กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

แนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(กพร.-IT-SEC-G1)

แก้ไขครั้งที่ ๑
สำเนาที่
วันที่ประกาศใช้

ผู้จัดทำ	ผู้ตรวจ	ผู้อนุมัติ
.....	.....	.....
(นายผดุงศักดิ์ โนจิตร)	(นายมานุส มณีนุษย์)	(นายธวัช ผลความดี)
วิศวกรเหมืองแร่ชำนาญการ	ผอ.ศสท.	รองอธิบดี กพร. (CIO)

สารบัญ

ประวัติเอกสาร

เวอร์ชั่น	วันที่	ผู้แก้ไข	หมายเหตุ
๑.๐	๒๑ มีนาคม ๒๕๕๔	นายผดุงศักดิ์ โนจิตร	สร้างเอกสาร

๑. บทนำ

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางสำหรับการปฏิบัติงาน การวางโครงสร้างพื้นฐาน การจัดเตรียมระบบ การให้บริการ และการใช้งานสารสนเทศเป็นไปอย่างมีความมั่นคงปลอดภัยตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กพร.

๒. วัตถุประสงค์

๒.๑. เพื่อลดความเสียหายที่จะเกิดขึ้นกับการใช้ระบบสารสนเทศ

๒.๒. เพื่อให้ผู้ใช้ทราบถึงกฎระเบียบ ข้อห้ามและแนวปฏิบัติในการใช้งานระบบสารสนเทศ ของ กพร.

๒.๓. เพื่อให้การใช้งานระบบสารสนเทศมีความมั่นคงปลอดภัยมากขึ้น

๒.๔. เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้ระบบสารสนเทศให้ชัดเจน

๒.๕. เพื่อให้ระบบสารสนเทศ ของ กพร. มีมาตรฐานเป็นที่ยอมรับ โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001

๒.๖. เพื่อให้การดำเนินการใดๆ มีแนวทางปฏิบัติที่เป็นไปในแนวทางเดียวกัน

๓. คำนิยาม

การกำหนดนิยามในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสามารถดูได้จากเอกสารนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (กพร.-IT-SEC-P1) หัวข้อ ๑. กำหนดนิยาม

สำหรับเอกสารแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้มีการกำหนดนิยามเพิ่มเติม ดังนี้

๓.๑. **ทรัพยากร** หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของ ศสท. กพร.

๓.๒. **ผู้ดูแลระบบคอมพิวเตอร์** หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายจากผู้อำนวยการศูนย์สารสนเทศอุตสาหกรรมพื้นฐานและการเหมืองแร่ให้ดูแลจัดการระบบคอมพิวเตอร์

๓.๓. **ผู้ดูแลระบบเครือข่าย** หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายจากผู้อำนวยการศูนย์สารสนเทศอุตสาหกรรมพื้นฐานและการเหมืองแร่ให้ดูแลจัดการระบบเครือข่าย

๓.๔. **ผู้ใช้** หมายถึง บุคลากรภายในกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่และ/หรือบุคคลหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้เครือข่ายคอมพิวเตอร์ และ/หรือ ระบบสารสนเทศของ กพร.

๓.๕. **บัญชีชื่อผู้ใช้** หมายถึง ชุดของชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ที่ผู้ดูแลระบบออกให้กับผู้ใช้ เพื่อเข้าใช้งานระบบ

๔. ขอบเขต

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ใช้เพื่อเป็นกรอบและแนวทางให้เจ้าหน้าที่ทางด้านสารสนเทศหรือผู้เกี่ยวข้องจัดเตรียมระบบให้มีความพร้อมในการรักษาความมั่นคงปลอดภัย และเป็นแนวทางที่ผู้ใช้งานภายในองค์กรและบุคคลภายนอกที่เกี่ยวข้องต้องปฏิบัติตาม

๕. แนวปฏิบัติการพิสูจน์ตัวตนผู้ใช้ และการใช้งานรหัสผ่าน

๕.๑. ในการใช้งานระบบใดๆ ที่มีความจำเป็นต้องมีการพิสูจน์เพื่อให้ทราบถึงตัวตนที่แท้จริงของผู้ใช้ ผู้ใช้แต่ละคนต้องมีบัญชีชื่อผู้ใช้ซึ่งประกอบด้วย ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นของตนเอง ห้ามใช้ร่วมกับผู้อื่น

๕.๒. ผู้ใช้มีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนเอง ห้ามทำการเผยแพร่ แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๕.๓. ผู้ใช้ต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากชื่อผู้ใช้ (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้หรือไม่ก็ตาม

๕.๔. ผู้ใช้ต้องตั้งรหัสผ่านให้เกิดความปลอดภัย ดังนี้

๕.๔.๑. ห้ามใช้ชื่อผู้ใช้ (Username) เป็นรหัสผ่าน

๕.๔.๒. มีความยาวของรหัสผ่านไม่น้อยกว่า ๘ อักขระ

๕.๔.๓. มีการผสมกันระหว่างตัวอักษรภาษาอังกฤษ ที่เป็นตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลขอารบิก และสัญลักษณ์พิเศษได้แก่ ! @ #) (/ $ % ^ & * ; + - =

๕.๔.๔. มีการจัดเรียงในลักษณะที่ยากต่อการเดาโดยบุคคลอื่น

๕.๔.๕. ควรเป็นรหัสผ่านที่ผู้ใช้สามารถจดจำได้ง่าย

๕.๔.๖. ไม่ควรใช้ชื่อ หรือนามสกุลของผู้ใช้ ชื่อของบุคคลในครอบครัว หรือชื่อของผู้เกี่ยวข้องกับผู้ใช้เป็นรหัสผ่านซึ่งจะทำให้ง่ายในการเดารหัสผ่าน

๕.๔.๗. ไม่ควรใช้หมายเลขโทรศัพท์ของผู้ใช้ หรือหมายเลขโทรศัพท์ที่เกี่ยวข้องเป็นรหัสผ่าน

๕.๔.๘. ไม่ควรใช้คำศัพท์ในพจนานุกรม

๕.๕. กรณีของการเปลี่ยนรหัสผ่าน นอกจากการตั้งรหัสผ่านให้ปลอดภัยแล้ว ผู้ใช้ต้องไม่ใช้งานรหัสผ่านซ้ำกับรหัสผ่านที่เคยใช้มาแล้ว อย่างน้อย ๓ ครั้ง

๕.๖. ห้ามผู้ใช้จดรหัสผ่าน หรือบันทึกรหัสผ่านเป็นไฟล์ ที่ผู้อื่นสามารถล่วงรู้ได้

๕.๗. ผู้ใช้ต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ระบบสารสนเทศของ กพร. หากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนระงับการใช้งาน หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้ต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๕.๗.๑. การใช้งานอินเทอร์เน็ต (Internet) ผู้ใช้ต้องทำการพิสูจน์ตัวตนก่อนจึงจะได้รับการอนุญาตให้ใช้งานได้

๕.๗.๒. การใช้งานระบบเครือข่ายคอมพิวเตอร์แบบไร้สาย (Wireless LAN) ผู้ใช้ต้องทำการพิสูจน์ตัวตนก่อนจึงจะสามารถใช้งานได้

๕.๗.๓. การใช้งานระบบสารสนเทศที่จำเป็นต้องใช้สิทธิ์ที่ต้องได้รับการอนุญาตก่อน ผู้ใช้ต้องทำการพิสูจน์ตัวตน

๕.๘. สำหรับระบบที่มีความเข้มงวดในการพิสูจน์ตัวตน เช่น การใช้งานลายนิ้วมือ อุปกรณ์โทเค่น (Token) หรือการใช้สมาร์ทการ์ด เป็นต้น ผู้ใช้ต้องระมัดระวังและรักษาความลับของการพิสูจน์ตัวตน เช่นเดียวกับการรักษาความลับของรหัสผ่าน

๕.๙. ระบบการพิสูจน์ตัวตนผู้ใช้ และการใช้งานรหัสผ่านของ กพร.จะมีการตั้งค่าให้มีการระงับการใช้งานบัญชีรายชื่อและรหัสผ่านของผู้ใช้เมื่อไม่มีการใช้งานติดต่อกันนานเกินกว่า ๙๐ วัน และจะมีการลบข้อมูลออกจากระบบเมื่อไม่มีการใช้งานติดต่อกันเกินกว่า ๑ ปี

๖. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยห้องคอมพิวเตอร์แม่ข่าย

๖.๑. ผู้ใช้งานต้องไม่เข้าไปในห้องเซิร์ฟเวอร์ของ กพร. ซึ่งถือว่าเป็นส่วนที่ต้องมีการควบคุมการเข้าถึงเป็นพิเศษ ยกเว้นกรณีที่ได้รับอนุญาตจากผู้ดูแลห้องคอมพิวเตอร์แม่ข่ายแล้วเท่านั้น

๖.๒. การเข้าใช้งานห้องคอมพิวเตอร์แม่ข่ายอนุญาตให้เฉพาะผู้ดูแลห้องคอมพิวเตอร์แม่ข่ายที่ได้รับมอบหมายจาก ผอ.ศสท. เท่านั้น

๖.๓. บุคคลภายนอกที่มีความจำเป็นต้องเข้าให้งานห้องคอมพิวเตอร์แม่ข่ายจะต้องได้รับอนุญาตจากผู้ดูแลห้องคอมพิวเตอร์แม่ข่าย และในขณะปฏิบัติงานจะต้องมีผู้ดูแลห้องคอมพิวเตอร์แม่ข่ายอยู่ด้วยตลอดเวลา

๖.๔. การเข้าใช้งานห้องคอมพิวเตอร์แม่ข่ายต้องมีการบันทึกรายละเอียดการเข้าใช้งานและลงลายมือชื่อทุกครั้ง

๗. แนวปฏิบัติการบริหารจัดการทรัพย์สิน

๗.๑. ผู้ใช้มีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่ กพร. มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้เอง

๗.๒. กรณีทำงานนอกสถานที่ผู้ใช้ต้องดูแลและรับผิดชอบทรัพย์สินของ กพร. ที่ได้รับมอบไว้ให้ใช้งาน

๗.๓. ผู้ใช้มีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้

๗.๔. ผู้ใช้ต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

๗.๕. ทรัพย์สินและระบบสารสนเทศต่างๆ ที่ กพร.จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของ กพร. เท่านั้น ห้ามมิให้ผู้ใช้นำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่ กพร. ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อ กพร.

๗.๖. ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๗.๕ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๘. แนวปฏิบัติการบริหารจัดการข้อมูลองค์กร

๘.๑. ผู้ใช้ต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของ กพร. หรือเป็นข้อมูลของบุคคลภายนอก

๘.๒. ข้อมูลทั้งหมดที่อยู่ภายในทรัพย์สินของ กพร. ถือเป็นสินทรัพย์ของ กพร. ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๘.๓. การใช้งานข้อมูลถือว่าผู้ใช้มีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของ กพร. หากเกิดการสูญหาย นำไปใช้ในทางที่ผิด หรือเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้ต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๘.๔. ผู้ใช้ต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

๘.๕. ผู้ใช้ต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

๘.๖. ผู้ใช้ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลที่อยู่ในความดูแลของผู้ใช้ กพร. จะให้การสนับสนุนและเคารพต่อสิทธิ์ในการปกป้องข้อมูลนั้น

๘.๗. ผู้ใช้มีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กพร. จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้ที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ กพร. ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับ กพร. ซึ่ง กพร. อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้ทราบ

๙. แนวปฏิบัติการบริหารจัดการระบบสารสนเทศ

๙.๑. ผู้ใช้มีสิทธิ์ที่จะพัฒนาโปรแกรม ระบบสารสนเทศ หรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

๙.๑.๑. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

๙.๑.๒. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

๙.๑.๓. พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๙.๑.๔. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

๙.๑.๕. กรณีที่ผู้ใช้นำเสนอข้อมูลบนเครือข่ายคอมพิวเตอร์ จะต้องไม่นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม

๙.๒. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของ กพร. ที่จัดเตรียมให้เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของ กพร.

๙.๓. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของ กพร. ที่จัดเตรียมให้เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของ กพร.

๙.๔. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของ กพร. ที่จัดเตรียมให้เพื่อประโยชน์ทางการค้า

๙.๕. ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของ กพร. โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

๙.๖. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของ กพร. ต้องหยุดชะงัก

๙.๗. ห้ามใช้ระบบสารสนเทศของ กพร. เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๙.๘. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๙.๙. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของ กพร. โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๑๐. แนวปฏิบัติการใช้งานซอฟต์แวร์ และลิขสิทธิ์

๑๐.๑. กพร. ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่ กพร. จัดหา หรืออนุญาตให้ใช้งาน หรือที่ กพร. มีลิขสิทธิ์ ผู้ใช้สามารถขอใช้งานได้ตามหน้าที่ หรือตามความจำเป็น

๑๐.๒. ซอฟต์แวร์ที่ กพร. ได้จัดเตรียมไว้ให้ผู้ใช้ ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้ทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๑๐.๓. กพร. ห้ามไม่ให้ผู้ใช้ทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ กพร. ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้จะต้องรับผิดชอบแต่เพียงผู้เดียว

๑๑. แนวปฏิบัติการป้องกันไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดี

๑๑.๑. คอมพิวเตอร์ของผู้ใช้ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti Virus) และโปรแกรมไม่ประสงค์ดี ดังนี้

๑๑.๑.๑. โปรแกรมป้องกันไวรัสให้ใช้ซอฟต์แวร์ Symantec Endpoint Protection

๑๑.๑.๒. โปรแกรมป้องกันไม่ประสงค์ดีที่มากับอุปกรณ์ USB ให้ติดตั้งซอฟต์แวร์ CPE Autorun Killer

๑๑.๒. ผู้ใช้จะต้องทำการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีกับข้อมูล ไฟล์ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้อื่น ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๑๑.๓. ผู้ใช้ต้องทำการอัพเดทโปรแกรมป้องกันไวรัส และอัพเดทระบบปฏิบัติการ ให้เป็นปัจจุบันอยู่เสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากไวรัส และโปรแกรมไม่ประสงค์ดี

๑๑.๔. ผู้ใช้ต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้ต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๑๑.๕. เมื่อผู้ใช้พบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้ต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

๑๑.๖. ผู้ใช้ควรระมัดระวัง และตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีจากการใช้งานสื่อบันทึกข้อมูลแบบพกพาต่างๆ เช่น ฟลอปปี้ดิสค์ (Floppy Disk) แฟลชไดรว์ (Flash Drive) หรือ ฮาร์ดดิสก์แบบพกพา เป็นต้น

๑๑.๗. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ โปรแกรมไม่ประสงค์ดี หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายกับระบบสารสนเทศของ กพร.

๑๑.๘. ผู้ใช้ควรระมัดระวัง และควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนการใช้งาน

๑๒. แนวปฏิบัติการสำรองและการกู้คืนข้อมูลของผู้ใช้

๑๒.๑. ผู้ใช้ต้องสำรองข้อมูลบนอุปกรณ์คอมพิวเตอร์ที่ผู้ใช้รับผิดชอบ ไว้บนสื่อบันทึกอื่นๆ เช่น แผ่นซีดี แผ่นดีวีดี แฟลชไดรว์ (Flash Drive) หรือ ฮาร์ดดิสก์แบบติดตั้งภายนอก เป็นต้น เพื่อป้องกันการสูญหายของข้อมูล

๑๒.๒. ผู้ใช้มีหน้าที่เก็บรักษาสื่อที่ใช้บันทึกข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๒.๓. สื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำข้อมูลกลับมาใช้งานได้อีก

๑๓. แนวปฏิบัติการใช้งานเครือข่ายไร้สาย

๑๓.๑. ห้ามหน่วยงานหรือบุคลากรภายใน กพร. หรือบุคคลภายนอก ทำการติดตั้งอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบไร้สาย (Wireless Access Point) ภายใน กพร.

๑๓.๒. บุคลากรภายใน กพร. ให้ใช้เฉพาะอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบไร้สายที่ทาง กพร. จัดเตรียมไว้เท่านั้น หากหน่วยงานหรือบุคลากรภายใน กพร. มีความประสงค์จะใช้งานอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบไร้สายเพิ่มเติมต้องแจ้งให้ทาง ศสท. ทราบ และเป็นผู้ดำเนินการติดตั้ง

๑๓.๓. บริการเครือข่ายไร้สาย (SSID) ที่ กพร. เปิดให้บริการมี ดังนี้

๑๓.๓.๑. บริการเครือข่ายไร้สายสาย (SSID) DPIM-WIFI

๑๓.๓.๑.๑. ใช้สำหรับเชื่อมต่ออุปกรณ์คอมพิวเตอร์แบบไร้สาย (Wireless LAN) ที่ต้องการการรักษาความมั่นคงปลอดภัยสูง และใช้งานร่วมกับเครือข่ายคอมพิวเตอร์ภายใน (LAN)

๑๓.๓.๑.๒. การเชื่อมต่อกับระบบเครือข่ายไร้ ใช้การรักษาความปลอดภัยแบบ WPA2-Enterprise ใช้การเข้ารหัสข้อมูลแบบ TKIP และใช้กระบวนการตรวจสอบตัวตนแบบ PEAP

๑๓.๓.๑.๓. การเชื่อมต่อกับระบบเครือข่ายไร้สาย ผู้ใช้จะต้องพิสูจน์ตัวตนผู้ใช้โดยใช้บัญชีชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของระบบเมล์ที่ได้ลงทะเบียนไว้กับทาง ศสท.

๑๓.๓.๒. บริการเครือข่ายไร้สายสาย (SSID) DPIM-REGIST

๑๓.๓.๒.๑. ใช้สำหรับอุปกรณ์ไร้สายที่ไม่สามารถใช้งาน DPIM-WIFI ได้ (อุปกรณ์โทรศัพท์มือถือ เครื่องพิมพ์ เป็นต้น)

๑๓.๓.๒.๒. ผู้ใช้จะต้องลงทะเบียนอุปกรณ์กับ ศสท. ก่อนจึงจะสามารถใช้งานได้

๑๓.๓.๒.๓. ระดับการเข้าถึงระบบเครือข่ายขึ้นอยู่กับการขออนุญาตในตอนลงทะเบียนอุปกรณ์กับ ศสท.

๑๓.๓.๓. บริการเครือข่ายไร้สายสาย (SSID) DPIM-GUEST

๑๓.๓.๓.๑. ใช้สำหรับให้บริการกับบุคลากรภายนอก

๑๓.๓.๓.๒. ผู้ใช้จะต้องลงทะเบียน ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) กับทาง ศสท. ก่อนจึงจะสามารถใช้งานได้

๑๓.๓.๓.๓. อนุญาตให้ใช้บริการเชื่อมต่อเข้าสู่เครือข่ายอินเตอร์เน็ตตามระยะเวลาที่กำหนดให้เท่านั้น ไม่อนุญาตให้เชื่อมต่อเข้าใช้งานเครือข่ายภายในของ กพร. (LAN) ได้

๑๔. แนวปฏิบัติการใช้งานไฟร์วอลล์

๑๔.๑. เครือข่ายคอมพิวเตอร์ของ กพร. อยู่ภายใต้การรักษาความปลอดภัยของไฟร์วอลล์ ผู้ใช้สามารถใช้บริการการเชื่อมต่อเครือข่ายเฉพาะที่ไฟร์วอลล์อนุญาตให้ใช้งานเท่านั้น โดยมีบริการที่อนุญาตให้ใช้งานได้ดังนี้ HTTP, HTTPS, MSN, Yahoo Messenger, RTSP

๑๔.๒. ในกรณีที่ผู้ใช้มีความจำเป็นต้องใช้งานบริการ หรือเปิดพอร์ตการเชื่อมต่อนอกเหนือจากที่กำหนด ผู้ใช้สามารถขอให้มีการเปิดพอร์ตการเชื่อมต่อได้ โดยมีข้อกำหนดดังนี้

๑๔.๒.๑. ผู้ขอใช้งานต้องยอมรับ และปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยอย่างเคร่งครัด

๑๔.๒.๒. วัตถุประสงค์ในการขอใช้งานจะต้องไม่ขัดต่อนโยบาย ประกาศ ระเบียบต่างๆ ของ กพร. และต่อกฎหมายที่เกี่ยวข้อง

๑๔.๒.๓. ผู้ขอใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษรต่อ ผอ.ศสท. โดยระบุข้อมูลดังนี้

๑๔.๒.๓.๑. วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งาน

๑๔.๒.๓.๒. หมายเลข IP ของเครื่องคอมพิวเตอร์ที่ผู้ใช้จะใช้ในการ เชื่อมต่อ

๑๔.๒.๓.๓. หมายเลย IP ของปลายทางที่ต้องการติดต่อสื่อสาร

๑๔.๒.๓.๔. หมายเลขพอร์ตที่ต้องการขอเปิดใช้

๑๔.๒.๓.๕. วันที่เริ่มใช้ และวันที่สิ้นสุดการใช้

๑๔.๓. ไฟร์วอลล์อนุญาตให้ผู้ใช้สามารถติดต่อกับเซิร์ฟเวอร์ได้เฉพาะบริการที่เซิร์ฟเวอร์เปิดให้บริการเท่านั้น

๑๔.๔. ผู้ดูแลระบบหรือผู้ใช้ที่มีความจำเป็นต้องใช้งานเซิร์ฟเวอร์นอกเหนือจากบริการปกติจะต้องลงทะเบียนขออนุญาตการใช้งานเป็นลายลักษณ์อักษรก่อนจึงจะสามารถใช้งานได้

๑๕. แนวปฏิบัติการใช้งานพร็อกซี่

๑๕.๑. ผู้ใช้ภายใน กพร. ไม่อนุญาตให้เชื่อมต่อกับเครือข่ายอินเตอร์เน็ตโดยตรง

๑๕.๒. ผู้ใช้ภายใน กพร. สามารถเชื่อมต่ออินเตอร์เน็ตได้โดยผ่านพร็อกซี่เซิร์ฟเวอร์ โดยมีการตั้งค่าดังนี้

๑๕.๒.๑. ชื่อพร็อกซี่เซิร์ฟเวอร์ (Proxy Server) proxy.dpim.go.th

๑๕.๒.๒. พอร์ตที่ใช้ในการเชื่อมต่อ (Port) 8080

๑๕.๓. ผู้ใช้จะต้องพิสูจน์ตัวตนผู้ใช้โดยใช้บัญชีชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของระบบเมล์ที่ได้ลงทะเบียนไว้กับทาง ศสท.

๑๕.๔. กพร. มีการจัดเก็บข้อมูลการจราจรบนเครือข่ายคอมพิวเตอร์ที่วิ่งผ่านพร็อกซี่เซิร์ฟเวอร์ที่สามารถระบุตัวตนผู้ใช้และปลายทางซึ่งเป็นไปตาม พรบ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๖. แนวปฏิบัติการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

๑๖.๑. ผู้ใช้จะต้องลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) กับทาง ศสท. ก่อนจึงจะสามารถใช้งานได้

๑๖.๒. เมื่อผู้ใช้ได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้ควรเปลี่ยนรหัสผ่าน (Password) โดยทันที

๑๖.๓. ผู้ใช้ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

๑๖.๔. ควรเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๓-๖ เดือน

๑๖.๕. การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้ต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๑๖.๖. การส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ให้กับผู้รับบริการ คู่สัญญา หรือตามภารกิจของ กพร. ผู้ใช้ควรใช้ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของ กพร. เท่านั้น ไม่ควรใช้ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของ กพร. ขัดข้อง

๑๖.๗. ผู้ใช้ไม่ควรนำที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ซึ่งเป็นของ กพร. ไปเผยแพร่สู่บุคคลอื่น ไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในเว็บบอร์ดในชุดคำถามหรือแบบสอบถามจากผู้ค้า เป็นต้น เว้นแต่การเผยแพร่นั้นเป็นไปเพื่อผลประโยชน์ทางราชการของ กพร. หรือได้รับอนุญาตจากผู้มีอำนาจแล้วเท่านั้น

๑๖.๘. การส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้ต้องระบุชื่อผู้รับ หัวข้อ ให้ชัดเจน และใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ปลุกปั่น ยั่วยุ เสียดสี หรือส่อในทางผิดกฎหมาย

๑๖.๙. ผู้ใช้ต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของ กพร. หรือก่อให้เกิดความเสียหายต่อ กพร.

๑๖.๑๐. ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

๑๖.๑๑. ไม่ควรใช้บัญชีรายชื่อจดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับ-ส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ และให้ถือว่าเจ้าของบัญชีรายชื่อจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์นั้น

๑๖.๑๒. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรล็อคเอาท์ออกจากระบบทุกครั้ง

๑๖.๑๓. ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของ กพร. เพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมายหรือกระทบต่อการดำเนินงานของ กพร. ตลอดจนเป็นการรบกวนผู้ใช้อื่น รวมทั้งผู้รับบริการของ กพร.

๑๗. แนวปฏิบัติการใช้งานเครือข่ายอินเตอร์เน็ต

๑๗.๑. ผู้ใช้ต้องเป็นบุคลากรสังกัด กพร. ที่ได้ลงทะเบียนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของระบบเมล์ที่ได้ลงทะเบียนไว้กับทาง ศสท.

๑๗.๒. ผู้ใช้ที่เป็นบุคคลภายนอกจะต้องลงทะเบียนกับทาง ศสท. ก่อน จึงจะสามารถใช้งานได้

๑๗.๓. ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ตก่อนนำข้อมูลมาใช้งาน

๑๗.๔. ผู้ใช้ต้องใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่หากมีความจำเป็นให้ดำเนินการนอกเวลาทำงาน

๑๗.๕. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit torrent) อีมูล (e-mule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๑๗.๖. ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

๑๗.๗. ผู้ใช้ต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีชื่อผู้ใช้ของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีต้องเป็นรับผิดชอบ

๑๗.๘. ห้ามผู้ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

๑๗.๙. ห้ามผู้ใช้ทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๑๗.๑๐. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑๗.๑๑. ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลด การอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

๑๗.๑๒. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๑๗.๑๓. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๑๗.๑๔. หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดโปรแกรมเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๑๘. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๑๘.๑. เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ ผู้ใช้ ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร

๑๘.๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๘.๓. ไม่อนุญาตให้ ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร

๑๘.๔. การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลควรดำเนินการโดยเจ้าหน้าที่ ศสท. เท่านั้น

๑๘.๕. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลเพื่อตรวจซ่อมควรจะต้องดำเนินการโดยเจ้าหน้าที่ของ ศสท. หรือในกรณีที่หน่วยงานเจ้าของเครื่องคอมพิวเตอร์ส่วนบุคคลต้องการดำเนินการเองควรได้รับความเห็นชอบจาก ศสท. ก่อนการดำเนินการ

๑๘.๖. ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๑๘.๗. เพื่อรักษาความปลอดภัยของคอมพิวเตอร์จากการใช้งานที่ไม่ถูกต้อง ผู้ใช้ควรมีการตั้งค่ารหัสผ่านในการเข้าใช้งาน และตั้งค่ารหัสผ่านการล็อคหน้าจอเมื่อไม่มีการใช้เกินกว่า ๑๐ นาที

๑๘.๘. เมื่อผู้ใช้ใช้งานคอมพิวเตอร์ส่วนบุคคลเสร็จแล้วหรือมีความจำเป็นต้องลุกจากเครื่องคอมพิวเตอร์ ผู้ใช้ควรทำการออกจากระบบ (Logoff) หรือล็อคหน้าจอเพื่อป้องกันการใช้งานจากบุคคลอื่น

๑๙. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๑๙.๑. เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ ผู้ใช้ ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร

๑๙.๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๙.๓. การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพาควรดำเนินการโดยเจ้าหน้าที่ ศสท. เท่านั้น

๑๙.๔. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาเพื่อตรวจซ่อมควรจะต้องดำเนินการโดยเจ้าหน้าที่ของ ศสท. หรือในกรณีที่หน่วยงานเจ้าของเครื่องคอมพิวเตอร์แบบพกพาต้องการดำเนินการเองควรได้รับความเห็นชอบจาก ศสท. ก่อนการดำเนินการ

๑๙.๕. ผู้ใช้ ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๑๙.๖. ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๑๙.๗. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๑๙.๘. ห้ามใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

๑๙.๙. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑๙.๑๐. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่นปลายปากกา กดสัมผัสหน้าจอให้เป็นรอยขีดข่วนหรือทำให้จอของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑๙.๑๑. ห้ามวางของทับบนหน้าจอและแป้นพิมพ์

๑๙.๑๒. การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๙.๑๓. ห้ามเคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

๑๙.๑๔. ห้ามใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น

๑๙.๑๕. ห้ามใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส

๑๙.๑๖. ห้ามวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๑๙.๑๗. ห้ามติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน เช่นในยานพาหนะที่กำลังเคลื่อนที่

๑๙.๑๘. การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าที่มีรอยขีดข่วนได้