สำเนา

บริษัท ศรีวิชัยเวชวิวัฒน์ จำกัด (มหาชน)

และบริษัทย่อย

ระเบียบและแนวทางการปฏิบัติ

เรื่อง

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของ กลุ่มโรงพยาบาลวิชัยเวช อินเตอร์เนชั่นแนล

ประกาศใช้ตั้งแต่วันที่ 1 มกราคม 2559

ลงชื่อ

(นายพฤทธิ์ โรจน์มหามงคล)

ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศฯ

ลงชื่อ

(ผศ.พญ.สายสุณี วนดุรงค์วรรณ)

ประธานเจ้าหน้าที่บริหาร

บริษัท ศรีวิชัยเวชวิวัฒน์ จำกัด (มหาชน)

และบริษัทย่อย

ระเบียบและแนวทางการปฏิบัติ

เรื่อง

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของ กลุ่มโรงพยาบาลวิชัยเวช อินเตอร์เนชั่นแนล

ประกาศใช้ตั้งแต่วันที่ 1 มกราคม 2559

สารบัญ

หมวดที่ 1 นโยบายความมั่นคงและความปลอดภัยขององค์กร (Security Policy) 1

1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) 1

1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร **(Information Security Policy Document)** 1

1.1.2 การตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัย **(Review of the Information Security Policy)** 1

หมวดที่ 2 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security) 2

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร (Internal Organization) 2

2.1.1 การให้ความสำคัญของผู้บริการและกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย **(Management Commitment to Information Security)** 2

2.1.2 การประสานงานความมั่นคงปลอดภัยภายใน **(Information Security Coordination)** 2

2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย **(Allocation of Information Security Responsibilities)** 2

2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ **(Authorization Process for Information Processing Facilities)** 2

2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร **(Confidentiality Agreements)** 3

2.1.6 การมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น **(Contact with authorities)** 3

2.1.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน **(Contact with Special Interest Groups)** 3

2.1.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ**(Independent Review of Information Security)** 3

2.2 โครงสร้างทางความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties) 4

2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก **(Identification of Risks Related to External Parties)**.4

2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร **(Addressing Security When Dealing with Customers)** 4

2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร **(Addressing Security in Third Party Agreements)** 4

หมวดที่ 3 การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset Management) 5

3.1 ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets) 5

3.1.1 ทะเบียนสินทรัพย์ **(Inventory of assets)** 5

3.1.2 ความเป็นเจ้าของสินทรัพย์ **(Ownership for Assets)** 5

3.1.3 การอนุญาตให้ใช้สินทรัพย์ **(Acceptable Use for Assets)** 5

3.2 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Information Classification) 10

3.2.1 วิธีการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร **(Classification Guidelines)** 10

3.2.2 การจัดทำป้ายชื่อ และการจัดการข้อมูลสารสนเทศ **(Information Labeling and Handing)** 10

หมวดที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security) 12

4.1 การสร้างความความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากรก่อนการทำงาน(Prior to Employment) 12

4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความปลอดภัย **(Roles and Responsibilities)** 12

4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening) 12

4.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) 12

4.2 การสร้างความความมั่นคงปลอดภัยขณะเป็นพนักงาน (During Employment) 13

4.2.1 การรับผิดชอบของผู้บริหาร (Management Responsibilities) 13

4.2.2 การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่เจ้าหน้าที่ (Information Security Awareness Education and Training) 13

4.2.3 การควบคุมระเบียบวินัย (Disciplinary Process) 14

4.3 การยกเลิกการจ้างงาน (Termination of Change of Employment) 14

4.3.1 การยกเลิกความรับผิดชอบ (Termination Responsibility) 14

4.3.2 การคืนทรัพย์สิน (Return on Assets) 14

4.3.3 การยกเลิกการเข้าถึง (Removal of Access rights) 14

หมวดที่ 5 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and Environmental Security) 15

5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas) 15

5.1.1 การกำหนดพื้นที่มั่นคงปลอดภัย (**Physical Security Perimeter**) 15

5.1.2 การควบคุมการเข้าออก (**Physical Entry Controls**) 15

5.1.3 การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ **(Securing Offices, Rooms and Facilities)** 16

5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อมอื่น ๆ (**Protecting Against External and Environmental Threats**) 16

5.1.5 การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย **(Working in Secure Areas)** 16

5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security) 16

5.2.1 การจัดตั้งและการป้องกันอุปกรณ์ (**Equipments Setting and Protection**) 16

5.2.2 การดูแลอุปกรณ์ต่าง ๆ (**Supporting Utilities**) 17

5.2.3 การเดินสายไฟและสายเคเบิล (**Cabling Security**) 17

5.2.4 การดูแลรักษาอุปกรณ์ (**Equipment Maintenance**) 17

5.2.5 การป้องกันอุปกรณ์และทรัพย์สินสารสนเทศที่ใช้งานอยู่นอกหน่วยงาน (**Security of Equipment Off-Premises**) 17

5.2.6 การจัดการอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้ใหม่ (**Secure Disposal or Re-use of Equipment**) 17

5.2.7 การนำอุปกรณ์ออกนอกพื้นที่ (Removal of Property) 17

หมวดที่ 6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของ เครือข่ายสารสนเทศขององค์กร (Communications and Operations Management) 18

6.1 การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational Procedures and Responsibilities) 18

6.1.1 คู่มือและขั้นตอนการปฏิบัติงาน (**Documented Operation Procedures)** 18

6.1.2 การแบ่งหน้าที่ความรับผิดชอบ (**Segregation of Duties)** 18

6.1.3 การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนาและทดสอบ (**Separation of development, test and operational facilities)** 19

6.2 การจัดการผู้ให้บริการภายนอก (Third Party Service Delivery Management) 19

6.2.1 การส่งมอบบริการ (**Service Delivery)** 19

6.2.2 การทบทวนและตรวจสอบบริการจากผู้ให้บริการภายนอก (**Monitoring and Review of Third Party Services)** 20

6.2.3 การจัดการการเปลี่ยนแปลงบริการจากผู้ให้บริการภายนอก (**Managing Changes to Third Party Services)** 20

6.3 การวางแผนและการยอมรับระบบสารสนเทศ (System Planning and Acceptance) 20

6.3.1 การจัดการขีดความสามารถ (Capacity Management) 20

6.4 การป้องกันซอฟต์แวร์ไม่ประสงค์ดี (Protection Against Malicious and Mobile Code) 21

6.4.1 การควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls Against Malicious Code) 21

6.4.2 การควบคุมโปรแกรมชนิดเคลื่อนที่ได้ (Controls Against Mobile Code) 22

6.5 นโยบายการสำรองข้อมูล (Information Back-up) 22

6.5.1 นโยบายการสำรองข้อมูล (Information Back-up) 22

6.6 การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management) 23

6.6.1 การบริหารและจัดการด้านความมั่นคงปลอดภัยบนเครือข่าย (Network Controls) 23

6.6.2 ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Services) 23

6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media Handing) 24

6.7.1 การบริหารและจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (**Management Of Removable Media)** 24

6.7.2 การทำลายสื่อบันทึกข้อมูล (**Disposal of Media)** 24

6.7.3 วิธีการปฏิบัติในการจัดการสื่อบันทึกข้อมูล (Information Handing Procedures) 25

6.7.4 การจัดการเอกสารที่เกี่ยวกับระบบสารสนเทศขององค์กรอย่างปลอดภัย (Security of System Documentation) 25

6.8 การแลกเปลี่ยนข้อมูลสารสนเทศ (Exchange Of Information) 25

6.8.1 นโยบายและกระบวนการแลกเปลี่ยนข้อมูลสารสนเทศ (**Information Exchange policies and procedures)** 25

6.8.2 สัญญาและข้อกำหนดในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements) 26

6.8.3 การจัดส่งสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัย (Physical Media in Transit) 26

6.8.4 การรักษาความมั่นคงปลอดภัยข้อมูลอิเล็กทรอนิกส์ (Electronic Messaging) 26

6.8.5 ข้อมูลเผยแพร่ต่อสาธารณะ (Publicly available information) 26

6.9 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring) 26

6.9.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging) 26

6.9.2 การตรวจสอบการใช้งานระบบ (Monitoring System Use) 26

6.9.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (**Protection of log Information**) 27

6.9.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (**Administrator and Operator Logs**) 27

6.9.5 การบันทึกเหตุการณ์ข้อผิดพลาด (**Fault Logging**) 27

6.9.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (**Clock Synchronization**) 27

หมวดที่ 7 การควบคุมการเข้าถึง (Access Control) 28

7.1 การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control) 28

7.1.1 นโยบายควบคุมการเข้าถึง **(Access Control Policy)** 28

7.2 การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management) 29

7.2.1 การลงทะเบียนผู้ใช้งานใหม่ **(User Registration)** 29

7.2.2 การบริหารสิทธิ์การเข้าถึงระบบของผู้ใช้งานระบบ **(Privilege Management)** 29

7.2.3 การบริหารจัดการรหัสผ่านผู้ใช้งาน **(User Password Management)** 29

7.2.4 การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน **(Review of User Access Rights)** 29

7.3 การรับผิดชอบหน้าที่ของผู้ใช้งาน (User Responsibilities) 30

7.3.1 การใช้งานรหัสผ่าน **(Password Use)** 30

7.3.2 การควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย **(Clear Desk and Clear Screen Policy)** 31

7.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control) 31

7.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on Use of Network Services) 31

7.4.2 การพิสูจน์ตัวตนของการเชื่อมต่อจากภายนอก **(User authentication for external connections)** 32

7.4.3 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ **(Remote Diagnostic And Configuration Port Protection)** 33

7.4.4 การจัดการแบ่งเครือข่ายภายในองค์กรกับภายนอกองค์กร **(Segregation in Networks)** 33

7.4.5 การควบคุมผู้ใช้งานในการใช้งานเครือข่าย **(Network Connection Control)** 33

7.4.6 การจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน **(Network Routing Control)** 33

7.5 การควบคุมการใช้งานระบบปฏิบัติการ (Operating System Access Control) 34

7.5.1 กระบวนการเข้าถึงระบบ (Secure Log – on Procedures) 34

7.5.2 การพิสูจน์ตัวตนสำหรับผู้ใช้งานระบบ (User Identification and Authentication) 34

7.5.3 การบริหารจัดการรหัสผ่าน **(Password Management System)** 34

7.5.4 การควบคุมการใช้งานโปรแกรมยูทิลิตี้ **(User of System Utilities)** 34

7.5.5 การกำหนดเวลาการใช้งานระบบ **(Session Time – out)** 34

7.6 **การควบคุมการใช้งานระบบสารสนเทศและสารสนเทศ (Application and Information Access Control)**.....35

7.6.1 การจำกัดการใช้งานสารสนเทศ **(Information Access Restriction)**.....35

7.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง **(Sensitive System Isolation)**.....35

7.7 การควบคุมการเข้าถึงข้อมูลสารสนเทศ (Information Technology Access Control).....35

7.7.1 การเข้าถึงข้อมูลสารสนเทศ **(Information Technology Access)**.....35

7.8 คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถานที่ (Mobile Computing).....36

7.8.1 การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา**(Mobile Computing and Communications)** 36

หมวดที่ 8 การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development, and Maintenance) ... 37

8.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems).....37

8.1.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัย **(Security Requirements Analysis and Specification)**.....37

8.2 ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ (Security of System Files).....37

8.2.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ **(Control of Operational Software)**.....37

8.3 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes) 38

8.3.1 กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ **(Change Control Procedures)**.....38

8.3.2 การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ **(Technical Review of Applications after Operating System Changes)**.....38

8.3.3 การควบคุมการเปลี่ยนแปลงซอฟท์แวร์สำเร็จรูป **(Restrictions on Changes to Software Packages)**.....39

8.3.4 การควบคุมการรั่วไหลของข้อมูล **(Information Leakage)** 39

8.3.5 การควบคุมการว่าจ้างการพัฒนาระบบ **(Outsourced Software Development)**.....39

หมวดที่ 9 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)..... 40

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคง (Reporting Information Security Events and Weaknesses).....40

9.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย **(Reporting Information Security Events)**.....40

9.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร **(Reporting Security Weaknesses)** 42

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of Information Security Incidents Improvements).....42

9.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ **(Responsibilities and Procedures)**.....42

9.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย **(Learning from Security Incidents)**.....42

9.2.3 การเก็บรวบรวมหลักฐาน (Collection of Evidence) 42

หน่วยที่ 10 การบริหารความต่อเนื่องของการดำเนินงานขององค์กร(Business Continuity Management) 43

10.1 การจัดการความต่อเนื่องของการดำเนินงานองค์กร (Aspects of Business Continuity) 43

10.1.1 ขอบเขตของการดำเนินกระบวนการจัดการความต่อเนื่องต้องครอบคลุมถึงการรักษาความปลอดภัยสารสนเทศ **(Including Information Security in the Business Continuity Management Process)** 43

10.1.2 กระบวนการจัดการความต่อเนื่องและการประเมินความเสี่ยง **(Business Continuity and Risk Assessment)** 43

10.1.3 การจัดทำและการประยุกต์ใช้แผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ**(Developing and Implementing Continuity Plans Including Information Security)** 44

10.1.4 กรอบโครงสร้างของขอบเขตของแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ **(Business Continuity Planning Framework)** 44

10.1.5 การทดสอบ การรักษาไว้ และการประเมินทบทวนแผนฉุกเฉิน **(Testing, Maintaining and Reassessing Business Continuity Plans)**.....45

หน่วยที่ 11 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน (Compliance)..... 46

11.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย (Compliance with Legal Requirements) 46

11.1.1 การระบุข้อกำหนดในการใช้งานระบบสารสนเทศ **(Identification of Applicable Legislation)** 46

11.1.2 ทรัพย์สินทางปัญญา **(Intellectual Property Rights, IPR)** 47

11.1.3 การเก็บและป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด **(Protection of Organizational Records)** 48

11.1.4 การป้องกันข้อมูลและความเป็นส่วนตัว **(Data protection and privacy of personal information)** 48

11.1.5 การป้องกันการใช้งานเครื่องมือ **(Prevention of misuse of information processing facilities)**.....48

11.1.6 การควบคุมการเข้ารหัส **(Regulation of cryptographic controls)**.....48

หมวดที่ 1 นโยบายความมั่นคงและความปลอดภัยขององค์กร (Security Policy)

1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์ : เพื่อกำหนดทิศทางและให้การสนับสนุนดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

<u>นโยบาย</u>

1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information Security Policy Document)

1) ต้องจัดทำนโยบายระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ โดยนโยบายฯ ดังกล่าวจะต้องได้รับอนุมัติก่อนนำไปใช้
2) ต้องจัดให้มีการเผยแพร่เอกสารนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกลุ่มโรงพยาบาลวิชัยเวช อินเตอร์เนชั่นแนลฯ ให้กับผู้บริหารและเจ้าหน้าที่ฝ่ายสารสนเทศ และบุคคลที่เกี่ยวข้องรับทราบ

1.1.2 การตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัย (Review of the Information Security Policy)

ต้องดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทุก 1 ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

หมวดที่ 2 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ

(Organizational of Information Security)

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

(Internal Organization)

วัตถุประสงค์ : เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

นโยบาย

2.1.1 การให้ความสำคัญของผู้บริการและกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management Commitment to Information Security)

1) ผู้บริหารต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัยโดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ
2) ผู้บริหารต้องแต่งตั้งคณะและกลุ่มผู้ทำงานหลัก ตลอดจนทรัพยากรที่จำเป็น เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศองค์กร

2.1.2 การประสานงานความมั่นคงปลอดภัยภายใน (Information Security Coordination)

ผู้บริหารต้องกำหนดให้มีตัวแทนเจ้าหน้าที่จากหน่วยงานต่าง ๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงและปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน

2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of Information Security Responsibilities)

ผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน

2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization Process for Information Processing Facilities)

ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่ก่อนให้มีการใช้กระบวนการนี้

2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร(Confidentiality Agreements)

เจ้าหน้าที่ประสานงานกลุ่มบริหารทรัพยากรบุคคลต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร รวมทั้งเงื่อนไขหรือข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับ จะต้องได้รับการปรับปรุงอยู่สม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร

2.1.6 การมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น(Contact with authorities)

ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงาน การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย **(ThaiCERT)** เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงและความปลอดภัยในกรณีที่มีความจำเป็น

2.1.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with Special Interest Groups)

ต้องกำหนดรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่าง ๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความสนใจด้านความมั่นคงและความปลอดภัยสารสนเทศหรือสมาคมต่าง ๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วม

2.1.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent Review of Information Security)

ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร

2.2 โครงสร้างทางความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)

วัตถุประสงค์ : เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

<u>นโยบาย</u>

2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of Risks Related to External Parties)

ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing Security When Dealing with Customers)

ต้องระบุและบังคับใช้ข้อกำหนดทางด้านความมั่นคงและความปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing Security in Third Party Agreements)

ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอกเมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

หมวดที่ 3 การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset Management)

3.1 ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

วัตถุประสงค์: เพื่อให้สินทรัพย์ขององค์กรได้รับการป้องกันและปกป้องอย่างเหมาะสม

นโยบาย

3.1.1 ทะเบียนสินทรัพย์ (Inventory of assets)

1) ต้องจัดทำและเก็บทะเบียนสินทรัพย์ ซึ่งรวมถึงสินทรัพย์ข้อมูลและเอกสาร (Information and Document Asset) สินทรัพย์ซอฟแวร์ (Software Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ขององค์กร โดยปฏิบัติตามระเบียบและแนวทางการปฏิบัติ เรื่องการบริหารทรัพย์สิน
2) ต้องมีการตรวจสอบสินทรัพย์ (Inventory Check) ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ทุกประเภทตามระยะเวลาที่กำหนดไว้
3) ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์เมื่อมีสินทรัพย์ใหม่ หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

3.1.2 ความเป็นเจ้าของสินทรัพย์ (Ownership for Assets)

ต้องกำหนดบุคคล หรือหน่วยงานผู้รับผิดชอบ ข้อมูลและสินทรัพย์ทั้งหมดด้านเทคโนโลยีสารสนเทศอย่างชัดเจน

3.1.3 การอนุญาตให้ใช้สินทรัพย์ (Acceptable Use for Assets)

- **การอนุญาตให้ใช้งานสินทรัพย์ด้านอุปกรณ์คอมพิวเตอร์มีดังนี้**

1) ระบบเทคโนโลยีสารสนเทศ และอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่องค์กรเป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานขององค์กร การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่

2) เจ้าหน้าที่ ตลอดจนบุคคล และ/หรือนิติบุคคลที่ได้รับว่าจ้าง จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศ ด้วย
3) ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ขององค์กรอย่างระมัดระวังและให้การปกป้องเสมือนเป็นสินทรัพย์ของตน - เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งหมดขององค์กรต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
4) ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายขององค์กร รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ขององค์กร ก่อนได้รับอนุญาต
5) เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในองค์กร อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์ตามคำแนะนำที่ระบุไว้ในเอกสารขั้นตอนการปฏิบัติงาน เรื่อง การใช้เครื่องคอมพิวเตอร์ในการปฏิบัติงาน
6) อุปกรณ์คอมพิวเตอร์ขององค์กร ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตและเจ้าหน้าที่สารสนเทศต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ บนเครื่องคอมพิวเตอร์ขององค์กร อย่างเด็ดขาด

➢ **การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้**

1) ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ขององค์กร
2) ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญขององค์กร ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูลก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศขององค์กร
3) ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอเพื่อให้ผู้ใช้งานทั่วไปขององค์กร มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้

4) รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการท างานขององค์กรเท่านั้น

➢ **การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้**

1) องค์กรจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการทำวิจัยการค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการขององค์กร
2) ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้องค์กร และบุคคลผู้ที่เกี่ยวข้องกับองค์กรเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
3) การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้องค์กรขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
4) ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป็อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
5) ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสม หรือผิดกฎหมาย
6) องค์กรไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ดบล็อก ไลน์ เฟซบุ๊ค) ของเจ้าหน้าที่ ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

➢ **การอนุญาตให้ใช้งานอีเมล์มีดังนี้**

1) ผู้ใช้งานอีเมล์ทั้งหมดขององค์กร ต้องมี E-mail Account เป็นของตนเอง
2) E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำ อีเมล์ไปใช้ในทางที่ผิด

3) E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น hr@vichaivej.comอาจได้รับการสร้างขึ้นเพื่อเป็นE-mail Account กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ E-mail Account นั้น
4) E-mail Account ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมล์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายขององค์กร ถือเป็นสินทรัพย์ขององค์กร
5) ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือติดต่อสื่อสารกับระบบอีเมล์ขององค์กร
6) พื้นที่เก็บอีเมล์บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัดผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ให้เป็นไปตามขนาดที่องค์กรกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงาน และอีเมล์ตามที่กฎหมายกำหนดไว้เท่านั้น
7) ขนาดของอีเมล์และไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมล์และไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนดผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้
8) ห้ามใช้ E-mail Account ขององค์กรเพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
9) ห้ามใช้ E-mail Account ขององค์กรในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ดบล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับองค์กร
10) ผู้ใช้งานอีเมล์ต้องตั้งค่าให้อีเมล์ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน องค์กรและเบอร์โทรศัพท์ติดต่อ
11) ห้ามผู้ใช้งานทำสำเนาข้อความหรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
12) ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนขององค์กร
13) ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์หัวจดหมายอีเมล์ลายเซ็นในอีเมล์ หรือe-mail Accountของบุคคลอื่นโดยเด็ดขาด
14) ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้e-mail Accountของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม

15) ผู้ใช้งานต้องหลีกเลี่ยงการใช้คำสั่ง “Reply with History” ซึ่งเป็นการตอบกลับอีเมล์พร้อมไฟล์แนบไปยังผู้รับ ยกเว้นในกรณีที่จำเป็นต้องใช้งานเท่านั้น อย่างไรก็ตามเมื่อมีการใช้งานคำสั่ง “Reply with History” ผู้ใช้งานควรทำการลบไฟล์แนบทิ้งเสียก่อนที่จะทำการส่งอีเมล์

16) ผู้ใช้งานต้องทำการส่งอีเมล์ให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้น และห้ามใช้คำสั่ง “Reply All” ถ้าหากอีเมล์ฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน

17) ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้าต่าง ๆ(Spam Mail) เป็นต้น

18) ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่ง อีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด

19) ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

20) ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อองค์กร

21) ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)

22) เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่าเครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

3.2 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Information Classification)

วัตถุประสงค์: เพื่อทำให้แน่ใจว่าสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม

นโยบาย

3.2.1 วิธีการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines)

1) เจ้าหน้าที่ต้องทำการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับ
2) เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับข้อมูลดิจิตอลหรือสารสนเทศดิจิตอลนั้น

3.2.2 การจัดทำป้ายชื่อ และการจัดการข้อมูลสารสนเทศ (Information Labeling and Handing)

1) ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูล และอุปกรณ์สินทรัพย์สารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร
2) ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย
3) ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น
4) ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม
5) ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งานโดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน
6) ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสารฯลฯ โดยทันที

7) เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล
8) เจ้าหน้าที่ต้องไม่พูดคุยหรือใช้งานข้อมูลลับขององค์กรในพื้นที่สาธารณะ เช่น ลิฟท์ ร้านอาหาร ฯลฯ
9) สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น PDA, Thumb-Drive, CD-Rom เป็นต้น) ที่มีข้อมูลลับขององค์กร บันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง
10) ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินงานขององค์กรทั้งหมด ทั้งที่มีการเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ใช้งาน ต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใด ๆ เกิดขึ้น ตัวอย่างเช่น การติดไวรัส ฮาร์ดดิสก์เสีย เป็นต้น

หมวดที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

4.1 การสร้างความความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากรก่อนการทำงาน (Prior to Employment)

วัตถุประสงค์: เพื่อกำหนดและคัดสรรบุคคลก่อนที่จะเข้ามาทำงาน เพื่อลดความเสี่ยงจากความผิดพลาด การขโมยการปลอมแปลง และการนำไปใช้ในทางที่ไม่เหมาะสมของพนักงานอันเกิดจากการปฏิบัติงานกับระบบสารสนเทศและทรัพยากรสารสนเทศอื่น ๆ ขององค์กร

นโยบาย

4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความปลอดภัย (Roles and Responsibilities)

ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับเจ้าหน้าที่ที่หน่วยงานทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกว่าจ้างมาปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศของหน่วยงาน

4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

1) เจ้าหน้าที่บริหารทรัพยากรบุคคล ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นผู้บริหาร พนักงานชั่วคราวหรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน
2) เจ้าหน้าที่บริหารทรัพยากรบุคคล ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และหน่วยงาน ว่าจะไม่เปิดเผยความลับของหน่วยงาน โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างเจ้าหน้าที่นั้น ๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

4.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

1) เจ้าหน้าที่ประสานงานกลุ่มบริหารทรัพยากรบุคคลต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ
2) เพื่อให้การบริหารจัดการ Login หรือ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด เจ้าหน้าที่บริหารทรัพยากรบุคคล ต้องแจ้งให้สำนักเทคโนโลยีสารสนเทศทราบทันทีเมื่อมีเหตุดังนี้
   - การว่าจ้างงาน

- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร พนักงาน และลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

4.2 การสร้างความความมั่นคงปลอดภัยขณะเป็นพนักงาน (During Employment)

วัตถุประสงค์: เพื่อให้เจ้าหน้าที่ได้ตระหนักถึงภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้แก่พนักงานเพื่อให้สามารถป้องกันภัยดังกล่าวได้

นโยบาย

4.2.1 การรับผิดชอบของผู้บริหาร (Management Responsibilities)

ต้องกำหนดให้เจ้าหน้าที่ พนักงาน และเจ้าหน้าที่หน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบและปฏิบัติตามนโยบาย กฎระเบียบและขั้นตอนการทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศด้วย

4.2.2 การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่เจ้าหน้าที่ (Information Security Awareness Education and Training)

1) ต้องจัดอบรมให้ความรู้แก่เจ้าหน้าที่เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัย และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศด้วย
2) เจ้าหน้าที่ใหม่ทุกคน ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานก่อนหรืออย่างน้อยภายใน 30 วันนับจากเข้าทำงานในหน่วยงาน โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย
3) เจ้าหน้าที่บริหารทรัพยากรบุคคลหรือเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่บุคลากรด้วย

4.2.3 การควบคุมระเบียบวินัย (Disciplinary Process)

ผู้บริหารต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติขององค์กรแต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกฎหมายนั้น ๆ

4.3 การยกเลิกการจ้างงาน (Termination of Change of Employment)

วัตถุประสงค์: เพื่อให้มีการยกเลิกสิทธิ์กับเจ้าหน้าที่ที่ถูกยกเลิกการจ้างงานหรือหมดสัญญาฯ

<u>นโยบาย</u>

4.3.1 การยกเลิกความรับผิดชอบ (Termination Responsibility)

เจ้าหน้าที่บริหารทรัพยากรบุคคล มีหน้าที่ดูแลหากมีการแต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงตำแหน่งใด ๆ ที่เกี่ยวข้องกับความรับผิดชอบในองค์กร

4.3.2 การคืนทรัพย์สิน (Return on Assets)

เจ้าหน้าที่ของกลุ่มโรงพยาบาลวิชัยเวช อินเตอร์เนชั่นแนล ซึ่งพ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

4.3.3 การยกเลิกการเข้าถึง (Removal of Access rights)

หลังจากมีการยกเลิกหรือเปลี่ยนแปลงตำแหน่งการเป็นเจ้าหน้าที่ของกลุ่มโรงพยาบาลวิชัยเวช อินเตอร์เนชั่นแนลแล้วเจ้าหน้าที่บริหารทรัพยากรบุคคลจะต้องแจ้งให้เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศเพื่อยกเลิกการเข้าถึงข้อมูลต่าง ๆ ของหน่วยงานและเจ้าหน้าที่บริหารทรัพยากรบุคคลทำการแจ้งต่อพนักงานอื่นๆ, ลูกค้า,บริษัทคู่ค้า, Third Party/Outsource ที่เกี่ยวข้องให้รับทราบ ตามเหมาะสม

หมวดที่ 5 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and Environmental Security)

5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

วัตถุประสงค์: เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นทรัพย์สินของกลุ่มโรงพยาบาลวิชัยเวช อินเตอร์เนชั่นแนล

นโยบาย

5.1.1 การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

หน่วยงานสารสนเทศจะต้องมีการจำแนก และกำหนดพื้นที่ในการใช้งานระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้เมื่อมีการกำหนดพื้นที่แล้วให้มีการควบคุมการเข้าออก

5.1.2 การควบคุมการเข้าออก (Physical Entry Controls)

หน่วยงานสารสนเทศต้องจัดให้มีการควบคุมการเข้าออกในบริเวณ“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” โดยให้ผ่านเข้าออกได้เฉพาะเจ้าหน้าที่สารสนเทศที่มีสิทธิ์ เท่านั้น และมีแนวทางปฏิบัติ ดังนี้

1) ต้องกำหนดเจ้าหน้าที่สารสนเทศที่มีสิทธิ์ผ่านเข้าออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในห้องคอมพิวเตอร์แม่ข่าย (Data Center) อย่างชัดเจน โดยต้องมีการบันทึกข้อมูลการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Data Canter) ของเจ้าหน้าที่สารสนเทศทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี
2) หากมีบุคคลอื่นใดที่ไม่ใช่เจ้าหน้าที่สารสนเทศ ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการ ล่วงหน้าหน่วยงานต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่ เป็นการชั่วคราว ทั้งนี้จะต้องมีการลงลายมือชื่อ และจดบันทึกกิจกรรมในการขอเข้าออกไว้เป็นหลักฐาน พร้อมทั้งมีเจ้าหน้าที่สารสนเทศเป็นผู้กำกับดูแลการเข้าออกและจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี

5.1.3 การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ(Securing Offices, Rooms and Facilities)

1) หน่วยงานสารสนเทศต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ให้กับสำนักงาน ห้องทำงานและ เครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออกของบุคคลเป็นจำนวนมาก ประตูหน้าต่างของสำนักงานหรือห้องต้องใส่กุญแจเสมอเป็นต้น
2) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่าง เหมาะสม วิธีการทำลายข้อมูล สื่อบันทึกวัสดุ และอุปกรณ์เหล่านี้โดยปฏิบัติตามเอกสารวิธีปฏิบัติงานเรื่องการ ทำลายสื่อบันทึกข้อมูล
3) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อมอื่น ๆ (Protecting Against External and Environmental Threats)

หน่วยงานต้องมีการป้องกันจากการถูกทำลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น

5.1.5 การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Working in Secure Areas)

1) หัวหน้าของแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในบริเวณนั้น เป็นต้น
2) หน่วยงานต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวีดีโอ” และ “ห้าม สูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

<u>นโยบาย</u>

5.2.1 การจัดตั้งและการป้องกันอุปกรณ์ (Equipments Setting and Protection)

เจ้าหน้าที่สารสนเทศต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิด ขึ้นกับอุปกรณ์เหล่านั้น

5.2.2 การดูแลอุปกรณ์ต่าง ๆ (Supporting Utilities)

1) เจ้าหน้าที่สารสนเทศต้องกำหนดให้มีระบบกระแสไฟฟ้าสำรอง เช่นใช้ Uninterruptible Power Supply (UPS) เป็นต้น
2) เจ้าหน้าที่สารสนเทศต้องมีการตรวจสอบระบบไฟฟ้าสำรอง อย่างสม่ำเสมอ

5.2.3 การเดินสายไฟและสายเคเบิล (Cabling Security)

1) เจ้าหน้าที่สารสนเทศกำหนดให้มีการติดตั้งสายไฟฉุกเฉินในจุดที่มีความสำคัญต่อการปฏิบัติงานเช่น ห้องคอมพิวเตอร์แม่ข่าย (Data Center) เป็นต้น
2) บริเวณที่มีการเดินสายเคเบิลเข้ามาภายในอาคารสำนักงาน และมีการติดตั้งตู้พักสายต้องล็อคไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่ที่มีสิทธิ์เท่านั้น

5.2.4 การดูแลรักษาอุปกรณ์ (Equipment Maintenance)

เจ้าหน้าที่สารสนเทศต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีแผนบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอย่างน้อยปีละ 1 ครั้ง เป็นต้น

5.2.5 การป้องกันอุปกรณ์และทรัพย์สินสารสนเทศที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises)

หน่วยงานต้องกำหนดให้มีการป้องกันทรัพย์สินและอุปกรณ์ของหน่วยงาน เช่น เครื่องคอมพิวเตอร์โน๊ตบุ๊ค, อุปกรณ์ต่อพ่วงต่างๆ เป็นต้น เมื่อถูกนำไปใช้งานนอกหน่วยงาน จะต้องมีการบันทึกการยืม - คืนอุปกรณ์

5.2.6 การจัดการอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้ใหม่ (Secure Disposal or Re-use of Equipment)

หน่วยงานสารสนเทศต้องกำหนดให้มีวิธีการในการตรวจสอบอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น ทั้งนี้ เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าวก่อนนำอุปกรณ์ไปแจกจ่าย

5.2.7 การนำอุปกรณ์ออกนอกพื้นที่ (Removal of Property)

อุปกรณ์ ข้อมูลหรือซอฟต์แวร์จะต้องได้รับการอนุญาตจากผู้ที่เกี่ยวข้องก่อนนำออกจากโรงพยาบาล

หมวดที่ 6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของ เครือข่ายสารสนเทศขององค์กร (Communications and Operations Management)

6.1 การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational Procedures and Responsibilities)

วัตถุประสงค์ : เพื่อให้การปฏิบัติงานและการบริหารจัดการโครงสร้างพื้นฐานด้านสารสนเทศเป็นไปอย่าง ถูกต้องและปลอดภัย

<u>นโยบาย</u>

6.1.1 คู่มือและขั้นตอนการปฏิบัติงาน (Documented Operation Procedures)

1) หน่วยงานสารสนเทศต้องจัดทำคู่มือและ/หรือขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน เช่น ขั้นตอนการแจ้ง เหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอน การปฏิบัติ และเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ
2) คู่มือและขั้นตอนการปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนและผู้รับผิดชอบการ ปฏิบัติงานนั้น ๆ คู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนเมื่อมีการเปลี่ยนแปลงสำคัญเกิดขึ้น
3) หน่วยงานสารสนเทศมีการกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระการทำละเมิด

6.1.2 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties)

หน่วยงานสารสนเทศต้องมีการกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศและ เครือข่ายให้เกิดความชัดเจน เพื่อหลีกเลี่ยงการใช้งานสินทรัพย์ผิดวัตถุประสงค์ หรือโดยไม่มีสิทธิ์

6.1.3 การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนาและทดสอบ (Separation of development, test and operational facilities)

หน่วยงานสารสนเทศต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ควรมีการแยกเครื่องกับระบบที่ใช้งานจริง หากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริง

6.2 การจัดการผู้ให้บริการภายนอก (Third Party Service Delivery Management)

วัตถุประสงค์ : เพื่อให้มีและคงไว้ซึ่งระดับการรักษาความปลอดภัยสารสนเทศ และระดับการให้บริการที่เหมาะสมและสอดคล้องกับข้อตกลงการบริการกับหน่วยงานภายนอก

นโยบาย

6.2.1 การส่งมอบบริการ (Service Delivery)

ทางโรงพยาบาลต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการของหน่วยงานภายนอก โดยต้องประกอบไปด้วย รายละเอียด ดังนี้

1) การยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร
2) ขอบเขต รายละเอียด และระดับการให้บริการ (Service Level Agreement)
3) เอกสารต่าง ๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้านกายภาพและด้าน Logical เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัยสารสนเทศได้ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
4) ข้อตกลงการเชื่อมโยงระบบเครือข่ายของหน่วยงานภายนอก
5) ข้อมูลที่หน่วยงานภายนอกสามารถเข้าถึงได้และขั้นตอนและวิธีการร้องขอข้อมูลขององค์กรกรณี ต้องการข้อมูลเพิ่มเติม
6) สัญญาในการไม่เปิดเผยข้อมูลขององค์กร
7) การยืมหรือการร้องขอใช้อุปกรณ์ขององค์กร
8) ข้อกำหนดทางด้านกฎหมาย เช่น ความลับส่วนบุคคล (Privacy) และการป้องกันข้อมูล

6.2.2 การทบทวนและตรวจสอบบริการจากผู้ให้บริการภายนอก (Monitoring and Review of Third Party Services)

ต้องจัดทำข้อตกลง กำหนดสิทธิ์สำหรับผู้ให้บริการที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของผู้ให้บริการภายนอก

6.2.3 การจัดการการเปลี่ยนแปลงบริการจากผู้ให้บริการภายนอก (Managing Changes to Third Party Services)

การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอกที่เกี่ยวข้องกับบริการด้านสารสนเทศขององค์กรทุกครั้ง ต้องเป็นไปตามเอกสารวิธีปฏิบัติงานเรื่องการให้บริการของหน่วยงานภายนอก

6.3 การวางแผนและการยอมรับระบบสารสนเทศ (System Planning and Acceptance)

วัตถุประสงค์ : เพื่อลดความเสี่ยงต่อการเกิดความล้มเหลวของระบบลงให้เหลือน้อยที่สุด

<u>นโยบาย</u>

6.3.1 การจัดการขีดความสามารถ (Capacity Management)

1) หน่วยงานสารสนเทศต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถทรัพยากรด้านเทคโนโลยีสารสนเทศปัจจุบันอย่างสม่ำเสมอ
2) หน่วยงานสารสนเทศต้องมีการวางแผนจัดการขีดความสามารถของระบบอย่างน้อยปีละ 1 ครั้งโดยพิจารณาจากความต้องการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศ เช่น CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น การเปลี่ยนแปลงของเทคโนโลยี เป็นต้น
3) แผนการจัดการขีดความสามารถของระบบต้องประกอบด้วยวิธีการจัดการขีดความสามารถ อาทิ การ Tunning

6.4 การป้องกันซอฟต์แวร์ไม่ประสงค์ดี (Protection Against Malicious and Mobile Code)

วัตถุประสงค์ : เพื่อเป็นแนวทางการป้องกันให้ซอฟต์แวร์และข้อมูลสารสนเทศจากซอฟต์แวร์ไม่ประสงค์ดี ต่าง ๆ

นโยบาย

6.4.1 การควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls Against Malicious Code)

1) เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์โน๊ตบุ๊ค ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส รุ่นล่าสุดที่ได้รับการอนุมัติจากหน่วยงานสารสนเทศและต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง โดยปฏิบัติตามเอกสารวิธีปฏิบัติงานเรื่องการจัดการควบคุมซอฟต์แวร์ไม่ประสงค์ดี (Controls Against Malicious Code Procedure)
2) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Latest Pattern) อยู่เสมอ เครื่องให้บริการ เครื่องคอมพิวเตอร์และโน้ตบุ๊คทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส
3) เอกสารการตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก 6 เดือน
4) ห้ามเจ้าหน้าที่ทำการดาวน์โหลดแชร์แวร์หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต โดยปราศจากการอนุมัติ จากหน่วยงานสารสนเทศหลังจากการอนุมัติแล้ว เจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัส ก่อนการใช้งาน
5) ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล์ สำเนาจากแผ่นดิส หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัส
6) ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใด ๆ ตัวอย่างเช่น ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง (ม้าโทรจัน) อีเมล์บอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ขององค์กร
7) ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส
8) ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้นที่ได้รับอนุญาตให้สามารถรับ- ส่งผ่านระบบเครือข่ายขององค์กรได้ ทั้งนี้ ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสขององค์กร ก่อนเปิดใช้งานเสมอ

6.4.2 การควบคุมโปรแกรมชนิดเคลื่อนที่ได้ (Controls Against Mobile Code)

เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์โน๊ตบุ๊ค ต้องได้รับการปรับค่าติดตั้งอย่างเหมาะสม เพื่อป้องกัน Active Code ต่าง ๆ (เช่น Java, Active X) จากแหล่งที่ไม่น่าเชื่อถือในอินเทอร์เน็ต

6.5 นโยบายการสำรองข้อมูล (Information Back-up)

วัตถุประสงค์: เพื่อเป็นแนวทางในการกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุการณ์ต่าง ๆ เช่น ภัยธรรมชาติ ระบบเสียหาย ฯลฯ

นโยบาย

6.5.1 นโยบายการสำรองข้อมูล (Information Back-up)

1) หน่วยงานสารสนเทศต้องกำหนดความถี่ในการทำการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบ โดยปฏิบัติตามเอกสารวิธีปฏิบัติงานเรื่องการจัดการการสำรองข้อมูลสารสนเทศ (Backup & Restore Procedure)
2) หน่วยงานสารสนเทศต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพ สามารถใช้งานได้ตลอดเวลา
3) หน่วยงานสารสนเทศต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ
4) หน่วยงานสารสนเทศต้องกำหนดระยะเวลาในการสำรองข้อมูลตามระดับการบริหารความเสี่ยง
5) หน่วยงานสารสนเทศต้องมีกระบวนการสำรองข้อมูลและการกู้ข้อมูลของทุกระบบ ต้องมีการทำเอกสาร และมีการตรวจสอบเป็นระยะ ๆ
6) หน่วยงานสารสนเทศต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล และการเรียกคืนข้อมูลในแต่ละครั้ง
7) ข้อมูลสำรองต้องได้รับการทดสอบเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์
8) หน่วยงานสารสนเทศต้องลงบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูล ต้องได้รับการตรวจสอบเป็นประจำทุกปี

9) กระบวนการในการเก็บข้อมูลระหว่างสถานที่ระบบคอมพิวเตอร์และสถานที่เก็บข้อมูลต้องได้รับการตรวจสอบอย่างน้อยปีละ 1 ครั้ง

10) สื่อที่ใช้เก็บข้อมูลต้องมีป้ายบอกรายละเอียด ซึ่งประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
    - ชื่อระบบ
    - วันสร้าง
    - ระดับความสำคัญของข้อมูล
    - รายละเอียดติดต่อผู้ดูแลข้อมูล

6.6 การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

วัตถุประสงค์: เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายขององค์กร

นโยบาย

6.6.1 การบริหารและจัดการด้านความมั่นคงปลอดภัยบนเครือข่าย (Network Controls)

1) หน่วยงานสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด
2) การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย
3) หน่วยงานสารสนเทศ ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและเครือข่ายที่หน่วยงานนั้นรับผิดชอบ
4) หน่วยงานสารสนเทศ ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งหน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย
5) บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานขององค์กรด้วย

6.6.2 ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Services)

1) ระบบเครือข่ายทั้งหมดของโรงพยาบาลที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

2) หน่วยงานสารสนเทศ ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของโรงพยาบาลและต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่าย ที่เป็นส่วนที่ใช้งานจริงของโรงพยาบาลทั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายโรงพยาบาลได้
3) ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของ โรงพยาบาลโดยไม่ได้รับอนุญาตจากหน่วยงานสารสนเทศ
4) ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลโดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง
5) ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router , Switch , Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด
6) ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของโรงพยาบาลทำการเชื่อมต่อออกไปยังเครือข่ายภายนอก ผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในโรงพยาบาลโดยเด็ดขาด

6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media Handing)

วัตถุประสงค์: ป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลขององค์กร

นโยบาย

6.7.1 การบริหารและจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้(Management Of Removable Media)

หน่วยงานสารสนเทศ ต้องกำหนดวิธีการปฏิบัติและสิทธิ์สำหรับการใช้งานสื่อบันทึกข้อมูล โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการลงทะเบียนสื่อเคลื่อนที่ และสอบทานการใช้งาน

6.7.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

1) หน่วยงานสารสนเทศควรจัดทำระเบียบวิธีปฏิบัติงานสำหรับการทำลายสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึกข้อมูล (Disposal of media)

2) การทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูลจะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม
3) หน่วยงานสารสนเทศ ควรทำลายสื่อที่ใช้ในการบันทึกข้อมูล เอกสาร และอุปกรณ์สำนักงานภายใต้สิ่งแวดล้อมที่ได้มีการควบคุม (Controlled Environment)

6.7.3 วิธีการปฏิบัติในการจัดการสื่อบันทึกข้อมูล (Information Handing Procedures)

1) หน่วยงานสารสนเทศ ต้องมีการจัดการข้อมูล โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการจัดการทรัพย์สินสารสนเทศขององค์กร
2) หน่วยงานสารสนเทศ ต้องมีการจัดการด้านการป้องกันการรั่วไหลหรือเปิดเผยออกไป โดยมีแนวทางปฏิบัติ ดังนี้
   - ต้องมีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน
   - กำหนดบุคลากรที่มีสิทธิ์ในการใช้งาน
   - ต้องเก็บสื่อบันทึกไว้ในสถานที่และสิ่งแวดล้อมที่ปลอดภัยจากการเสียหายที่อาจเกิดขึ้นได้ เช่น อุณหภูมิสูงหรือต่ำเกินไป

6.7.4 การจัดการเอกสารที่เกี่ยวกับระบบสารสนเทศขององค์กรอย่างปลอดภัย (Security of System Documentation)

1) หน่วยงานสารสนเทศต้องมีการกำหนดวิธีปฏิบัติและสิทธิ์สำหรับการใช้เอกสารที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงานให้ชัดเจน
2) หน่วยงานสารสนเทศ ต้องมีการเก็บรักษาเอกสารที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรอย่างเหมาะสม
3) หน่วยงานสารสนเทศ ต้องป้องกันการรั่วไหล หรือการเปิดเผยของข้อมูลที่สำคัญที่อยู่ในเอกสารที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร

6.8 การแลกเปลี่ยนข้อมูลสารสนเทศ (Exchange Of Information)

วัตถุประสงค์: เพื่อป้องกันการสูญหายของสารสนเทศและซอฟต์แวร์ รวมทั้งเพื่อป้องกันการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต หรือการนำสารสนเทศไปใช้ในทางที่ไม่เหมาะสม

<u>นโยบาย</u>

6.8.1 นโยบายและกระบวนการแลกเปลี่ยนข้อมูลสารสนเทศ (Information Exchange policies and procedures)

หน่วยงานสารสนเทศ ต้องมีการดำเนินการแลกเปลี่ยนสารสนเทศ โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการแลกเปลี่ยนสารสนเทศ (Information Exchange Procedure)

6.8.2 สัญญาและข้อกำหนดในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements)

หน่วยงานสารสนเทศ ต้องมีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูล โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการแลกเปลี่ยนสารสนเทศ (Information Exchange Procedure)

6.8.3 การจัดส่งสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัย (Physical Media in Transit)

หน่วยงานสารสนเทศ ต้องมีวิธีการจัดส่งสื่อบันทึกข้อมูล (สารสนเทศซอฟต์แวร์) ให้มีความมั่นคงปลอดภัย โดยปฏิบัติตามวิธีปฏิบัติงานเรื่องการส่งผ่านสื่อบันทึกข้อมูล (Physical Media in Transit)

6.8.4 การรักษาความมั่นคงปลอดภัยข้อมูลอิเล็กทรอนิกส์ (Electronic Messaging)

หน่วยงานสารสนเทศ ต้องมีการกำหนดวิธีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

6.8.5 ข้อมูลเผยแพร่ต่อสาธารณะ (Publicly available information)

ข้อมูลเผยแพร่ต่อสาธารณะมีการป้องกันการแก้ไขโดย หน่วยงานสารสนเทศ ต้องมีการทบทวนความเที่ยงตรงและถูกต้องของข้อมูล

6.9 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

วัตถุประสงค์ : เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

นโยบาย

6.9.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging)

หน่วยงานสารสนเทศ ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้ โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการเฝ้าระวังการใช้งานระบบ (System Usage Monitoring Procedure)

6.9.2 การตรวจสอบการใช้งานระบบ (Monitoring System Use)

หน่วยงานสารสนเทศ ต้องกำหนดให้ตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่ โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการเฝ้าระวังการใช้งานระบบ (System Usage Monitoring Procedure)

6.9.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log Information)

หน่วยงานสารสนเทศ ต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับกาการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

6.9.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and Operator Logs)

หน่วยงานสารสนเทศ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่น ๆ รวมถึงอุปกรณ์คอมพิวเตอร์และเครือข่าย

6.9.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging)

หน่วยงานสารสนเทศ ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศวิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามความเหมาะสม

6.9.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock Synchronization)

หน่วยงานสารสนเทศ ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ในหน่วยงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกระบุตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ขององค์กรถูกบุกรุกตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

หมวดที่ 7 การควบคุมการเข้าถึง (Access Control)

7.1 การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

วัตถุประสงค์: เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย

นโยบาย

7.1.1 นโยบายควบคุมการเข้าถึง (Access Control Policy)

1) หน่วยงานสารสนเทศมีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการบริหารจัดการบัญชีผู้ใช้งาน
2) หน่วยงานสารสนเทศต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาตามความจำเป็นในการใช้งาน
3) ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้
4) หน่วยงานสารสนเทศต้องมีการบันทึก (Log)และติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ
   หน่วยงานสารสนเทศต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

7.2 การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

วัตถุประสงค์: เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

นโยบาย

7.2.1 การลงทะเบียนผู้ใช้งานใหม่ (User Registration)

การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการบริหารจัดการผู้ใช้งาน โดยผู้ใช้งานต้องได้รับการทบทวน และพิจารณาอนุมัติตามขั้นตอนขององค์กรอย่างเคร่งครัด

7.2.2 การบริหารสิทธิ์การเข้าถึงระบบของผู้ใช้งานระบบ (Privilege Management)

1) หน่วยงานสารสนเทศต้องกำหนดสิทธิ์ของผู้ใช้งานและแยกตามหน้าที่ความรับผิดชอบในการเข้าถึงระบบสารสนเทศแต่ละระบบ
2) ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ

7.2.3 การบริหารจัดการรหัสผ่านผู้ใช้งาน (User Password Management)

หน่วยงานสารสนเทศต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยอยู่เสมอ ตามคู่มือการปฏิบัติงานเรื่องการบริหารจัดการบัญชีผู้ใช้งาน

7.2.4 การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

หน่วยงานสารสนเทศต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง ตามคู่มือการปฏิบัติงานเรื่องการบริหารจัดการบัญชีผู้ใช้งาน

7.3 การรับผิดชอบหน้าที่ของผู้ใช้งาน (User Responsibilities)

วัตถุประสงค์: เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ สามารถเข้าถึงระบบสารสนเทศได้

นโยบาย

7.3.1 การใช้งานรหัสผ่าน (Password Use)

1) ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ
2) ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศขององค์กร การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่านและการจัดการควบคุมการใช้รหัสผ่าน
3) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
   - ควรได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาและผู้ดูแลระบบงานนั้น ๆ
   - ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
   - ควรกำหนดระยะเวลาในการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
   - ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด
4) ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษา User Name และรหัสผ่านของตนเอง รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้ ให้มีความมั่นคงปลอดภัยอย่างสม่ำเสมอ
5) รหัสผ่านต้องได้รับการเปลี่ยนแปลงเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้
6) รหัสผ่านต้องมีความมั่นคงปลอดภัยตามที่ได้กำหนดไว้ในวิธีการปฏิบัติงานเรื่องแนวทางการใช้เทคโนโลยีสารสนเทศ และการสื่อสาร
7) รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัยห้ามใช้ Account ร่วมกันหรือให้ผู้อื่นเข้าใช้งาน Account ของตนโดยเด็ดขาด
8) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่าน User ID และรหัสผ่านของตนทั้งหมด

9) รหัสผ่านของ Account ที่มีสิทธิพิเศษในระบบสำคัญขององค์กรต้องได้รับการควบคุมโดยหน่วยงานสารสนเทศหรือผู้ที่ได้รับมอบหมายหน้าที่อย่างเป็นทางการ

10) ผู้ใช้งานทุกคนต้องได้รับการฝึกอบรมเพื่อให้มีความรู้และความตระหนักในการใช้งานรหัสผ่านอย่างถูกต้อง และรับทราบเทคนิคต่าง ๆ ที่ใช้ในการหลอกลวงและนำไปสู่การโจรกรรมข้อมูล

11) ระบบหรือการกระทำใด ๆ ที่ไม่สอดคล้องกับนโยบายฉบับนี้ต้องได้รับการบันทึกประเมิน และพิจารณาอนุมัติอย่างเหมาะสม

12) หากผู้ใช้งานสงสัยว่า User ID หรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อหน่วยงานสารสนเทศและทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที

7.3.2 การควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy)

เจ้าหน้าที่ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสิ่งต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอ คอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญ ปรากฏในขณะไม่ได้ใช้งาน

7.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

วัตถุประสงค์: เพื่อควบคุมการใช้บริการบนเครือข่ายขององค์กร

<u>นโยบาย</u>

7.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on Use of Network Services)

1) หน่วยงานสารสนเทศต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะเพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศ อาทิ
   - ใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย อาทิ Secure Socket Layer (SSL) Simple Network Management Protocol (SNMP)
   - จำกัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ Bandwidth เช่น การรับ – ส่งไฟล์ขนาดใหญ่ ฟังเพลงออนไลน์ ดูทีวีออนไลน์ หรือ เล่นเกมส์ออนไลน์ ในช่วงเวลาทำการ ยกเว้นกรณีที่ได้รับอนุญาต
2) ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ

- อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายทั้งหมดต้องได้รับการตั้งค่าให้มีความปลอดภัยและการมีการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย
- ระบบสายสัญญาณต้องได้รับมาตรฐานอุตสาหกรรมและได้รับการติดตั้งโดยผู้ที่มีความชำนาญที่ผ่านการพิจารณาอนุมัติแล้ว
- อุปกรณ์เครือข่าย อาทิ Router , Firewall , Switch , Wireless Access Point ต้องได้รับการติดตั้งค่าตามความจำเป็นด้านความมั่นคงปลอดภัยของอุปกรณ์นั้น ๆ หรือตามคำแนะนำขององค์กรด้านความมั่นคงปลอดภัยต่าง ๆ อาทิ SANS Institute หรือ NSA
- IP Address ต้องได้รับการลงทะเบียน แจกจ่ายและบริหารจัดการโดยเจ้าหน้าที่สารสนเทศ
- อุปกรณ์เครือข่ายที่สำคัญ เช่น Router , Core Switch ต้องมีอุปกรณ์สำรองไฟฟ้า (UPS) เสมอ
- การเปลี่ยนแปลงระบบเครือข่ายหรืออุปกรณ์เครือข่ายต้องได้รับการควบคุมโดยปฏิบัติตามคู่มือปฏิบัติงานเรื่องการจัดการการเปลี่ยนแปลงระบบคอมพิวเตอร์ (Change Management Procedure)
- ระบบเครือข่ายต้องได้รับการออกแบบหรือตั้งค่าให้ทำงานได้อย่างมีประสิทธิภาพ (Reliable) มีความยืดหยุ่น (Flexible) รวมถึงสามารถรองรับการขยายตัวและความต้องการใช้งานในอนาคต (Scalable)

3) ข้อตกลงการให้บริการเครือข่ายต้องระบุถึงรายละเอียด และข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ และการบริหารจัดการบริการเครือข่ายทั้งหมด หากบริการเครือข่ายนั้นได้รับการดำเนินการโดยหน่วยงานภายนอก ต้องมีการระบุถึงสิทธิของบริษัทฯ ในการติดตามตรวจสอบ และตรวจประเมินการทำงานของหน่วยงานภายนอกด้วย

7.4.2 การพิสูจน์ตัวตนของการเชื่อมต่อจากภายนอก (User authentication for external connections)

เจ้าหน้าที่สารสนเทศต้องมีกลไกในการพิสูจน์ตัวตนที่เหมาะสมในการควบคุมการเข้าถึงของผู้ใช้งานจากภายนอก โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการบริหารจัดการผู้ใช้งาน (User Management Procedure)

7.4.3 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic And Configuration Port Protection)

1) หน่วยงานสารสนเทศต้องมีการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ และต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
2) พอร์ตที่ไม่เกี่ยวข้องกับการปฏิบัติงานหรือการดำเนินงานต้องถูกระงับการใช้งาน

7.4.4 การจัดการแบ่งเครือข่ายภายในองค์กรกับภายนอกองค์กร (Segregation in Networks)

1) หน่วยงานสารสนเทศต้องออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีใช้งานแบ่งตามกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ
2) หน่วยงานสารสนเทศต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

7.4.5 การควบคุมผู้ใช้งานในการใช้งานเครือข่าย (Network Connection Control)

1) หน่วยงานสารสนเทศต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้นและให้ผู้ใช้งานปฏิบัติตามนโยบายเรื่อง การอนุญาตให้ใช้สินทรัพย์
2) บริการเครือข่าย (Network services) ที่ไม่เกี่ยวข้องกับการปฏิบัติงานหรือการดำเนินงานต้องถูกระงับการใช้งาน

7.4.6 การจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน (Network Routing Control)

1) หน่วยงานสารสนเทศต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน ดังนี้
   - ตรวจสอบความน่าเชื่อถือของต้นทางและปลายทางเพื่อควบคุมการเชื่อมต่อให้เป็นไปตามที่กำหนดไว้ใน Routing Table เท่านั้น เพื่อป้องกันการเชื่อมต่อกับเครือข่ายที่ไม่เหมาะสม
   - ตรวจสอบเส้นทางการเชื่อมต่อที่กำหนดไว้ใน Routing Table อย่างสม่ำเสมอ
   - IP Address ของเครือข่ายภายในต้องไม่ถูกเปิดเผยต่อเครือข่ายภายนอก อาทิ การใช้เทคโนโลยี Network Address Translation (NAT)

7.5 การควบคุมการใช้งานระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์: เพื่อป้องกันการใช้งานระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

7.5.1 กระบวนการเข้าถึงระบบ (Secure Log – on Procedures)

หน่วยงานสารสนเทศต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะปฏิเสธการใช้งานหากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน 5 ครั้ง เป็นต้น

7.5.2 การพิสูจน์ตัวตนสำหรับผู้ใช้งานระบบ (User Identification and Authentication)

เจ้าหน้าที่สารสนเทศต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานระบบเป็นรายบุคคล ก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

7.5.3 การบริหารจัดการรหัสผ่าน (Password Management System)

หน่วยงานสารสนเทศต้องจัดให้มีระบบหรือวิธีในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

7.5.4 การควบคุมการใช้งานโปรแกรมยูทิลิตี้ (User of System Utilities)

หน่วยงานสารสนเทศต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ผู้ใช้งานระบบ เป็นต้น

7.5.5 การกำหนดเวลาการใช้งานระบบ (Session Time – out)

หน่วยงานสารสนเทศต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย เมื่อเครื่องคอมพิวเตอร์ลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อกหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ

7.6 การควบคุมการใช้งานระบบสารสนเทศและสารสนเทศ (Application and Information Access Control)

วัตถุประสงค์: เพื่อป้องกันการใช้งานระบบสารสนเทศและสารสนเทศโดยไม่ได้รับอนุญาต

นโยบาย

7.6.1 การจำกัดการใช้งานสารสนเทศ (Information Access Restriction)

1) หน่วยงานสารสนเทศต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน
2) บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น
3) บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ขององค์กรอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร

7.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive System Isolation)

หน่วยงานสารสนเทศต้องมีการแยกระบบสารสนเทศที่มีความสำคัญ หรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้ในองค์กร เป็นต้น

7.7 การควบคุมการเข้าถึงข้อมูลสารสนเทศ (Information Technology Access Control)

วัตถุประสงค์: เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

นโยบาย

7.7.1 การเข้าถึงข้อมูลสารสนเทศ (Information Technology Access)

สิทธ์การเข้าถึงไฟล์ข้อมูลสารสนเทศต้องได้รับการควบคุม และได้รับการพิจารณาอนุมัติเท่าที่จำเป็นเท่านั้น เพื่อให้ไฟล์ข้อมูลสารสนเทศได้รับการรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ รวมทั้งเป็นการแบ่งแยกสิทธิ์ และหน้าที่ของผู้ใช้งาน

7.8 คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถานที่ (Mobile Computing)

วัตถุประสงค์: เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาได้ รวมทั้งการปฏิบัติงานนอกสำนักงานให้เป็นไปอย่างปลอดภัย

นโยบาย

7.8.1 การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Mobile Computing and Communications)

หน่วยงานสารสนเทศต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook , Palmtops , Laptop) และอุปกรณ์สื่อสารอื่น ๆ เช่น เมื่อปฏิบัติงานนอกสถานที่

- ต้องใส่รหัสผ่านป้องกันหน้าจอทุกครั้ง
- ต้องใส่รหัสผ่านป้องกันข้อมูลที่สำคัญ

หมวดที่ 8 การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development, and Maintenance)

8.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

วัตถุประสงค์: เพื่อการสร้างความปลอดภัยให้กับระบบสารสนเทศ

นโยบาย

8.1.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัย (Security Requirements Analysis and Specification)

1) สำนักเทคโนโลยีสารสนเทศ กลุ่มโรงพยาบาลวิชัยเวช ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือ ซื้อมาใช้งาน
2) หน่วยงานดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้
   - มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย เช่น การสำรองข้อมูล ระบบเครือข่ายสำรอง เป็นต้น
   - มาตรการปฏิบัติหลังจากเกิดความเสียหาย เช่น แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล เป็นต้น

8.2 ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ (Security of System Files)

วัตถุประสงค์: เพื่อให้โครงการสารสนเทศได้รับการดำเนินการอย่างปลอดภัย

นโยบาย

8.2.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of Operational Software)

ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่ โดยปฏิบัติตามวิธีการปฏิบัติเรื่องการควบคุมระบบสารสนเทศที่ใช้ในการปฏิบัติงาน (Control of operational software)

8.2.2 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code)

1) ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานหรือให้บริการ เช่น
   - ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย
   - ต้องไม่เก็บ Source Code ที่อยู่ระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

8.3 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

วัตถุประสงค์: เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย

<u>นโยบาย</u>

8.3.1 กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (Change Control Procedures)

1) ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานได้จริง หรือให้บริการอยู่แล้ว เช่น
   - คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์
   - ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
   - ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
   - เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
   - ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

   โดยปฏิบัติตามวิธีการปฏิบัติเรื่อง การจัดการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Procedure)

8.3.2 การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications after Operating System Changes)

เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่าง ๆ ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

8.3.3 การควบคุมการเปลี่ยนแปลงซอฟท์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

8.3.4 การควบคุมการรั่วไหลของข้อมูล (Information Leakage)

ผู้พัฒนาระบบสารสนเทศต้องมีการป้องกันโอกาสการรั่วไหลของข้อมูล

8.3.5 การควบคุมการว่าจ้างการพัฒนาระบบ (Outsourced Software Development)

ในการทำสัญญาว่าจ้างการพัฒนาระบบของกลุ่มโรงพยาบาลวิชัยเวชฯ ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

หมวดที่ 9 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(Information Security Incident Management)

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคง (Reporting Information Security Events and Weaknesses)

วัตถุประสงค์: เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

นโยบาย

9.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events)

1) ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานของคณะกรรมการบริหารความเสี่ยงตามที่ได้กำหนดไว้
2) ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในองค์กรต่อผู้บังคับบัญชา หรือหน่วยงานจัดการความปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที
3) ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อคณะกรรมการบริหารความเสี่ยงทันที
4) ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย ต้องรายงานต่อคณะกรรมการบริหารความเสี่ยงทันทีทันที
5) ผู้ใช้งานและบุคคลภายนอก ที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในองค์กรต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา และคณะกรรมการบริหารความเสี่ยง และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง
6) การกระทำอื่น ๆ ที่ถือเป็นข้อห้ามขององค์กรมีดังนี้
    1. การกระทำใด ๆ ที่กฎหมายบัญญัติว่าเป็นความผิด ตลอดจนการกระทำในลักษณะอื่น ๆ ที่กล่าวถึงด้านล่างนี้ถือเป็นข้อห้ามขององค์กรที่ไม่ยินยอมให้พนักงานดำเนินการโดยเด็ดขาด ทั้งนี้มิได้เขียนระบุถึงข้อห้ามทั้งหมดที่ห้ามกระทำไว้ แต่เขียนเพื่อเป็นแนวทางให้แก่ผู้ใช้งานได้รับทราบเท่านั้น

หมายเหตุ : พนักงานบางส่วนอาจได้รับยกเว้นจากข้อห้ามบางข้อที่กล่าวไว้ด้านล่างนี้ (ตราบเท่าที่ไม่ขัดต่อกฎหมาย) หากเป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย เช่น ผู้ดูแลระบบสามารถระงับการเข้าถึงเครือข่ายของอุปกรณ์ใด ๆ หากการเข้าถึงนั้นรบกวนการทำงานของระบบเทคโนโลยีสารสนเทศ

2. การใช้งานทรัพยากรขององค์กรเพื่อการจัดหาหรือส่งต่อ วัสดุ เอกสาร หรือรูปภาพลามกอนาจารหรือที่ขัดต่อกฎหมาย
3. การฉ้อโกงโดยใช้ User ID และรหัสผ่านที่กำหนดให้ เพื่อเสนอขายสินค้าหรือบริการใด ๆ
4. การพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่าย
5. ตัวอย่างของการล่วงละเมิด ได้แก่ การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ตนไม่ได้รับอนุญาต เป็นต้น ส่วนตัวอย่างของการรบกวนการทำงานของระบบเครือข่าย ได้แก่ Sniffing, Pinged Floods , Pack Spoofing , Denial of Service และ Forged Routing Information ด้วยเจตนามุ่งร้าย เป็นต้น
6. การใช้งาน Bandwidth จำนวนมากโดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P File Sharing
7. การทำPort Scanning และ Security Scanning เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
8. การดักฟังหรือดักจับข้อมูลที่พนักงานไม่ได้รับอนุญาตให้รับรู้ด้วยวิธีการใด ๆ เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
9. การค้นหาจุดบกพร่องของระบบ เพื่อทำการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
10. การหลบเลี่ยงการพิสูจน์ตัวตนผู้ใช้งานหรือมาตรฐานด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ ระบบเครือข่ายใด ๆ
11. การใช้โปรแกรม / สคริปต์ / คำสั่งหรือการส่งข้อความใด ๆ โดยมีเจตนารบกวน ลดประสิทธิภาพการให้บริการ หรือระงับการใช้งานของผู้ใช้งาน ทั้งโดยผ่านระบบภายใน หรือผ่านระบบเครือข่ายต่าง ๆ
12. การให้ข้อมูลลับเกี่ยวกับรายชื่อพนักงาน รายชื่อลูกค้า ความลับขององค์กร และข้อมูลลับอื่น ๆแก่บุคคลภายนอก

13. การข่มขู่คุกคามทุกรูปแบบผ่านอีเมล์ โทรศัพท์ หรือระบบส่งข้อความ ไม่ว่าจะด้วยภาษาความถี่ หรือขนาดของข้อความ การแสดงความคิดเห็น หรือส่งข้อความใด ๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจำนวนมาก (Newsgroup Spam)
14. การละเมิดสิทธิส่วนบุคคล ลิขสิทธิ์ขององค์กรความลับขององค์กร สิทธิบัตร ทรัพย์สินทางปัญญาหรือกฎหมายอื่นใด

9.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting Security Weaknesses)

ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of Information Security Incidents Improvements)

วัตถุประสงค์: เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศของหน่วยงาน

นโยบาย

9.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

9.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from Security Incidents)

ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

9.2.3 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

หน่วยที่ 10 การบริหารความต่อเนื่องของการดำเนินงานขององค์กร(Business Continuity Management)

10.1 การจัดการความต่อเนื่องของการดำเนินงานองค์กร (Aspects of Business Continuity)

วัตถุประสงค์: เพื่อป้องกันการหยุดชะงักในการดำเนินงานขององค์กรที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ

นโยบาย

10.1.1 ขอบเขตของการดำเนินกระบวนการจัดการความต่อเนื่องต้องครอบคลุมถึงการรักษาความปลอดภัยสารสนเทศ (Including Information Security in the Business Continuity Management Process)

1) กลุ่มโรงพยาบาลวิชัยเวชฯ ต้องจัดตั้งคณะกรรมการ IMC (คณะกรรมการสารสนเทศและเวชสถิติ) ซึ่งประกอบไปด้วยตัวแทนจากสำนักเทคโนโลยีสารสนเทศ หน่วยงานเจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลข้อมูล เป็นต้น
2) IMC ต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงจัดให้มีการทดสอบแผนอย่างน้อยปีละหนึ่งครั้งโดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการจัดทำแผนการบริหารความต่อเนื่องให้กับธุรกิจ (Business Continuity Plans Development and Execution Procedure)

10.1.2 กระบวนการจัดการความต่อเนื่องและการประเมินความเสี่ยง (Business Continuity and Risk Assessment)

1) มีการระบุเหตุการณ์ที่เป็นผลให้กระบวนการทางธุรกิจหยุดชะงักและความเป็นไปได้ของผลกระทบที่จะเกิดขึ้นซึ่งเป็นผลเนื่องมาจากการรักษาความมั่นคงปลอดภัยสารสนเทศ
   - การพัฒนาแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ (IT Contingency plan Development)
   - การประชาสัมพันธ์และการฝึกอบรม
   - การทดสอบปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ

10.1.3 การจัดทำและการประยุกต์ใช้แผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ

(Developing and Implementing Continuity Plans Including Information Security)

1) IMC ต้องจัดทำแนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ควรพิจารณาดังนี้
   - เตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินงานขององค์กรและการให้บริการด้วยเทคโนโลยีสารสนเทศของ VIH
   - การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่นกำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
   - การดำเนินการเพื่อให้สามารถดำเนินงานขององค์กรเป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหายเป็นต้น
   - การกลับสู่การทำวันงานปกติ เพื่อให้การดำเนินงานของ VIH กลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

10.1.4 กรอบโครงสร้างของขอบเขตของแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

(Business Continuity Planning Framework)

1) IMC ต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศต้องประกอบไปด้วยองค์ประกอบอย่างน้อยดังนี้
   - ชื่อแผน
   - วัตถุประสงค์
   - ขอบเขตของแผน
   - รายละเอียดของระบบเทคโนโลยีสารสนเทศ
   - การกำหนดผู้รับผิดชอบสั่งการ ผู้มีอำนาจตัดสินใจ และสั่งการในการนำแผนมาปฏิบัติโครงสร้างการบังคับบัญชา และผู้สั่งการแทน
   - การบันทึกการเปลี่ยนแปลงของแผน
   - กำหนดแผนการปฏิบัติงานเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง
   - การกลับคืนสู่การทำงานปกติ
   - การประชาสัมพันธ์ และการฝึกอบกรม
   - การทดสอบ ปรับปรุงและสอบทานแผนฉุกเฉิน
   - การปรับปรุงและสอบทานแผน

10.1.5 การทดสอบ การรักษาไว้ และการประเมินทบทวนแผนฉุกเฉิน (Testing, Maintaining and Reassessing Business Continuity Plans)

1) IMC (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องกำหนดเวลาการทดสอบแผน กำหนดการทดสอบแผนฉุกเฉินที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้น จนสิ้นสุดกระบวนการทดสอบ
2) IMC ต้องกำหนดเหตุการณ์จำลองที่จะใช้ทดสอบ และรายละเอียด ในการกำหนดรายละเอียดของเหตุการณ์จำลอง ควรระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผนฉุกเฉิน
3) IMC ต้องกำหนดทรัพยากรต่าง ๆ ที่ใช้ในการทดสอบแผนฉุกเฉิน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุม ประสานงานและรับผิดชอบในการจัดการทดสอบแผนฉุกเฉิน รวมถึงสถานที่ และอุปกรณ์เครื่องมือต่าง ๆ และงบประมาณที่ต้องใช้ด้วย
4) IMC ต้องกำหนดแผนงาน แนวทางและระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

หน่วยที่ 11 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน (Compliance)

11.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย (Compliance with Legal Requirements)

วัตถุประสงค์: เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับรวมทั้งสัญญาต่าง ๆ

นโยบาย

11.1.1 การระบุข้อกำหนดในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation)

1) ต้องมีการศึกษาและกำหนดรายการของนโยบายกฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน
2) เจ้าหน้าที่กลุ่มโรงพยาบาลวิชัยเวชฯ ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการตรวจสอบกับกฎหมายIT และมีรายการดังต่อไปนี้เป็นอย่างน้อย
   - นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
   - พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
   - พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์
   - พ.ร.บ. ลิขสิทธิ์
3) ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศขององค์กร ถือเป็นทรัพย์สินขององค์กร (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้โรงพยาบาลสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า
4) เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ กำหนดไว้

5) โรงพยาบาลขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมล์ของผู้ใช้งานโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตาม การจะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใด ๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งศาล ตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น
6) ห้ามเจ้าหน้าที่กลุ่มโรงพยาบาลวิชัยเวชฯ ใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศขององค์กรกระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม
7) การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศไม่ขัดต่อข้อกฎหมายใด ๆ ทั้งราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

11.1.2 ทรัพย์สินทางปัญญา (Intellectual Property Rights, IPR)

1) ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด
2) ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่ ตามคู่มือการปฏิบัติงานเรื่องการตรวจสอบการใช้ซอฟต์แวร์ที่ละเมิดทรัพย์สินทางปัญญา (Monitoring of illegal Software Usage Procedure)
3) ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศขององค์กรโดยเด็ดขาด
4) เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่กลุ่มโรงพยาบาลวิชัยเวชฯ มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือ พลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของสำนักงาน เพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาต และในขณะเดียวกันไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของสำนักงาน โดยไม่ได้รับอนุญาต ทั้งนี้เพื่อจะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

5) กำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้งเพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่า มีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็นอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

11.1.3 การเก็บและป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Organizational Records)

ต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎหมาย ระเบียบ หรือข้อบังคับ ที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบหน่วยงาน ว่าด้วยงานสารบรรณ และกฎหมาย

11.1.4 การป้องกันข้อมูลและความเป็นส่วนตัว (Data protection and privacy of personal information)

ต้องมีการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมายระเบียบสัญญา ที่เกี่ยวกับองค์กร

11.1.5 การป้องกันการใช้งานเครื่องมือ (Prevention of misuse of information processing facilities)

ต้องมีการป้องกันระบบสารสนเทศ ระบบคอมพิวเตอร์และเครือข่าย ไม่ให้ผู้ใช้งานใช้งานในทางที่ผิด หรือโดยไม่มีสิทธิ

11.1.6 การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

1) ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง