# ภาคผนวก

# ภาคผนวก ก

# แบบสอบถาม ความรู้ ความเข้าใจ การรักษาความมั่นคงปลอดภัยสารสนเทศ

**แบบสอบถามความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยสารสนเทศ**

กระผม จ.ส.อ.ศรวัสย์ สนธิ นักศึกษา มหาวิทยาลัยธุรกิจบัณฑิตย์ จึงใคร่ขอความร่วมมือ ตอบแบบสอบถาม เกี่ยวกับ ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของ กองบัญชาการกองทัพไทย เพื่อเป็นข้อมูลในการทำวิจัยสารนิพนธ์ ทั้งนี้ข้อมูลที่ได้จากการตอบแบบสอบถามในงานวิจัยนี้อาจเป็นประโยชน์แก่ผู้ศึกษาค้นคว้าต่อไปได้

**<u>ส่วนที่ 1</u>** ข้อมูลส่วนบุคคลทั่วไป

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงใน ❒ หรือเติมข้อความลงในช่องว่างตรงตามความเป็นจริง

1. เพศ

❒ 1. ชาย ❒ 2. หญิง

2. อายุ

❒ 1. ต่ำกว่า 20 ปี ❒ 2. ตั้งแต่ 21 ปี ถึง 30 ปี

❒ 3. ตั้งแต่ 31 ปี ถึง 40 ปี ❒ 4. ตั้งแต่ 41 ปี ถึง 50 ปี

❒ 5. ตั้งแต่ 51 ปี ขึ้นไป

3. ระดับการศึกษา

❒ 1. ระดับมัธยมศึกษาตอนต้น ❒ 2. ระดับมัธยมศึกษาตอนปลาย

❒ 3. ระดับประกาศนียบัตรวิชาชีพ ❒ 4. ระดับประกาศนียบัตรวิชาชีพชั้นสูง

❒ 5. ระดับปริญญาตรี ❒ 6. ระดับปริญญาโทขึ้นไป

4. ระดับหน้าที่ทำงาน

❒ 1. ระดับข้าราชการชั้นสัญญาบัตร ❒ 2. ระดับข้าราชการชั้นประทวน

❒ 3. ระดับข้าราชการลูกจ้างพนักงานราชการ

5. เคยได้รับการฝึกอบรม หลักสูตร การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือไม่

❒ 1. เคยผ่านหลักสูตร ❒ 2. ไม่เคยผ่านหลักสูตร

**<u>ส่วนที่ 2</u> พฤติกรรมการใช้ระบบอินทราเน็ตและอินเตอร์เน็ตภายในองค์กร**

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงใน ❒ หรือเติมข้อความลงในช่องว่างตรงตามความเป็นจริง

1. ปัจจุบันท่านใช้คอมพิวเตอร์สำนักงานหรือของส่วนตัว

❒ สำนักงาน ❒ ส่วนตัว

2. คอมพิวเตอร์ของท่านมีคนอื่นใช้นอกจากท่านหรือไม่

❒ ใช้ ❒ ไม่ใช้

3. ท่านเคยนำอุปกรณ์สื่อสารชนิดอื่นๆ มาเชื่อมต่อในเครือข่าย กองบัญชาการกองทัพไทย หรือไม่ และเป็นอุปกรณ์ชนิดใด

❒ เคยนำเชื่อมต่อ อุปกรณ์ชนิด ..... ❒ ไม่เคยเชื่อมต่อ

4. ท่านใช้คอมพิวเตอร์ในการทำงานระบบอินทราเน็ตและอินเตอร์เน็ตใน กองบัญชาการกองทัพไทย ในเรื่องใดบ้าง (ตอบได้มากกว่า 1 ข้อ)

❒ 1. พิมพ์งานเอกสาร ❒ 2. จัดเก็บข้อมูล
❒ 3. ดูหนังฟังเพลง ❒ 4. Download ข้อมูล
❒ 5. ค้นหาข้อมูล ❒ 6. ใช้ Email
❒ 7. ท่องเว็บไซต์ ❒ 8. อ่านข่าวสาร
❒ 9. Social Network ❒ 10. เล่น Game
❒ 11. ซื้อขาย online ผ่านInternet ❒ 12. อื่นๆ ระบุ .....

**<u>ส่วนที่ 3</u> แบบทดสอบความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ**

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงใน ❒ หรือเติมข้อความลงในช่องว่างตรงตามความเป็นจริง

3.1 แบบทดสอบความรู้การรักษาความปลอดภัยสารสนเทศเกี่ยวกับข้อมูล

1) คอมพิวเตอร์ที่ดีควรเข้ารหัสเพื่อป้องกันผู้อื่นอย่างไร

❒ มั่นตั้งรหัสอย่างน้อย 8 ตัวอักษร ทั้งตัวหนังสือและตัวเลข
❒ ตั้งรหัสที่ง่ายต่อการจำของตัวเอง
❒ ตั้งรหัสและจดบันทึกเอาไว้

2) มาตรฐานเกี่ยวข้องกับการบริหารการ รักษาความปลอดภัยข้อมูล และเป็นแนวทางในการสร้าง ดูแล และปรับปรุงระบบบริหารการรักษาความปลอดภัยคือ ISO/IEC

❒ ISO/IEC 17025
❒ ISO/IEC 27001
❒ ISO/IEC 20000

3) ข้อมูลทางคอมพิวเตอร์ในปัจจุบันของท่านถูกจัดเก็บอย่างไร

❒ จัดเก็บเป็นระเบียบ แยกหมวดหมู่ ง่ายต่อการค้นหา
❒ ไม่ได้จัดเก็บเป็นระเบียบข้อมูลจัดวางไว้หน้า Desktop
❒ จัดเก็บไว้ในที่อื่น ๆ .....

4) เมื่อคอมพิวเตอร์ของท่านเสียมีการส่งซ่อมควรทำอย่างไร

❒ Backup Data และลบข้อมูลออกก่อนส่งซ่อม
❒ ส่งซ่อมกับเจ้าหน้าที่ซ่อมบำรุง
❒ ส่งซ่อมกับช่างผู้ชำนาญตามร้านเอง

5) ท่านตั้งแชร์ข้อมูลผ่ายระบบเครือข่ายอย่างไร

❒ แบบ Full อ่านและเขียนได้ ❒ แบบ อ่านได้อย่างเดียว
❒ แบบ อ่านได้อย่างเดียวและตั้งรหัสในการแชร์ข้อมูล

3.2 แบบทดสอบความรู้การรักษาความปลอดภัยสารสนเทศเกี่ยวกับการป้องกัน Virus และช่องโหว่ด้านต่าง ๆ

1) คอมพิวเตอร์ของท่านมี โปรแกรม Antivirus ที่เจ้าหน้าที่ติดตั้งของอะไร

- ❒ Nod32 Antivirus
- ❒ AVG Antivirus
- ❒ McAfee Antivirus
- ❒ AVIRA Antivirus
- ❒ อื่น ๆ ระบุ .....

2) เมื่อท่านนำ Flash drive ไป Save งานแล้วนำมาเปิดที่เครื่องของท่านควรปฏิบัติอย่างไร

- ❒ Scan Virus ก่อนเปิดทุกครั้ง
- ❒ เสียบแล้วเปิดทันที
- ❒ นำไปเสียบเครื่องอื่นก่อน เพื่อให้มั่นใจว่าไม่มี Virus
- ❒ ถามเจ้าของ Flash drive หรือ เครื่องคอมพิวเตอร์ที่นำไม่ Save งานว่ามีหรือไม่ เพื่อมั่นใจ ก่อนเปิดงานทันที

3) มัลแวร์ (Malware) คืออะไร

- ❒ โปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์
- ❒ โปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่ถูกออกแบบมาให้แพร่กระจาย
- ❒ โปรแกรมที่สามารถคัดลอกตัวเองและสามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ
- ❒ โปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่น ๆ

4) Backdoor คืออะไร

- ❒ รูรั่วในการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่ผู้ออกแบบหรือผู้ดูแลจงใจทิ้งไว
- ❒ ซอฟต์แวร์ที่ออกแบบเพื่อสร้างความสนุกสนาน แต่ก็ทาให้เสียเวลาการทำงานของระบบคอมพิวเตอร์
- ❒ พยายามหลอกล่อให้เหยื่อจ่ายเงินหรือโอนเงิน และมีเทคนิคหลอกลวงที่สมบูรณ์แบบ
- ❒ ประตูหลังของช่องทางที่ให้ Virus เข้าไปโจมตีทำให้คอมเสียหาย

5) สปายแวร์ (Spyware) คืออะไร

- ❒ โปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่ถูกออกแบบมาให้แพร่กระจาย
- ❒ โปรแกรมที่ใช้บางอย่างเพื่อลวงตาแต่ทากิจกรรมบางอย่างในเครื่องคอมพิวเตอร์
- ❒ โปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่น ๆ
- ❒ โปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์

3.3 แบบทดสอบความรู้การรักษาความปลอดภัยสารสนเทศเกี่ยวกับด้านกฎหมาย ว่าด้วย การกระทำผิด พรบ. เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นโยบาย และระเบียบ ของกองบัญชาการกองทัพไทย เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

1) พรบ. คอมพิวเตอร์ พ.ศ.2550 มีทั้งหมดกี่หมวด

❒ 1 หมวด ❒ 2 หมวด

❒ 3 หมวด ❒ 4 หมวด

2) ผู้ใดเข้าโดยมิชอบ ซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ต้องโทษอย่างไร

❒ จำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

3) ผู้ใดเข้าโดยมิชอบ ซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ต้องโทษอย่างไร

❒ จำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จ โดยเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

❒ จำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

❒ จำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

5) ระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ ของกองทัพไทย ออกใช้เมื่อไร

❒ 14 ก.พ.2547

❒ 23 ก.พ.2547

❒ 10 มิ.ย.2550

❒ 24 มี.ค.2552

**<u>ส่วนที่ 4</u> แบบทดสอบพฤติกรรมเสี่ยงต่อภัยคุกคามต่อเครือข่ายภายใน กองบัญชาการกองทัพไทย**
คำชี้แจง โปรดทำเครื่องหมาย ✓ เลือกคำตอบตรงตามความเป็นจริง

| ลำดับ | ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยสารสนเทศ | การปฏิบัติ | |
|---|---|---|---|
| | | เคย | ไม่เคย |
| 1. | ท่านเคยจดบันทึกรหัสผ่านเพื่อง่ายต่อการจดจำใกล้บริเวณโต๊ะคอมพิวเตอร์หรือไม่ | | |
| 2. | ท่านเคย Backupไฟล์ข้อมูลอยู่อย่างสม่ำเสมอหรือไม่ | | |
| 3. | ท่านเคยส่งซ่อมคอมพิวเตอร์โดยไม่ Backup ข้อมูลออกก่อน | | |
| 4. | ท่านเคยแชร์ไฟล์ข้อมูลที่สำคัญโดยเข้ารหัสหรือไม่ | | |
| 5. | ท่านเคยแชร์ข้อมูลผ่านเครือข่ายแบบ อ่านได้เขียนได้ | | |
| 6. | ท่านเคยใช้ Free Email ในเครือข่ายกองบัญชาการกองทัพไทย | | |
| 7. | ท่านเคยใช้คอมพิวเตอร์ดาวน์โหลด โปรแกรมฟรีแวร์ จากเว็บไซต์อินเตอร์เน็ตมาติดตั้งหรือไม่ | | |
| 8. | ท่านเคยศึกษานโยบายการป้องกัน Virus บนคอมพิวเตอร์ขององค์กรหรือไม่ | | |
| 9. | ท่านเคยนำ USB flash drive ไปใช้กับคอมพิวเตอร์ ที่ไม่มีระบบป้องกัน Antivirus | | |
| 10. | ท่านเคยศึกษาวิธีป้องกันเกี่ยวกับภัยคุกคามเพื่อป้องกันภัยจากคอมพิวเตอร์ ในระบบสารสนเทศ | | |

**<u>ส่วนที่ 5</u> ความคิดเห็นและข้อเสนอแนะอื่น ๆ เกี่ยวกับเรื่องระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กองบัญชาการกองทัพไทย**

.....

.....

.....

.....

.....

.

ขอขอบคุณสำหรับความร่วมมือมา ณ ที่นี้

# ภาคผนวก ข

## ระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัย ระบบสารสนเทศ ของ กองบัญชาการกองทัพไทย พ.ศ.2547

ระเบียบ กองบัญชาการทหารสูงสุด
วาดวยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย
พ.ศ.๒๕๔๗

---

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทยเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ จึงวางระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย พ.ศ.๒๕๔๗”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ บรรดาระเบียบ และคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับระเบียบนี้ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ และลูกจ้างที่มีการปฏิบัติเกี่ยวกับ ระบบสารสนเทศ รวมทั้ง บุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของ กองบัญชาการทหารสูงสุด และเหล่าทัพ

ข้อ ๕ ในระเบียบนี้

๕.๑ ระบบสารสนเทศ (Information System) หมายความว่า ระบบข่าวสารของ กองทัพไทย ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์ และระบบสื่อสาร มาช่วยในการสร้างสารสนเทศ ของกองทัพไทย และสามารถนำข่าวสารมาใช้ในการวางแผน การบริหาร การพัฒนา และควบคุมซึ่งมีองค์ประกอบดังนี้

๕.๑.๑ ระบบคอมพิวเตอร์ (Computer System) หมายถึง ระบบที่ประกอบด้วยฮาร์ดแวร์ (Hardware) ซอฟตแวร์ (Software) และบุคลากรทางคอมพิวเตอร์ (Peopleware)

๕.๑.๒ ระบบสื่อสาร (Communication System) หมายความว่า ระบบที่ประกอบด้วยผู้รับ ผู้ส่งและสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล ทั้งระบบวงจรทางสาย และระบบไร้สาย รวมถึงอุปกรณ์ต่อพวงอื่น ๆ เช่น Hub, Switching, Router เป็นต้น

๕.๑.๓ สารสนเทศ (Information) ข้อเท็จจริงที่ได้จากการสกัดข้อมูลให้มีความหมายโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความหรือ

/ภาพกราฟฟิก ...

ภาพกราฟฟิกที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๕.๒ เครือข่ายระบบสารสนเทศ หมายความว่า การติดต่อสื่อสาร หรือการส่งข้อมูลกันระหว่างระบบสารสนเทศภายใน บก.ทหารสูงสุด, เหล่าทัพ และการติดต่อสื่อสาร หรือการส่งข้อมูลกันระหว่าง เหล่าทัพ กับ บก.ทหารสูงสุด

ข้อ ๖ ให้ เจ้ากรมการสนเทศทหาร กองบัญชาการทหารสูงสุด เป็นผู้รักษาการให้เป็นไปตามระเบียบนี้

**หมวด ๑**

**กล่าวทั่วไป**

ข้อ ๗ ความมุ่งหมายของระเบียบนี้

๗.๑ เพื่อกำหนดหลักการและมาตรการในการรักษาความปลอดภัยระบบสารสนเทศ ของ กองทัพไทย

๗.๒ พิทักษ์รักษาและป้องกัน มิให้ข้อมูลและสิ่งที่เป็นความลับของทางราชการรั่วไหลหรือรู้ไปถึง หรือตกไปอยู่ในมือของฝ่ายตรงข้ามหรือบุคคลผู้ไม่มีอำนาจหน้าที่

๗.๓ ป้องกันการจารกรรมทั้งจากบุคคลภายในและภายนอกส่วนราชการ

๗.๔ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่เครื่องจักรคำนวณ อุปกรณ์เครื่องใช้ อาคาร สถานที่ และเอกสาร เป็นต้น

ข้อ ๘ หัวหน้าส่วนราชการสามารถกำหนดมาตรการรักษาความปลอดภัยให้ระบบสารสนเทศของส่วนราชการ และแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการเพิ่มเติมได้โดยให้สอดคล้องและไม่ขัด หรือแย้งกับระเบียบนี้

ข้อ ๙ เหตุผลในการประกาศใช้ระเบียบนี้ คือ วางระเบียบกองบัญชาการทหารสูงสุดในการรักษาความปลอดภัยระบบสารสนเทศของ กองทัพไทย เกี่ยวกับระบบคอมพิวเตอร์, ระบบสื่อสาร, สารสนเทศเครือข่ายระบบสารสนเทศ เพื่อให้ใช้บังคับแก่ส่วนราชการ ข้าราชการและลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอก ที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศ ของ กองบัญชาการทหารสูงสุด และเหล่าทัพ

ข้อ ๑๐ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พรบ. ข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ หรืออื่น ๆ ที่ได้ประกาศใช้ทดแทน

/หมวด ๒ ...

**หมวด ๒**

**การรักษาความปลอดภัยเกี่ยวกับบุคคล**

ข้อ ๑๑ ความมุ่งหมาย เพื่อเป็นการคัดเลือด ให้ได้บุคคลที่มีลักษณะเหมาะสมแก่การบรรจุใน อัตราที่เกี่ยวกับการปฏิบัติหน้าที่ที่ระบบสารสนเทศ และเพื่อกำหนดระดับความไว้วางใจในการมอบหมายหน้าที่เกี่ยวกับความลับของทางราชการ ตลอดจนควบคุมบุคคลที่ไม่เกี่ยวข้องและหรือบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับระบบสารสนเทศ

ข้อ ๑๒ บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

ข้อ ๑๓ หัวหน้าส่วนราชการ จะต้องจัดให้มีการควบคุม ดูแล และตรวจสอบสิทธิ์การเข้าถึงระบบสารสนเทศอย่างเข็มงวด โดยคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก

**หมวด ๓**

**การรักษาความปลอดภัย สถานที่**

ข้อ ๑๔ การรักษาความปลอดภัยเกี่ยวกับสถานที่ของระบบสารสนเทศให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ โดย

๑๔.๑ ส่วนราชการกำหนดมาตรการรักษาความปลอดภัยสถานที่จากการเข้าถึงโดยการได้ยิน และการมองเห็นของผู้ไม่มีอำนาจหน้าที่

๑๔.๒ ส่วนราชการกำหนดพื้นที่รักษาความปลอดภัยแบ่งเขตหวงห้ามเฉพาะเขตหวงห้ามเด็ดขาด ให้เหมาะสม

ข้อ ๑๕ ส่วนราชการจะต้องจัดทำแผนสำหรับเตรียมรับสถานการณ์ต่าง ๆ ได้แก่ แผนป้องกันระบบสารสนเทศ แผนการดำเนินการฟื้นฟูระบบคอมพิวเตอร์ แผนการเคลื่อนย้ายและแผนการทำลายระบบสารสนเทศในเวลาจำเป็นให้พร้อมที่จะปฏิบัติหน้าที่ได้ทันท่วงที และจัดให้มีการซักซ้อมความเข้าใจอย่างสม่ำเสมอ

ข้อ ๑๖ ส่วนราชการควรจัดให้มีสถานที่สำรองในการดำเนินการระบบสารสนเทศ

**หมวด ๔**

**การรักษาความปลอดภัยระบบสารสนเทศ**

ข้อ ๑๗ ส่วนราชการจะต้องจัดให้มีมาตรการรักษาความปลอดภัยระบบสารสนเทศที่เหมาะสม และดำเนินการตามมาตรการนั้นโดยเคร่งครัด เพื่อให้เกิดความปลอดภัยสูงสุดต่อระบบสารสนเทศ

/ข้อ ๑๘ ...

ข้อ ๑๘ ส่วนราชการต้องจัดทำระบบสำรองและการกู้คืนสภาพข้อมูลสารสนเทศตามวงรอบที่เหมาะสมและทันสมัยที่สุด

ข้อ ๑๙ ส่วนราชการต้องจัดให้มีแผนการสำรองและแผนการกู้คืนสภาพระบบสารสนเทศและทดสอบอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒๐ ต้องจัดให้มีแผนการรักษาและป้องกันความลับของข้อมูล

๒๐.๑ ต้องไม่เข้าถึงข้อมูลผู้อื่น โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

๒๐.๒ ห้ามทำการพิมพ์หรือทำสำเนาข้อมูลที่เป็นชั้นความลับ เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๒๐.๓ ต้องมีการกำหนดผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์ในระบบสารสนเทศของหน่วย

ข้อ ๒๑ การรักษาความปลอดภัยเกี่ยวกับเครือข่ายคอมพิวเตอร์

๒๑.๑ ส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิ์และอำนาจในสายงาน ที่มีการติดต่อแลกเปลี่ยนสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์เป็นผู้พิจารณาคุณสมบัติของผู้ใช้ที่ได้รับอนุญาตให้เข้าถึงและดำเนินการกับสารสนเทศดังกล่าว รวมทั้งพิจารณาระดับการป้องกันที่ต้องการ

๒๑.๒ การส่งข้อมูลที่มีชั้นความลับผ่านเครือข่ายคอมพิวเตอร์ จะต้องได้รับอนุมัติจากผู้มีสิทธิ์และอำนาจในสายงานที่กำหนดชั้นความลับนั้นก่อน แล้วจึงส่งเข้ารหัสตามมาตรฐานที่ได้รับการรับรองจากส่วนราชการ

ข้อ ๒๒ ส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิ์และอำนาจในสายงานสามารกำหนดระเบียบปฏิบัติของการเข้าใช้ที่สอดคล้องกับระเบียบนี้

ข้อ ๒๓ ส่วนราชการต้องจัดให้มีการรักษาความปลอดภัยฐานข้อมูล

เพื่อกำหนดมาตรการป้องกันฐานข้อมูลจากการเข้าถึง การเปลี่ยนแปลง การโอนถ่ายข้อมูล หรือการกระทำใด ๆ โดยผู้ไม่เกี่ยวข้อง โดย

๒๓.๑ ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ในฐานข้อมูลต้องได้รับการจัดระดับ การป้องกัน ผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

๒๓.๒ ส่วนราชการเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์ และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็นเพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

/ ๒๓.๓ ในกรณี ...

๒๓.๓ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างราชการให้จัดทำข้อตกลงการใช้

๒๓.๔ ต้องจัดให้มีแผนการป้องกันไวรัสคอมพิวเตอร์เพื่อป้องกันฐานข้อมูลถูกทำลายโดย

๒๓.๔.๑ ห้ามเจ้าหน้าที่นำคอมพิวเตอร์ซอฟต์แวร์ หรือข้อมูลที่ไม่มั่นใจว่าติดไวรัสคอมพิวเตอร์มาติดตั้ง หรือใช้งาน เว้นแต่คอมพิวเตอร์ซอฟแวร์นั้น ได้ผ่านการตรวจสอบจากเจ้าหน้าที่ความคุมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการก่อน

๒๓.๔.๒ ห้ามเจ้าหน้าที่ปรับแต่ง หรือยกเลิก การทำงานของคอมพิวเตอร์ซอฟต์แวร์ป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการจัดหามาให้

๒๓.๔.๓ กรณีที่มีการเชื่อมต่อกับระบบอินเตอร์เน็ต จะต้องจัดให้มีแผนการใช้งานคอมพิวเตอร์ ในระบบอินเตอร์เน็ต โดยคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก

ข้อ ๒๔ ส่วนราชการจะต้องจัดทำเอกสารประกอบระบบสารสนเทศให้สมบูรณ์ครบถ้วนในทุกด้าน เพื่อความสะดวกในการปรับปรุง แก้ไข และพัฒนาระบบใหม่ เมื่อมีความจำเป็น

**หมวด ๕**

**การรักษาความปลอดภัยในการพัฒนาระบบสารสนเทศ**

ข้อ ๒๕ ในการพัฒนาระบบสารสนเทศ ส่วนราชการจะต้องมีมาตรการที่เหมาะสม ในการรักษาความปลอดภัย ต่องานที่กำลังพัฒนา

ข้อ ๒๖ เมื่อพัฒนาระบบสารสนเทศแล้ว จะต้องจัดให้มีการทดสอบระบบสารสนเทศที่พัฒนาขึ้นมาอย่างละเอียดถี่ถ้วน โดยทดสอบในระบบที่แยกต่างหากจากระบบที่มีอยู่เดิมจนกว่าจะเกิดความมั่นใจในการใช้งาน จึงนำมาใช้งานจริงร่วมกัน หรือทดแทนระบบที่มีอยู่เดิม

ข้อ ๒๗ บุคคลภายนอกที่เข้ามาพัฒนาระบบสารสนเทศ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ โดยเคร่งครัด

/ หมวด ๖ ...

**หมวด ๖**

**การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ**

ข้อ ๒๘ ความมุ่งหมาย เพื่อให้ทราบถึงสาเหตุแห่งการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ การปฏิบัติของเจ้าหน้าที่ และความรับผิดชอบของผู้บังคับบัญชาเมื่อปรากฏการละเมิด

ข้อ ๒๙ สาเหตุแห่งการละเมิดการรักษาความปลอดภัย

การละเมิดการรักษาความปลอดภัยอันเป็นเหตุให้ความลับของทางราชการรั่วไหล เครื่องจักรคำนวณ อุปกรณ์วัสดุ และสถานที่ ถูกทำลาย หรือข้อมูลถูกลบล้าง แก้ไข จนเกิดความเสียหายขึ้น มีสาเหตุจากการขาดจิตสำนึกและวินัยในการรักษาความปลอดภัย ประมาทเลินเล่อเกียจคร้าน ไม่เคร่งครัดต่อหน้าที่ หรือเห็นแก่ประโยชน์ส่วนตัว รวมถึงการจารกรรมและการก่อวินาศกรรมอันเกิดจากการกระทำของบุคคลภายนอก หรือข้าราชการที่ตกเป็นเครื่องมือของฝ่ายตรงข้าม

ข้อ ๓๐ การปฏิบัติเพื่อปรากฏการละเมิดการรักษาความปลอดภัย

๓๐.๑ ผู้ใดตรวจพบหรือทราบว่ามีการละเมิด หรือสงสัยว่าจะมีการละเมิดการรักษาความปลอดภัยเกิดขึ้น ต้องรีบรายงานผู้บังคับบัญชา หรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือเจ้าหน้าที่ผู้รับผิดชอบ

๓๐.๒ เมื่อปรากฏว่าการละเมิดการรักษาความปลอดภัยได้เกิดขึ้นแล้ว เจ้าหน้าที่ที่เกี่ยวข้องหรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ต้องรีบดำเนินการดังนี้

๓๐.๒.๑ รายงานผู้บังคับบัญชา และแจ้ง เจ้ากรมการสนเทศทหาร กองบัญชาการทหารสูงสุด เพื่อให้คำแนะนำช่วยเหลือในเรื่องดังกล่าว

๓๐.๒.๒ สำรวจความเสียหายอันเกิดจากการละเมิดการรักษาความปลอดภัย ค้นหาสาเหตุแห่งการละเมิด ตลอดจนจุดอ่อน ข้อบกพร่อง และความปลอดภัยของเครื่องจักรคำนวณและอุปกรณ์

๓๐.๒.๓ ในกรณีที่ระบบการรหัสของหน่วยสูญหาย หรือสงสัยว่ารั่วไหลให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วย รายงานด่วนให้ผู้บังคับบัญชาตามลำดับชั้นทราบ โดยเร็วที่สุด และพิจารณานำระบบรหัสสำรองที่เตรียมไว้ใช้แทน

๓๐.๒.๔ หากปรากฏหลักฐานหรือสงสัยว่า ถูกจารกรรม หรือก่อวินาศกรรมให้รายงานผู้บังคับบัญชา ตามลำดับชั้นทราบ เพื่อสั่งการให้เจ้าหน้าที่ผู้มีอำนาจในด้านการสืบสวนและสอบสวนดำเนินการต่อไป

/ ข้อ ๓๑ ...

ข้อ ๓๑ ความรับผิดชอบของผู้บังคับบัญชา

๓๑.๑ แจ้งให้ส่วนราชการเจ้าของเรื่องเดิม หรือเจ้าของข้อมูลที่มีข่ายงานร่วมกันทราบทันที

๓๑.๒ สั่งการสอบสวนหาตัวผู้กระทำผิด และผู้รับผิดชอบโดยเร็วที่สุด

๓๑.๓ พิจารณาแก้ไขข้อบกพร่อง และป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

๓๑.๔ พิจารณาสั่งการลงทัณฑ์ หรือดำเนินคดีตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิด และผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้ จะโดยเจตนาหรือไม่เจตนาและการละเมิดนั้นจะเกิดความเสียหาย หรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

ข้อ ๓๒ ความรับผิดชอบของเจ้าของเรื่องเดิม

เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของเรื่องเดิมดำเนินการดังนี้

๓๒.๑ พิจารณาว่าเอกสารกรรมวิธีข้อมูล ประมวลลับ หรือรหัสที่จำเป็นในการใช้วงจรสื่อสารทางสายมีผลกระทบกระเทือนเสียหายอย่างใดหรือไม่

๓๒.๒ ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันทีในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติ พร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นควร

ข้อ ๓๓ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรงให้อยู่ในดุลพินิจของผู้บังคับบัญชาแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติหากจำเป็นให้รายงานหน่วยเหนือตามความเหมาะสม

ข้อ ๓๔ ให้ส่วนราชการที่มีหน่วยกรรมวิธีข้อมูลอัตโนมัติอยู่ในสังกัด ออกระเบียบปลีกย่อยได้ โดยไม่ขัดต่อระเบียบนี้

ประกาศ ณ วันที่ ๒๓ กุมภาพันธ์ ๒๕๔๗

(ลงชื่อ) พลเอก สมทัต อัตตะนันทน์

(สมทัต อัตตะนันทน์)

ผู้บัญชาการทหารสูงสุด