างต่อเนื่อง มีประสิทธิภาพ

วัตถุประสงค์

๑. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบของฐานข้อมูลและสารสนเทศของกรมการอุตสาหกรรมทหาร

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างมีระบบและต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

กรอบแนวทางในการจัดทำแผน

การจัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ อันอาจมีผลกระทบต่อฐานข้อมูลและสารสนเทศ (IT Contingency Plan) มีแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ดังนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
๒. แนวทางการป้องกันและเตรียมการเบื้องต้น
๓. การเตรียมความพร้อม
๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
๕. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ
๖. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ
๗. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม
๘. การติดตามและรายงานผล

<u>ภัยพิบัติ</u>

ภัยที่อาจก่อให้เกิดความเสียหายกับฐานข้อมูลและสารสนเทศของกรมการอุตสาหกรรมทหาร สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

๑. ภัยพิบัติจากภายนอก

๑.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง

๑.๔ ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

๑.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๑.๖ ไวรัสคอมพิวเตอร์

๑.๗ ระบบเสียหายจากภัยสงครามเหตุจลาจลและการเกิดสถานการณ์ความไม่สงบ

๒. ภัยพิบัติจากภายใน

๒.๑ ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๒.๓ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

<u>แนวทางการป้องกันความเสียหายจากภัยพิบัติ</u>

<u>๑. ภัยพิบัติจากภายนอก</u>

๑.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

๑.๑.๑ <u>การป้องกันและการดำเนินการอัคคีภัย</u>

(๑) กำหนดเวรรักษาการณ์รักษาความปลอดภัย

(๒) อบรมแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิง การหนีไฟขั้นต้นให้แก่ข้าราชการตำรวจทุกราย

(๓) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย

(๔) จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

๑.๑.๒ <u>การป้องกันอุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม</u>

(๑) เปิดเครื่องปรับอากาศ สำหรับเครื่องแม่ข่ายตลอด ๒๔ ชั่วโมง และตรวจสอบการทำงานให้ใช้งานได้อย่างสม่ำเสมอ

(๒) เครื่องคอมพิวเตอร์แม่ข่ายต้องไม่อยู่ในบริเวณที่น้ำท่วมถึง

(๓) ติดตามข่าวสารภัยพิบัติตามสถานการณ์ที่เกิดขึ้น

๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๒.๑ ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของ แผนกกรรมวิธีและข้อมูลยุทธภัณฑ์เป็นผู้รับผิดชอบนำเข้าไป

๑.๒.๒ จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตน (Finger Scan) และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

๑.๒.๓ ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๑.๓ ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง

๑.๓.๑ การตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ตลอดเวลา

๑.๓.๒ จัดให้มีเครือข่ายสำรอง สำหรับใช้ในกรณีที่เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้

๑.๓.๓ ประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อแก้ไขปัญหา

๑.๔ ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

๑.๔.๑ ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที

๑.๔.๒ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ ตรวจสอบระบบสำรองไฟฟ้า (UPS) ทุกวันศุกร์

๑.๔.๓ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้หยุดบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์รวมทั้งอุปกรณ์ต่าง ๆ

๑.๔.๔ สำรองข้อมูลที่สำคัญบนสื่อที่สามารถจัดเก็บข้อมูลได้อย่างเหมาะสม (DVD , CD , External Harddisk , Handy drive ฯลฯ)

๑.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๑.๕.๑ สแกนหาจุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

๑.๕.๒ ติดตั้ง Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตสามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

๑.๕.๓ ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

๑.๕.๔ จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๑.๕.๕ ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่มีการใช้งาน

๑.๕.๖ กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติดังนี้

(๑) ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(๒) ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น

(๓) จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

(๔) เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๕) ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย ๘ อักขระ

(๖) ตั้งรหัสผ่านโดยใช้เทคนิคส่วนตัวที่ง่ายต่อการจำรหัสผ่านที่ได้กำหนดไว้

(๗) ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓, abcd เป็นต้น หรือเป็นกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑๑๑, aaa, bbbเป็นต้น

(๘) เปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ ๖ เดือน ส่วนในกรณีของผู้ดูแลระบบ ให้เปลี่ยนรหัสผ่านใหม่ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุก ๆ ๓ เดือน

(๙) เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(๑๐) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

(๑๑) ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เช่น บันทึกไว้ในหน้าจอล็อกอิน (ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง จะได้ไม่ต้องใส่รหัสผ่านอีกครั้ง)

(๑๒) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

๑.๕.๗ ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอก โดยการนำระบบ DMZมากรอง IP ที่จะเข้ามายังระบบเครือข่าย

๑.๕.๘ ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ DDOS

๑.๖ ไวรัสคอมพิวเตอร์

๑.๖.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอและต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๑.๖.๒ ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

(๑) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

(๒) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

(๓) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๑.๖.๓ ใช้ความระมัดระวังในการเปิด E-mail

(๑) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

(๒) ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๑.๖.๔ ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต

(๑) ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ

(๒) ไม่ควรเปิด website ที่แนะนำมาทาง E-mail

(๓) ไม่ดาวน์โหลดไฟล์จาก website ที่ไม่น่าเชื่อถือ

(๔) ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ

(๕) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๑.๖.๕ ปิดการใช้งานฟังก์ชัน Autoplay เพื่อป้องกันไม่ให้ไวรัสที่แพร่ระบาดผ่านทางสื่อเก็บข้อมูลแบบพกพาใช้เป็นช่องทางในการรันไฟล์ไวรัสโดยอัตโนมัติ

๑.๗ ระบบเสียหายจากภัยสงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

เนื่องจากเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ ในการป้องกันหากไม่สามารถย้ายสถานที่หรือป้องกันสถานที่ได้ ควรมีการ Back Up ข้อมูลไว้มากกว่า ๑ Back Up และแยกสถานที่จัดเก็บ และถ้าเกิดความเสียหายเกิดขึ้นกับข้อมูล ก็สามารถนำข้อมูลที่มีการ Back Up ไว้ และอุปกรณ์คอมพิวเตอร์ สำรองมาใช้แทน หากเกิดความเสียหายร้ายแรงควรมีศูนย์คอมพิวเตอร์สำรองเพิ่ม

๒. ภัยพิบัติจากภายใน

๒.๑ ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๑.๑ การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน

๒.๑.๒ การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนด ทุกสัปดาห์ โดยจะสำรองข้อมูลโครงสร้างข้อมูล Source Code และบันทึกข้อมูลลงในสื่อบันทึก

๒.๑.๓ ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้สำรองไว้ในสื่อบันทึก ทุกสัปดาห์

๒.๑.๔ จัดเจ้าหน้าที่ในการบำรุงรักษาสื่อบันทึกข้อมูลของเครื่องคอมพิวเตอร์แม่ข่าย เพื่อลดความเสียหายของข้อมูล

๒.๒ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๒.๒.๑ ติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องแม่ข่ายและลูกข่ายเพื่อให้สามารถตรวจสอบได้

๒.๒.๒ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ

๒.๒.๓ หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๒.๒.๔ สร้างความรู้ความเข้าใจในการป้องกันและแก้ไขปัญหาจากไวรัสคอมพิวเตอร์เบื้องต้น

๒.๓ บุคลากรขาดความรู้ในการใช้เครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ ซึ่งอาจทำให้ฐานข้อมูลและสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๒.๓.๑ ให้ความรู้แก่ผู้ใช้งานผ่านช่องทางต่างๆ เช่น website, หนังสือเวียน เป็นต้น

๒.๓.๒ ใส่กุญแจตู้อุปกรณ์เครือข่ายเพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่ หรือบุคลากรที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

ขั้นตอนปฏิบัติในมาตรการที่สำคัญ

๑. การจัดเตรียมอุปกรณ์ที่จำเป็น

๑.๑ แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

๑.๒ เทปสำรองข้อมูลและระบบงานที่สำคัญ

๑.๓ แผ่นโปรแกรม antivirus/spyware

๑.๔ แผ่น driver อุปกรณ์ต่างๆ

๑.๕ ระบบสำรองไฟฉุกเฉิน

๑.๖ อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

๒. การสำรองข้อมูล (Back Up)

๒.๑ การสำรองข้อมูลอัตโนมัติโดยระบบเครื่องประมวลผลแม่ข่าย โดยสำรองข้อมูลไว้ในสื่อบันทึก ๑ ชุด

๒.๒ การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตาม ระยะเวลาที่กำหนดเป็นประจำทุกสัปดาห์ โดยสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในสื่อบันทึก

๓. การกู้ข้อมูล (Recovery)

๓.๑ ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูลที่ได้สำรองไว้ในสื่อบันทึก ทุกสัปดาห์

๓.๒ ทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้สำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียทุกสัปดาห์

<u>ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ</u>

๑. กรณีเครื่องลูกข่าย

๑.๑ ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ฐานข้อมูลและสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือดูแลทราบ หรือ กรณีมีเหตุอันทำให้เจ้าหน้าที่ผู้เกี่ยวข้องไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้หน่วยงานที่เกี่ยวข้องทราบ

๑.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ดึงสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องโดยเร็ว

๑.๓ ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของเครื่อง คอมพิวเตอร์ที่พบการขัดข้อง ให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๑.๔ ให้เจ้าหน้าที่ที่เกี่ยวข้อง แจ้งเหตุขัดข้องนั้นให้หัวหน้า หรือผู้บังคับบัญชาทราบโดยเร็ว

๒. กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

๒.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒.๒ ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๒.๓ ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๒.๔ รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๒.๕ ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ Server และระบบเครือข่ายโดยเร็วที่สุด

๒.๖ ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบ นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๒.๗ ผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

๓. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

๓.๑ เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆ ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

๓.๒ สแกนและกำจัดไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัส

๓.๓ แจ้งเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อตรวจสอบ

๔. หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัยเพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติ ดังนี้

๔.๑ ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

๔.๒ ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

๔.๓ ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉิน มิให้ปิดตายหรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเองไปยังทางออกฉุกเฉิน เพื่อให้ไปถึงทางได้ แม้ว่าไฟดับหรือปกคลุมไปด้วยควัน

๔.๔ เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้จากนั้นออกจากอาคารแล้วแจ้งหน่วยดับเพลิงทันที

๔.๕ เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

๔.๖ หากเพลิงไหม้ในห้องทำงานให้ออกจากห้อง ปิดประตู แล้วแจ้งฝ่ายอาคารและ สถานที่เพื่อแจ้งหน่วยดับเพลิงทันที

๔.๗ หากเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนออกจากอาคารให้วางมือบนประตู หาก ประตูมีความเย็นอยู่ ค่อยๆ เปิดประตู แล้วไปยังทางหนีไฟฉุกเฉินที่ใกล้ที่สุด

๔.๘ หากเพลิงไหม้อยู่บริเวณใกล้ประตู จะมีความร้อน ห้ามเปิดประตูโดยเด็ดขาด ให้รีบแจ้งหน่วยดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเพลิงไหม้ หาผ้าเปียก ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

๔.๙ เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

๔.๑๐ ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

๕. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับส่งมาก ดังนั้น สิ่งที่มักจะเกิดขึ้นและยากต่อการหลีกเลี่ยงคือ ผลกระทบต่างๆ ที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลสำคัญ รวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ประกอบด้วย

๕.๑ เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาเปิดใช้งาน ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

๕.๒ เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

<u>แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม</u>

การคืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑. จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน

๒. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง

๔. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้เป็นการชั่วคราว

๕. นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็วภายใน ๔๘ ชั่วโมง

๖. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่นๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบ

๑. ระดับนโยบาย

ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจน ติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

๒. ระดับปฏิบัติ

หัวหน้าแผนกกรรมวิธีข้อมูลยูทธภัณฑ์ และประจำแผนกกรรมวิธีข้อมูลยูทธภัณฑ์ กรมการอุตสาหกรรมทหาร ฯ รวมถึงเจ้าหน้าที่ผู้ดูแลระบบที่ได้รับมอบหมายของหน่วยในการรับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และรักษาความปลอดภัยระบบฐานข้อมูลและฐานข้อมูลและสารสนเทศ โดยแบ่งทีมงาน ดังนี้

๒.๑ ทีมบริหารจัดการการกู้คืนระบบ ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ

๒.๒ ทีมกู้คืนเครือข่าย ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติ

๒.๓ ทีมกู้คืนแอพพลิเคชัน ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน

๒.๔ ทีมประเมินความเสียหาย เป็นทีมให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน

๒.๕ ทีมอาคารสถานที่ เป็นทีมที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร เครื่องปรับอากาศให้พร้อมใช้งาน

๒.๖ ทีมจัดการทั่วไป เป็นทีมประสานงานช่วยเหลือทีมอื่นๆ ให้บรรลุวัตถุประสงค์ในการทำงาน

๒.๗ ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง

๒.๘ ทีมแก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อไฟระเบิด ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรอง ข้อมูลที่สำคัญ จากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่

๒.๙ ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบ ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ สูบน้ำออกจากห้องควบคุมระบบและตรวจสอบการรั่วซึม

๒.๑๐ ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย

๒.๑๑ ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery) ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ได้ทันทีและครบถ้วนสมบูรณ์

๒.๑๒ ทีมแก้ไขปัญหา เนื่องจากแผ่นดินไหว ทำหน้าที่แจ้งเหตุต่อผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ เพื่อผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ ดำเนินการประกาศสั่งการตามแผนที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้ และหลังจากเหตุแผ่นดินไหวสงบลงให้ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้อำนวยการกอง

ควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม ฯ เพื่อทราบและสั่งการต่อไป

๒.๑๓ ทีมแก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชาเพื่อผู้บังคับบัญชา ดำเนินการสั่งการตามแผนที่เตรียมไว้ เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลงให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้บังคับบัญชาเพื่อทราบและสั่งการต่อไป

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บริหารบังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้

๑.	กรมการอุตสาหกรรมทหาร	๐ ๒๒๔๑ ๐๔๓๐
๒.	ผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม	๐ ๒๒๔๑ ๔๐๔๙ ต่อ ๖๐๑
๓	รองผู้อำนวยการกองควบคุมยุทธภัณฑ์และพัฒนาอุตสาหกรรม	๐ ๒๒๔๑ ๔๐๔๙ ต่อ ๖๐๒
๔	หัวหน้าแผนกกรรมวิธีข้อมูลยุทธภัณฑ์	๐ ๒๒๔๑ ๔๐๔๙ ต่อ ๖๐๔
๕	กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม	๐ ๒๕๐๑ ๖๖๖๐
๖	สถานีตำรวจนครบาลดุสิต	๐ ๒๒๔๑ ๕๐๔๓
๗	การไฟฟ้านครหลวงเขตสามเสน	๐ ๒๒๔๒ ๐๑๓๐
๘	บริษัท สมาร์ท อัลลายแอนส์ จำกัด	๐ ๒๖๔๓ ๙๑๐๑