# นโยบายความมั่นคงปลอดภัย
# ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
# (ICT Security Policy)

*** ใช้สำหรับเผยแพร่บุคคลภายนอก ***

☑ อนุมัติ ☐ ไม่อนุมัติ

(นายชนินทร์ ขาวจันทร์)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

30 ต.ค. 2563

ใช้สำหรับเผยแพร่บุคคลภายนอก

# นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานคณะกรรมการส่งเสริมการลงทุน เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักงาน อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้อง สำนักงานจึงได้กำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารขององค์กรขึ้น โดยมีประเด็นและวัตถุประสงค์ ครอบคลุมและเป็นไปตามมาตรฐาน ISO/IEC 27001:2013 ดังนี้

## 1. นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)

1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์: เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของสำนักงาน เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

รายละเอียดที่เกี่ยวข้อง:

1) เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information Security Policy Document)
2) การตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัย (Review of the Information Security Policy)

## 2. โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศภายในสำนักงาน (Internal Organization)

วัตถุประสงค์: เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของสำนักงาน ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย

รายละเอียดที่เกี่ยวข้อง:

1) บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)
2) การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)
3) การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with Authorities)
4) การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with Special Interest Groups)
5) การบริหารจัดการโครงการเพื่อให้มีความมั่นคงปลอดภัย (Information Security in Project Management)

2.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Devices and Teleworking)

วัตถุประสงค์: เพื่อรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศของการปฏิบัติการระยะไกลหรือการปฏิบัติงานจากภายนอกและการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา

รายละเอียดที่เกี่ยวข้อง:

1) นโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)
2) การปฏิบัติงานจากระยะไกล (Teleworking)

## 3. การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)

3.1 การจัดหาบุคลากรก่อนการจ้างงาน (Prior to Employment)

วัตถุประสงค์: เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ ที่ได้รับพิจารณาจ้างงานสำนักงาน

รายละเอียดที่เกี่ยวข้อง:

1) การสรรหาบุคลากร (Screening)
2) ข้อกำหนดและเงื่อนไขของการจ้างงาน (Terms and conditions of employment)

3.2 การสร้างความมั่นคงปลอดภัยขณะเป็นเจ้าหน้าที่ (During employment)

วัตถุประสงค์: เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงาน

รายละเอียดที่เกี่ยวข้อง:

1) หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)
2) การสร้างความตระหนัก การให้ความรู้และการอบรมให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)
3) กระบวนการทางวินัย (Disciplinary Process)

3.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์: เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของการเปลี่ยนหน้าที่ หรือสิ้นสุดการจ้างงาน

รายละเอียดที่เกี่ยวข้อง:

1) การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

## 4. การบริหารจัดการสินทรัพย์ (Asset Management)

4.1 การความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

วัตถุประสงค์: เพื่อให้สินทรัพย์ของสำนักงาน ได้รับการป้องกันและปกป้องอย่างเหมาะสม

รายละเอียดที่เกี่ยวข้อง:

1) ทะเบียนสินทรัพย์ (Inventory of assets)
2) ความเป็นเจ้าของสินทรัพย์ (Ownership for Assets)
3) การอนุญาตให้ใช้สินทรัพย์ (Acceptable Use for Assets)
4) การคืนสินทรัพย์ (Return on Assets)

4.2 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Information Classification)

วัตถุประสงค์: เพื่อทำให้แน่ใจว่าสารสนเทศของสำนักงาน ได้รับการปกป้องในระดับที่เหมาะสม

รายละเอียดที่เกี่ยวข้อง:

1) การกำหนดชั้นความลับของสารสนเทศ (Classification of Information)
2) การจัดทำป้ายชื่อ ของข้อมูล (Labeling of Information)
3) การจัดการสินทรัพย์ (Handling of Asset)

4.3 การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media Handing)

วัตถุประสงค์: เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของสำนักงาน โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

รายละเอียดที่เกี่ยวข้อง:

1) การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)
2) การทำลายสื่อบันทึกข้อมูล (Disposal of Media)
3) การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

## 5. การควบคุมการเข้าถึง (Access Control)

5.1 การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

วัตถุประสงค์: เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย

รายละเอียดที่เกี่ยวข้อง:

1) นโยบายควบคุมการเข้าถึง (Access Control Policy)
2) การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services)

5.2 การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

วัตถุประสงค์: เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

รายละเอียดที่เกี่ยวข้อง:

1) การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration)
2) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)
3) การบริหารจัดการสิทธิ์ตามระดับสิทธิ์การเข้าถึง (Management of Privileged Access Right)
4) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User)
5) การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)
6) การถอนหรือการจัดการสิทธิ์การเข้าถึง (Removal or Adjustment of Access Rights)

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilies)

วัตถุประสงค์: เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลที่ใช้ในการพิสูจน์ตัวตน

รายละเอียดที่เกี่ยวข้อง:

1) การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

5.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

วัตถุประสงค์: เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

รายละเอียดที่เกี่ยวข้อง:

1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)
2) ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure)
3) ระบบบริหารจัดการรหัสผ่าน (Password Management System)
4) การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)
5) การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code)

## 6. การเข้ารหัสข้อมูล (Cryptography)

6.1 การกำหนดการควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)

วัตถุประสงค์: เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องการความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

รายละเอียดที่เกี่ยวข้อง:

1) นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)
2) การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management)

## 7. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and Environmental Security)

7.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

วัตถุประสงค์: เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพ ที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์สำนักงาน

รายละเอียดที่เกี่ยวข้อง:

1) การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)
2) การควบคุมการเข้าออก (Physical Entry Controls)
3) การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)
4) การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อมอื่น ๆ (Protecting against External and Environmental Threats)
5) การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Working in Secure Areas)
6) การกำหนดพื้นที่สำหรับบุคคลภายนอกใช้รับ-ส่งสิ่งของ (Delivery and Loading Areas)

7.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment)

วัตถุประสงค์: เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่นๆ

รายละเอียดที่เกี่ยวข้อง:

1) การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Seting and Protection)
2) การดูแลอุปกรณ์ต่างๆ (Supporting Utilities)
3) การเดินสายไฟและสายเคเบิล (Cabling Security)
4) การดูแลรักษาอุปกรณ์ (Equipment Maintenance)
5) การนำสินทรัพย์ขององค์กรออกนอกสำนักงาน (Removal of Asset)
6) การป้องกันอุปกรณ์และสินทรัพย์สารสนเทศที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment and asset Off-Premises)
7) การจัดการอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้ใหม่ (Secure Disposal or Re-use of Equipment)
8) การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment)
9) การควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy)

## 8. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)

8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

วัตถุประสงค์: เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

รายละเอียดที่เกี่ยวข้อง:

1) การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)
2) การจัดการการเปลี่ยนแปลง (Change Management)
3) การจัดการขีดความสามารถ (Capacity Management)
4) การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนา ทดสอบและสภาพแวดล้อมในการปฏิบัติงาน (Separation of Development, Testing and Operational Environment)

8.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์: เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้อง และมั่นคงปลอดภัย

รายละเอียดที่เกี่ยวข้อง:

1) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

8.3 การสำรองข้อมูล (Backup)

วัตถุประสงค์: เพื่อเป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่างๆ เช่น ภัยธรรมชาติ ระบบเสียหาย ฯลฯ

รายละเอียดที่เกี่ยวข้อง:

1) การสำรองข้อมูล (Information Backup)

8.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์: เพื่อให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน

รายละเอียดที่เกี่ยวข้อง:

1) การบันทึกข้อมูลเหตุการณ์ (Event logging)
2) การป้องกันข้อมูลล็อก (Protection of Log Information)
3) ข้อมูลล็อกของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ (Administrator and Operator Logs)
4) การตั้งเวลาให้ถูกต้อง (Clock Synchronization)

8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operation Software)

วัตถุประสงค์: เพื่อให้ระบบที่ให้บริการ สามารถให้บริการและมีการทำงานที่ถูกต้อง

รายละเอียดที่เกี่ยวข้อง:

1) การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems)

8.6 การบริหารจัดการช่องโหว่ทางเทคนิค ( Technical Vulnerability Management)

วัตถุประสงค์: เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

รายละเอียดที่เกี่ยวข้อง:

1) การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)
2) การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

8.7 การพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations)

วัตถุประสงค์: เพื่อให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดำเนินงานของหน่วยงาน

รายละเอียดที่เกี่ยวข้อง:

1) การวางแผนการตรวจสอบระบบสารสนเทศทั้งหมด (Information System Audit Controls)

## 9. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

9.1 การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

วัตถุประสงค์: เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของสำนักงาน

รายละเอียดที่เกี่ยวข้อง:

1) การควบคุมการเข้าถึงเครือข่าย (Network Control)
2) การความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)
3) การจัดแบ่งเครือข่ายภายในสำนักงานฯ (Segregation in Network)

9.2 การถ่ายโอนข้อมูล (Information Transfer)

วัตถุประสงค์: เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในองค์กร และถ่ายโอนข้อมูลกับภายนอกหน่วยงาน

รายละเอียดที่เกี่ยวข้อง:

1) นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information Transfer Policies and Procedures)

2) ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on Information Transfer)
3) การรักษาความมั่นคงปลอดภัยการส่งข้อความอิเล็กทรอนิกส์ (Electronic Messaging)
4) การรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or Non-Disclosure Agreements)

## 10. การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)

10.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

วัตถุประสงค์: เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

รายละเอียดที่เกี่ยวข้อง:

1) การกำหนดความต้องการด้านความมั่นคงปลอดภัย (Information Security Requirements Analysis and Specification)
2) ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)
3) การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

10.2 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

วัตถุประสงค์: เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศที่มีความมั่นคงปลอดภัย ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ (development lifecycle)

รายละเอียดที่เกี่ยวข้อง:

1) นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)
2) กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)
3) การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes)
4) การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)
5) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)
6) สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)
7) การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (Outsourced Development)
8) การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)
9) การทดสอบเพื่อรับรองระบบ (System acceptance testing)

10.3 ข้อมูลสำหรับการทดสอบ (Test data)

วัตถุประสงค์: เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

รายละเอียดที่เกี่ยวข้อง:

1) การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

## 11. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

11.1 ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

วัตถุประสงค์: เพื่อให้มีการป้องกันสินทรัพย์ขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

รายละเอียดที่เกี่ยวข้อง:

1) นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)
2) การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Assessing security within supplier agreements)
3) ห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)

11.2 การบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

วัตถุประสงค์: เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ ของผู้ให้บริการภายนอก

รายละเอียดที่เกี่ยวข้อง:

1) การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services)
2) การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Chages to Supplier Services)

## 12. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

12.1 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์: เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของสำนักงาน ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

รายละเอียดที่เกี่ยวข้อง:

1) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)
2) การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events)
3) การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)
4) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)
5) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

6) การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from Information Security Incidents)
7) การเก็บรวบรวมหลักฐาน (Collection of Evidence)

## 13. การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

13.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)
วัตถุประสงค์: เพื่อป้องกันการหยุดชะงักในการดำเนินงานของสำนักงาน ที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ
รายละเอียดที่เกี่ยวข้อง:
1) การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)
2) การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implement information security continuity)
3) การตรวจสอบ ทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

13.2 การเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)
วัตถุประสงค์: เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ
รายละเอียดที่เกี่ยวข้อง:
1) สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนทศ (Availability of information processing facilities)

## 14. การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน (Compliance)

14.1 การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)
วัตถุประสงค์: เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับรวมทั้งสัญญาต่างๆ
รายละเอียดที่เกี่ยวข้อง:
1) การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)
2) ทรัพย์สินทางปัญญา (Intellectual Property Rights)
3) การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)
4) ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)
5) การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

14.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

วัตถุประสงค์: เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

รายละเอียดที่เกี่ยวข้อง:

1) การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)
2) การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)
3) การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

**********