มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน และต้องปฏิบัติเพิ่มเติม

1) วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบ สารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ โดยอาจจะ กำหนดระยะเวลาและขอบเขตของการตรวจสอบ รวมถึงการเลือกเครื่องมือและเทคนิคที่จะใช้ในการตรวจสอบ

2) ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูก ละเมิดการใช้งาน (Compromise) อาจจะดำเนินการเข้ารหัสข้อมูล (Encryption): การเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายจะช่วยป้องกันการถูกตีความหรือดักฟัง ทำให้ไม่สามารถเข้าถึงข้อมูลได้โดยง่าย

3) ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน อย่างสมำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอโดยการดำเนินการอาจใช้การใช้เทคโนโลยีการแจ้งเตือนอัตโนมัติ (Automated notification technology) เพื่อแจ้งเตือนผู้ที่เกี่ยวข้องเมื่อเกิดภาวะฉุกเฉินและอัพเดตสถานการณ์

4) กำหนดขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์
อาจจะผ่านระบบ Authentication เช่น Two-Factor Authentication (2FA) หรือ Multi-Factor Authentication (MFA) เพื่อเพิ่มความปลอดภัยในการเข้าสู่ระบบ รวมถึงการใช้งานเครื่องมือตรวจสอบรหัสผ่าน (Password Strength Checker) เพื่อป้องกันการใช้รหัสผ่านที่ง่ายต่อการเดาได้ และการใช้งานเครื่องมือควบคุมการเข้าถึง (Access Control Tool) เพื่อจัดการสิทธิ์การเข้าถึงของผู้ใช้งานในระบบปฏิบัติการคอมพิวเตอร์

5) ไม่ควรนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของ หน่วยงาน หากมิได้รับอนุญาตยกตัวอย่างเช่นควรมีการกำหนดนำเข้า-นำออกของอุปกรณ์และซอฟต์แวร์โดยเฉพาะอย่างยิ่งในสถานที่ที่มีข้อมูลสำคัญหรือข้อมูลที่ต้องการความมั่นคงปลอดภัย และควรมีการสอนแนะนำเจ้าหน้าที่และผู้ใช้งานเกี่ยวกับนำเข้า-นำออกของอุปกรณ์และซอฟต์แวร์ เพื่อให้ผู้ใช้เข้าใจถึงความสำคัญของการควบคุมการนำเข้า-นำออก นอกจากนี้ ยังควรใช้เครื่องมือป้องกันการนำอุปกรณ์และซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานโดยไม่ได้รับอนุญาต

6) มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้าน หรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน เช่น ควรมีการกำหนดสิทธิ์และบทบาทในการติดต่อกับหน่วยงานเหล่านั้น รวมถึงแนวทางในการสื่อสารหรือการติดต่อที่เหมาะสมกับสถานการณ์และเป้าหมายของการติดต่อ
โดยควรใช้ช่องทางที่ปลอดภัยเช่นการใช้โทรศัพท์ที่มีการเข้ารหัสและการใช้ Virtual Private Network (VPN) เพื่อเชื่อมต่อกับหน่วยงานภายนอก
นอกจากนี้ยังควรมีการตรวจสอบและติดตามผลการติดต่อกับหน่วยงานเหล่านั้นเพื่อให้มั่นใจว่าการติดต่อนั้นได้ดำเนินไปโดยปลอดภัยและเป็นไปตามวัตถุประสงค์ที่ต้องการ

7) การออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถานที่ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ โดในการป้องกันความมั่นคงปลอดภัยด้านกายภาพ สามารถใช้เครื่องมือต่าง ๆ เช่น ระบบกล้องวงจรปิด (CCTV)
เพื่อตรวจสอบการเข้าถึงพื้นที่หรือสถานที่ ระบบประตูอัตโนมัติ (Automatic door access system)
เพื่อควบคุมการเข้าถึงสถานที่ ระบบปรับอากาศ (Air conditioning system)
เพื่อควบคุมอุณหภูมิและความชื้นภายในสถานที่

8) ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรมใช้เครื่องมือ
ที่เรียกว่า "code obfuscation" หรือ "code obfuscator" ซึ่งเป็นเครื่องมือที่ใช้เข้ารหัส (encode) โค้ดของโปรแกรมเพื่อทำให้ผู้ไม่ได้รับอนุญาตไม่สามารถอ่านหรือแกะระบบ (decompile) โค้ดของโปรแกรมได้ ซึ่งจะช่วยเพิ่มความปลอดภัยให้กับโปรแกรมได้ โดยที่ผู้ไม่ได้รับอนุญาตจะไม่สามารถเข้าใจโค้ดที่อยู่ในรูปแบบที่เข้ารหัสแล้วได้

นอกจากนี้ยังสามารถใช้เครื่องมือการตรวจสอบการโจมตี (Intrusion Detection System) หรือเครื่องมือป้องกันการเข้าถึง (Access Control Tool) เพื่อจำกัดการเข้าถึงของผู้ไม่ได้รับอนุญาตในการเข้าถึงโปรแกรมและซอร์สโค้ดของโปรแกรมได้ด้วย

9) **ระบบเวลาของระบบสารสนเทศต่าง ๆ ที่ใช้ในหน่วยงานหรือในขอบเขตงานด้านความมั่นคงปลอดภัย (Security domain) ต้องมีความสอดคล้องกัน (Synchronization) โดยให้มีการตั้งค่าพร้อมกับเวลาจากแหล่งเวลาที่เชื่อถือได้ การเลือกใช้แหล่งที่มาจะเลือกใช้การตั้งเวลาตามที่เป็นเวลาสากลตามเวลามาตรฐานประเทศไทยโดย กรมอุทกศาสตร์ กองทัพเรือ แล้วนำมาตั้งค่าเป็นเวลาในระบบ**

10) ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของ หน่วยงานจากระยะไกล เพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล ควรมีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสม เช่น การใช้ระบบรหัสผ่าน (password) ที่มีความปลอดภัยเพียงพอ หรือการใช้ระบบการตรวจสอบตัวตนสองขั้นตอน เช่น การใช้รหัสผ่าน (password) ร่วมกับการตรวจสอบชื่อผู้ใช้ (username) หรือการใช้ระบบการตรวจสอบตัวตนด้วยเทคโนโลยีที่สูงขึ้น เช่น การใช้เทคโนโลยีบิ๊วเมตริกส์ (biometrics) เช่น การสแกนลายนิ้วมือ (fingerprint), การสแกนรูปหน้า (facial recognition), หรือการสแกนลายตา (iris scan) เป็นต้น