นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

A5 มาตรการควบคุมด้านบริษัทฯ Organizational Controls

5.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)

5.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information Security Policy Document)

1) ต้องจัดทำนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์ อักษร เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ โดยนโยบายดังกล่าวจะต้องได้รับการอนุมัติจากผู้บริหารสูงสุดในการนำไปใช้

2) ต้องจัดให้มีการเผยแพร่เอกสารนโยบายระบบบริหารความมั่นคงปลอดภัยสารสน เทศ ให้กับหน่วยงานภายนอกและผู้ที่เกี่ยวข้องในขอบเขตรับทราบ

5.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the Information Security Policy) ต้องดำเนินการตรวจสอบทบทวนและประเมินนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้อย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญทั้งจากภายในและภายนอกบริษัทฯ

5.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

5.2.1 ต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการดำเนินงาน ทางด้านความมั่นคงปลอดภัย สารสนเทศไว้อย่างชัดเจน

5.2.2 ผู้บริหารฯต้องแต่งตั้งคณะหรือกลุ่มผู้ทำงานหลักตลอดจนทรัพยากรที่จำเป็นเพื่อการบริหารและจัดการความมั่นคงปลอดภัยสารสนเทศ

5.3 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

ต้องแบ่งหน้าที่และกำหนดความรับผิดชอบที่ชัดเจนในการปฏิบัติงานเพื่อลดโอกาสที่จะใช้อำนาจ และหน้าที่ในการสร้างความเสียหายต่อบริษัทฯ ทั้งจากความตั้งใจและไม่ตั้งใจ

5.4 หน้าที่ความรับผิดชอบของผู้บริหาร (Management Responsibilities)

ต้องกำหนดให้พนักงานและผู้ที่ทำสัญญาจ้างทั้งหมดรักษาความมั่นคงปลอดภัยสารสนเทศโดย ปฏิบัติให้สอดคล้องกับนโยบายและแนวปฏิบัติของบริษัทที่ได้กำหนดไว้รวมทั้ง

5.4.1 ต้องสั่งการและสนับสนุนบุคลากรเพื่อนำสู่ความสัมฤทธิ์ผลของระบบบริหารจัดการความ มั่นคงปลอดภัยสารสนเทศ

5.4.2 กำหนดทิศทางการปฏิบัติของนโยบายเพื่อสร้างความมั่นคงปลอดภัยให้กระบวนการทางสารสนเทศทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

5.4.3 ต้องจัดหาทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อใช้ในการดำเนินการ

5.4.4 ต้องสื่อสารความสำคัญของระบบความมั่นคงปลอดภัยสารสนเทศที่สัมฤทธิ์ผลและดำเนิน การตามความต้องการของระบบความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

5.4.5 ต้องส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง

5.5 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with Authorities) - ISMS Contact List

5.5.1 ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อ กับผู้ที่เกี่ยวข้องภายในบริษัทฯ เมื่อเกิด เหตุการณ์ฉุกเฉิน

5.5.2 ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อ กับผู้ที่เกี่ยวข้องภายนอกบริษัทฯ เมื่อเกิดเหตุการณ์ฉุกเฉิน

5.6 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with Special Interest Groups) ISMS Contact with Interest Group

5.6.1 ต้องกำหนดรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษใน เรื่องเดียวกันกับกลุ่มที่มีความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ และข้อมูล สำหรับการติดต่อต้องได้รับการปรับปรุงให้ทันสมัยอย่างสม่ำเสมอ

5.6.2 ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่ง ชาติ ให้บริการอินเทอร์เน็ตศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ ประเทศไทย (Thai CERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความ มั่นคงปลอด ภัยเมื่อเกิดเหตุหรือกรณีที่มีความจำเป็นต้องติดต่อและข้อมูลสำหรับการ ติดต่อ ต้องได้รับการปรับปรุงให้ทันสมัยอย่างสม่ำเสมอ

5.7 Threat intelligence ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม

บริษัทฯ มีการจัดการข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะ ถูกรวบรวมและวิเคราะห์เพื่อสร้างข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม

การควบคุมนี้กำหนดให้ผู้รับผิดชอบต้องรวบรวมข้อมูลเกี่ยวกับภัยคุกคามและวิเคราะห์เพื่อ ดำเนินการลดผลกระทบที่เหมาะสม ข้อมูลนี้อาจเกี่ยวกับการโจมตีเฉพาะวิธีการและเทคโนโลยีที่ผู้โจมตี ใช้และ/หรือแนวโน้มการโจมตี ผู้รับผิดชอบรวบรวมข้อมูลนี้เป็นการภายใน รวมทั้งจากแหล่งข้อมูล ภายนอก

บริษัทฯ มีการกำหนดกระบวนการในการรวบรวมข้อมูลภัยคุกคามเพื่อประเมินความเสี่ยงและลด ความเสี่ยงในเหตุการณ์ที่จะเกิดขึ้นและบริษัทฯมีการทบทวนข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความ มั่นคงปลอดภัยสารสนเทศที่ได้รวบรวมไว้เป็นประจำทุก 3 เดือน เพื่อให้ทันต่อสถานการณ์ภัยคุกคาม ที่เปลี่ยนแปลงตลอดเวลา

5.8 การบริหารจัดการโครงการเพื่อให้มีความมั่นคงปลอดภัย (Information Security in Project Management)

5.8.1 ต้องมีการกำหนดระเบียบข้อบังคับกฎเกณฑ์ต่างๆเกี่ยวกับการดำเนินงานและการเข้าถึง ข้อมูลเพื่อให้งานโครงการมี ความมั่นคงปลอดภัย เช่น การกำหนดสิทธิในการเข้าถึง ข้อมูลของผู้ใช้งาน

5.8.2 กรณีโครงการที่จ้างบริษัทภายนอกโครงการที่หน่วยงานภายนอกดำเนินการให้และโครง การที่จัดทำเองต้องปฏิบัติตามวิธีปฏิบัติงานเรื่องการจัดทำโครงการด้านเทคโนโลยีสารสนเทศ เพื่อให้การบริหารจัดการโครงการเกิดความมั่นคงปลอดภัยและลดผลกระทบจาก ความเสี่ยงที่อาจเกิดขึ้น เช่น จ้าง Outsource มาพัฒนาโปรแกรม

5.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ (Inventory of information and other associated assets)

5.9.1 ทะเบียนสินทรัพย์ (Inventory of Assets)

1) ต้องจัดทำบัญชีรายการทรัพย์สินที่อยู่ในความรับผิดชอบและตรวจสอบดูแลปรับปรุงบัญชีรายการทรัพย์สินดังกล่าวอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

2) บัญชีรายการทรัพย์สินต้องครอบคลุมถึงทรัพย์สิน ได้แก่ ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์(Software) โมเดล AI และชุดข้อมูล ข้อมูลและสารสนเทศ (Data and Information) เครือข่าย (Network) บุคลากร (Personnel) และบริการ (Service) พร้อมกับกำหนดผู้ดูแลรับผิดชอบทรัพย์สิน

5.10 การใช้งานข้อมูลและทรัพย์สินสารสนเทศที่เกี่ยวข้องอื่นๆ อย่างเหมาะสม (Acceptable Use for information and other associated Assets)

5.10.1 ต้องกำหนดขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บทรัพย์สินสารสนเทศเพื่อมิให้ ข้อมูลสารสนเทศรั่วไหล หรือถูกนำไปใช้ผิดประเภท

1) ผู้ใช้งานต้องไม่ทิ้งหรือปล่อยให้ทรัพย์สินสารสนเทศที่มีความสำคัญ เช่น เอกสารสื่อบันทึกข้อมูลให้อยู่ในสถานที่ที่ไม่มีความปลอดภัย สถานที่สาธารณะ หรือ พบเห็นได้ง่าย เป็นต้น

2) การจัดการสินทรัพย์ (Handling of Asset)

(1) ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น

(2) พนักงานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้

(3) งานโดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไปข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัสหรือวิธีการอื่นใดของระบบปฏิบัติการหรือระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม

(4) พนักงานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถ ปิดล็อกได้เมื่อไม่ได้ใช้งานโดยเฉพาะอย่างยิ่งเมื่ออยู่นอกช่วงเวลาการทำการ หรือเมื่อต้องทิ้งเอกสาร หรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน

(5) ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่างๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร ฯลฯ โดยทันที

(6) พนักงานต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอกยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

(7) สื่อบันทึกข้อมูลและอุปกรณ์คอมพิวเตอร์พกพาต่างๆ เช่น USB-Drive เป็นต้น ที่มีข้อมูล ลับอยู่ต้องได้รับการดูแลรักษา และใช้งานอย่างระมัดระวัง

5.11 การคืนสินทรัพย์ (Return on Assets)

พนักงาน บริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) ซึ่งพ้นสภาพจากการจ้างงาน ต้องคืน สินทรัพย์ทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก กุญแจ คอมพิวเตอร์ อุปกรณ์ต่อพ่วง คู่มือและเอกสารต่างๆ ให้แก่ผู้บังคับบัญชาหรือเจ้าหน้าที่ที่เกี่ยวข้องดำเนินการ ก่อนวันสุดท้ายของการว่าจ้างงานโดยอ้างอิงจากข้อมูลจากระบบที่บันทึกไว้

5.12 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Classification Information Control)

การกำหนดชั้นความลับของสารสนเทศ (Classification of Information) ต้องมีการจำแนกหมวด หมู่ชั้นความลับ (Sensitivity) ระบุความสำคัญ (Criticality) และข้อกำหนดทางกฎหมาย (Legal Requirement) ของข้อมูลทั้งที่อยู่ในรูปแบบสำเนาถาวร (Hardcopy) และ สำเนาอิเล็กทรอนิกส์ (Softcopy) ที่อยู่ในความรับผิดชอบ เพื่อป้องกันสารสนเทศให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม

5.13 การจัดทำป้ายชื่อของข้อมูล (Labeling of Information Control)

5.13.1 ต้องจัดการให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์สารสนเทศที่เกี่ยวข้อง

5.13.2 ข้อมูลในรูปแบบสำเนาถาวรจะต้องทำป้ายสัญลักษณ์บอกชั้นความลับส่วนข้อมูลในรูป แบบสำเนาอิเล็กทรอนิกส์จะต้องทำป้ายสัญลักษณ์บอกภายในเนื้อหาข้อมูลสำหรับระดับ ความสำคัญและข้อกำหนดทางกฎหมายให้หน่วยงานพิจารณาตามความเหมาะสมและ อาจยกเว้นการจัดทำป้ายสัญลักษณ์ได้

5.14 การถ่ายโอนข้อมูล (Information Transfer)

5.14.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information Transfer Policies and Procedures) การรับ-ส่งข้อมูลหรือไฟล์อิเล็กทรอนิกส์ที่เป็นความลับระหว่างหน่วยงานภายในหรือ ภายนอกบริษัทต้องได้รับการเข้ารหัสข้อมูล (Cryptography Control)

5.14.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on Information Transfer) กำหนดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลหรือไฟล์อิเล็กทรอนิกส์ระหว่างหน่วยงาน กับบุคคลหรือ หน่วยงานภายนอกกำหนดให้มีข้อตกลงในการรักษาความลับหรือ ไม่เปิดเผย ความลับอย่างเป็นลายลักษณ์อักษรกับผู้ให้บริการภายนอก

5.14.3 การรักษาความมั่นคงปลอดภัยการส่งข้อความอิเล็กทรอนิกส์ (Electronic Messaging) ต้องมีการกำหนดวิธีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

5.15 การควบคุมการเข้าถึง (Access Control)

5.15.1 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Business Requirement for Access Control)

1) นโยบายควบคุมการเข้าถึง (Access Control Policy)

(1) มีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศเพื่อควบคุมการเข้าถึงให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(2) กำหนดสิทธิการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยี สารสนเทศรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(3) ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไข หรือเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศได้

(4) ต้องบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่างๆของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมี ปัญหาเกิดขึ้น

(5) การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศจะกระทำได้ก็ต่อเมื่อได้รับการ อนุมัติและสามารถเข้าใช้ข้อมูลและระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้นๆเท่านั้นความปลอดภัยของข้อมูลและกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดนโยบายและขั้นตอนการทำงานของระบบเทคโนโลยีสารสนเทศซึ่งกระบวนการเหล่านี้หมายรวมถึงการให้สิทธิและการบริหารจัดการรหัสในการเข้าใช้งานการกำหนด ขอบเขตในการเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์และอุปกรณ์ที่เก็บข้อมูลประเภทอื่นๆ การสำรองข้อมูล และการกู้ข้อมูลที่เสียหายกลับคืนมา

5.15.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services)

1) ผู้ดูแลระบบเครือข่ายเป็นผู้ให้สิทธิการเข้าถึงระบบเครือข่ายและบริการทางเครือข่ายแก่ผู้ใช้งานตามความจำเป็นเท่านั้น

2) ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่าย โดยเฉพาะเพื่อรักษาความมั่นคงปลอดภัยแก่ข้อมูลและระบบเทคโนโลยีสารสนเทศ อาทิ

(1) การใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย เช่น Secure Socket Layer (SSL) Simple Network Management Protocol (SNMP), Web Certificate

(2) การจำกัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ Bandwidth เช่น การรับ-ส่งไฟล์ขนาดใหญ่ ฟังเพลง ออนไลน์ ดูทีวีออนไลน์ หรือเล่นเกมส์ออนไลน์ในช่วงเวลาทำการ

3) ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสมเพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ อาทิ

(1) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายทั้งหมดจำเป็นต้องได้รับการตั้งค่าให้มีความปลอดภัยและมีการ ตรวจสอบกิจกรรมต่างๆที่ เกี่ยวข้องกับระบบเครือข่าย ระบบสายสัญญาณต้องได้รับมาตรฐานอุตสาหกรรม และได้รับการติดตั้งโดย ผู้ที่มีความชำนาญที่ผ่านการพิจารณาอนุมัติแล้ว

(2) อุปกรณ์เครือข่าย อาทิ Router Firewall Switch Wireless Access Point ต้องได้รับการตั้งค่าตามความจำเป็นด้านความมั่นคงปลอดภัยของอุปกรณ์นั้นๆ หรือตามคำแนะนำของผู้ผลิต อาทิ SANS Institute หรือสำนักงานความมั่นคงแห่งชาติ (NSA : National Security Agency)

5.16 การบริหารจัดการอัตลักษณ์ (Identify management)

เพื่อให้สามารถระบุตัวตนที่เป็นลักษณะเฉพาะของแต่ละบุคคล และระบบต่างๆ ที่เข้าถึงสารสนเทศ และทรัพย์สินที่เกี่ยวข้องอื่น ๆ ขององค์กรและเพื่อให้สามารถมอบหมายสิทธิการเข้าถึงได้อย่างเหมาะสมองค์กรควรมีกระบวนการสนับสนุนในการจัดการการเปลี่ยนแปลงข้อมูลที่เกี่ยวข้องกับข้อมูล อัตลักษณ์ของผู้ใช้กระบวนการเหล่านี้อาจรวมถึงการทวนสอบเอกสารที่เชื่อถือได้ที่เกี่ยวข้องกับบุคคลเมื่อใช้อัตลักษณ์ที่บุคคลภายนอกให้หรือออกให้ (เช่น ข้อมูลประจำตัวบนสื่อสังคมออนไลน์) องค์กรควรตรวจสอบให้แน่ใจว่าข้อมูลอัตลักษณ์จากบุคคลภายนอกระดับความน่าเชื่อถือที่เหมาะสม และความเสี่ยงที่เกี่ยวข้องใด ๆ เป็นที่ทราบและได้รับการปฏิบัติอย่างเพียงพอ ซึ่งอาจรวมถึงการควบคุมต่างๆ ที่เกี่ยวข้องกับบุคคลภายนอก รวมทั้งการควบคุมต่าง ๆ ที่เกี่ยวข้องกับข้อมูลการยืนยันตัวตน

5.17 การพิสูจน์ตัวตน (Authentication information)

5.17.1 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User)

1) ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานต้องเก็บรักษารหัสผ่านของผู้ใช้งานให้เป็นความลับ

(1) ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานต้องกำหนดรูปแบบรหัสผ่านให้มีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยต้องมีการผสมกันระหว่างอักษรตัวพิมพ์เล็ก ตัวพิมพ์ ใหญ่ ตัวเลข อักขระพิเศษต่างๆ เช่น ! @ # $ % ^ & * () เข้าด้วยกัน เพื่อให้ยากต่อการคาดเดา

(2) รหัสผู้ใช้งานต้องไม่ซ้ำกับรหัสที่ใช้ก่อนหน้านี้อย่างน้อย 4 ครั้ง

(3) ทำการล๊อค บัญชีผู้ใช้ เมื่อมีการใส่รหัสผิดพลาดจำนวน 5 ครั้ง

2) การกำหนดรหัสผ่านให้กับผู้ใช้งานครั้งแรกให้ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งาน กำหนดรหัสผ่านชั่วคราวจากการสุ่ม

3) การส่งมอบรหัสผ่านให้กับผู้ใช้งานในครั้งแรกให้ใช้วิธี จัดส่ง Username และรหัสผ่านเป็นเอกสารปิดผนึกไปพร้อมกับการรับเครื่องคอมพิวเตอร์ที่ใช้งาน

4) ระบบจะบังคับให้ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านทันที ในครั้งแรกเมื่อทำการ Login เข้าใช้งานระบบ

5) ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานจัดทำระบบที่สามารถให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ของตนเองได้ และกำหนดให้เปลี่ยนรหัสผ่านทุก 1 ปี

5.17.2 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)
การใช้งานและเก็บรักษาข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานต้องดำเนินการตามนโยบาย หรือวิธีปฏิบัติของบริษัทสำหรับการใช้งานข้อมูลพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ เช่น

1) การเก็บรักษาข้อมูล Username และ Password ต้องเป็นความลับห้ามเปิดเผยให้บุคคลๆอื่นทราบ

2) หลีกเลี่ยงการเก็บบันทึกข้อมูลเว้นแต่สามารถเก็บไว้อย่างปลอดภัยได้

3) เมื่อได้รับข้อมูล Username และ Password ซึ่งเป็นข้อมูล Default ควรมีการแก้ไขทันทีเมื่อเข้าใช้งานระบบครั้งแรก

5.17.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System)
ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุม ดูแลให้ผู้ใช้งานระบบเปลี่ยน รหัสผ่านตามระยะเวลาที่กำหนดกรณีที่บางระบบไม่สามารถ ดำเนิน การได้อันเนื่องมาจากข้อจำกัดของระบบผู้ดูแลระบบต้องบริหารจัดการความมั่นคงปลอดภัยโดย ใช้มาตรการอื่นทดแทน

5.18 สิทธิการเข้าถึง (Access right)

5.18.1 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

1) ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานมีหน้าที่ในการกำหนดสิทธิการเข้าถึงข้อมูล และระบบเทคโนโลยีสารสนเทศให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน ในการปฏิบัติงานตามการให้สิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศที่ฝ่ายเทคโนโลยีสารสนเทศได้กำหนดไว้ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างน้อยปีละ 1 ครั้ง หรือมีการเปลี่ยนแปลง

2) ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานต้องกำหนดบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล โดยไม่ซ้ำซ้อนกัน และให้ถือว่าบัญชีผู้ใช้งานเป็นการระบุและยืนยันตัวตนของผู้ใช้งานต่อไป

3) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานเพื่อให้มีสิทธิสูงสุดผู้ใช้งานต้องได้รับความเห็นชอบและอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศ โดยมีการกำหนดระยะเวลาการใช้งาน และสามารถระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือเมื่อพ้นจากหน้าที่

4) ในกรณีระบบคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศที่มีข้อจำกัดเกี่ยวกับบัญชีผู้ใช้งานทำให้ผู้ ใช้งานต้องใช้บัญชีผู้ใช้งานร่วมกัน และถือรหัสผ่านร่วมกันให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้มอบหมายให้ผู้ใช้งานถือรหัสผ่านร่วมกัน

5) ผู้ใช้งานต้องรับทราบและยอมรับสิทธิ รวมถึงหน้าที่ที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศ รวมทั้งต้องปฏิบัติตามอย่างเคร่งครัด

5.18.2 การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

1) ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือมีการเปลี่ยนแปลง เมื่อเกิดการว่าจ้างงาน การเปลี่ยนแปลงหน้าที่ รับผิดชอบ การโยกย้ายหน่วยงาน การเกษียณ และการลาออกจากงาน

2) ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานจัดทำรายการชื่อผู้ใช้งานที่มีสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศแยกตามหน่วยงานภายใน และส่งให้ผู้บริหารระดับสูงฝ่ายต่างๆ เพื่อทบทวนสิทธิการเข้าถึงของผู้ใช้งานให้เหมาะสมกับหน้าที่รับผิดชอบ

5.18.3 การถอนหรือการจัดการสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

1) ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานต้องยกเลิกสิทธิของผู้ใช้งานในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อสิ้นสุดสภาพการเป็นพนักงาน เกษียณอายุ สิ้นสุดสัญญา หรือข้อตกลงการปฏิบัติงาน หรือเมื่อไม่มีหน้าที่รับผิดชอบในระบบ เทคโนโลยีสารสนเทศที่ได้รับสิทธิในการใช้งาน

2) ผู้ดูแลบริหารจัดการบัญชีผู้ใช้งานต้องปรับเปลี่ยนสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เหมาะสม เมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใดๆ ของผู้ใช้งานที่เกิดขึ้น หรือตามที่ได้รับแจ้งจากเจ้าของระบบเทคโนโลยีสารสนเทศ พร้อมทั้งแจ้งผู้ใช้งานให้ทราบถึงการปรับเปลี่ยนดังกล่าว

5.19 ความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

5.19.1 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)
ต้องกำหนดให้มีการจัดทำข้อกำหนดหรือสัญญาร่วมกันระหว่างบริษัทฯ กับผู้ให้บริการ ภายนอก และต้องจัดทำเป็นลายลักษณ์อักษร

5.20 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Assessing information Security within Supplier Agreements)

5.20.1 ต้องระบุและจัดทำข้อกำหนดข้อตกลงหรือสัญญาร่วมกันระหว่างบริษัทกับผู้ให้บริการภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกในเรื่องความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการเข้าถึงการประมวลผลการ จัดเก็บการสื่อสารและการให้บริการ โครงสร้างพื้นฐานของระบบสำหรับ

สารสนเทศของบริษัทฯ โดยผู้ให้บริการภายนอก โดยจัดให้มีการทำ Service Level Agreement ที่ครอบคลุมถึงข้อตกลงด้านความ ปลอดภัยในการให้บริการ โดยหน่วยงานภายนอก ได้แก่ คุณลักษณะและรายละเอียดของการให้บริการมาตรการจัดการด้านความมั่นคงปลอดภัยในการให้บริการโดยข้อตกลงนี้เป็นที่ยอมรับของทั้งสองฝ่าย และกำหนดให้มีการทบทวน Service Level Agreement ดังกล่าวอย่างน้อยปีละ 1 ครั้ง

5.20.2 สัญญาและข้อตกลงร่วมกันจะต้องมีการแสดงข้อความไม่เปิดเผยความลับข้อมูลการค้าและข้อมูลที่ได้ รับระหว่างการปฏิบัติงาน หรือเซ็นสัญญาสัญญารักษาความลับ (Non-disclosure Agreement: NDA) ควบคู่กัน

5.21 ห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Managing Information security in the ICT Supply Chain)

5.21.1 ข้อตกลงกับผู้ให้บริการภายนอกต้องรวมถึงความต้องการเรื่องการระบุความเสี่ยงอันเกิด จากห่วงโซ่ของการให้ บริการสารสนเทศ

5.21.2 สื่อสารกับผู้ค้าให้ส่งต่อนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และข้อปฏิบัติต่างๆ ไปยังผู้จ้างช่วง (กรณีที่ผู้ค้าทำสัญญากับผู้ค้ารายย่อยอื่นในการส่งมอบบริการ)

5.22 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

5.22.1 การติดตาม และทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and Review of Supplier Services).

1) ต้องจัดทำข้อตกลงกำหนดสิทธิที่จะตรวจสอบสภาพแวดล้อมการทำงานรวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อ จัดจ้างของหน่วยงานภายนอก

2) กำหนดให้มีการติดตามและประเมินผลงานอย่างสม่ำเสมอเพื่อตรวจสอบความ สอดคล้องการปฏิบัติ ตามสัญญา และข้อตกลงการบริการ

3) ทบทวนผลการดำเนินงานทุกครั้งในช่วงก่อนต่อสัญญาและทำสัญญาใหม่หรือเปลี่ยนแปลงเงื่อนไขในสัญญา

5.22.2 การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

1) การเปลี่ยนแปลงผู้ให้บริการภายนอกต้องพิจารณาผลการปฏิบัติงานความเหมาะสมในการเปลี่ยนแปลงตามความจำเป็น

2) มีการพิจารณาอย่างรอบคอบถึงความจำเป็นในการเปลี่ยนแปลงแก้ไขสัญญา หรือข้อตกลงร่วมกันหากต้องดำเนินการเปลี่ยนแปลงใดๆ ต้องได้รับอนุมัติจาก ผู้มีอำนาจก่อนเปลี่ยนแปลง รวมถึงการพิจารณาความเสี่ยงที่อาจกระทบต่อธุรกิจระหว่างการเปลี่ยนแปลง

5.23 Information Security for using Cloud Services.

บริษัทฯ มีการควบคุมข้อกำหนดด้านความปลอดภัยสำหรับบริการระบบคลาวด์เพื่อให้มีการ ปกป้องข้อมูลของบริษัทฯ ในระบบคลาวด์ได้ดียิ่งขึ้นซึ่งรวมถึงการซื้อใช้งาน จัดการ และยุติการใช้ บริการคลาวด์ บริษัทฯ จัดทำมาตรการด้านความปลอดภัยสำหรับบริการระบบคลาวด์ และกำหนด เกณฑ์สำหรับการเลือกผู้ให้บริการระบบคลาวด์ นอกจากนี้ บริษัทฯ มีการกำหนดกระบวนการ พิจารณาการใช้งานระบบคลาวด์ที่ยอมรับได้ และกำหนดความมั่นคงปลอดภัยสารสนเทศเมื่อยกเลิกการใช้บริการระบบคลาวด์

5.24 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ และการปรับปรุง (Management of Information Security Incidents and Improvements)

5.24.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures) ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่ เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน และขั้นตอนดังกล่าวต้องมีความ รวดเร็วได้ผล และมีความเป็นระบบที่ดี

5.24.2 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events) พนักงานที่พบเห็นเหตุการณ์ (Event) หรืออุบัติการณ์ (Incident) ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ต้องแจ้งผู้มีหน้าที่เกี่ยวข้องโดยเร็วที่สุดเพื่อให้ผู้เกี่ยวข้องดำเนินการตรวจสอบ และแก้ไขได้ทันเวลา เช่น ไวรัสคอมพิวเตอร์ ข้อมูลสารสนเทศสูญหาย ระบบคอมพิวเตอร์ล้มเหลว เป็นต้น

5.24.3 การรายงานจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Weaknesses)
ต้องมีมาตรการควบคุมพนักงาน ผู้ทำสัญญาจ้างที่ใช้งานระบบ และผู้ให้บริการสารสน เทศของบริษัทต้องทำการจดบันทึก และรายงานข้อสังเกต หรือจุดอ่อนด้านความมั่นคงปลอดภัย สำหรับสารสนเทศที่น่าสงสัยใดๆ ในระบบหรือบริการต่างๆ

5.25 การประเมินและตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Assessment of and Decision on Information Security Events)

ต้องมีมาตรการควบคุมสถานการณ์ความมั่นคงปลอดภัยสำหรับสารสนเทศที่ต้องถูกประเมิน และตัดสินใจถ้าสถานการณ์ดังกล่าวถูกจัดหมวดหมู่เป็นเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

5.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to Information Security Incidents)

มาตรการควบคุมปลอดภัยสำหรับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองตามขั้นตอนปฏิบัติงานที่เป็นเอกสาร

5.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัย (Learning from Information Security Incidents)

มาตรการควบคุมความรู้ที่ได้รับจากการวิเคราะห์และการแก้ปัญหาเหตุการณ์ความมั่นคง ปลอดภัยสารสนเทศต้องถูกนำไปใช้เพื่อลดโอกาส หรือผลกระทบของเหตุการณ์ในอนาคต

5.28 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

บริษัทต้องกำหนดแนวปฏิบัติงาน และนำมาใช้ในการระบุเก็บรวบรวม จัดหา และเก็บรักษา สารสนเทศที่สามารถนำมาเป็นหลักฐาน

5.29 ความมั่นคงปลอดภัยสารสนเทศระหว่างการหยุดชะงัก (Information security during disruption)

ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทาง ธุรกิจ (Information Security Aspects of Business Continuity Management)

5.29.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity)
การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity) ต้องจัดทำแผนเตรียมความพร้อมฉุกเฉิน (Contingency Plan) เพื่อรับมือ

สถานการณ์ฉุกเฉินที่เกิดขึ้นได้ทั้งวิธีการทาง อิเล็กทรอนิกส์และทางกายภาพโดยแผนเตรียมความพร้อมกรณีฉุกเฉินต้องมีรายละเอียดอย่างน้อย

1) การกำหนดหน้าที่ และความรับผิดชอบของบุคคลที่เกี่ยวข้อง
2) การกำหนดขั้นตอนการปฏิบัติในการกู้คืนระบบเทคโนโลยีสารสนเทศ
3) การกำหนดขั้นตอนการปฏิบัติในการสำรองข้อมูล และทดสอบการกู้คืนข้อมูลที่ สำรองไว้
4) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก

5.29.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implement Information Security Continuity)

ต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์ อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละ 1 ครั้ง

5.29.3 การตรวจสอบ ทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัย สารสนเทศ (Verify Review and Evaluate Information Security Continuity)

1) ต้องกำหนดเวลาการทดสอบแผนกำหนดการทดสอบแผนฉุกเฉินที่ชัดเจนรวมถึงกำหนดระยะเวลาที่ ใช้ในการทดสอบตั้งแต่เริ่มต้นจนสิ้นสุดกระบวนการทดสอบ
2) ต้องกำหนดเหตุการณ์จำลองที่จะใช้ทดสอบและรายละเอียดในการกำหนดราย ละเอียดของเหตุการณ์จำลองควรระบุวัตถุประสงค์ขอบเขตของระบบงานหรือ กระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้น ตอนการทดสอบแผนฉุกเฉิน

5.30 ต้องกำหนดทรัพยากรต่างๆ ที่ใช้ในการทดสอบแผนฉุกเฉิน กำหนดผู้รับผิดชอบ ที่จะทำหน้าที่ ควบคุมประสานงาน และรับผิดชอบในการจัดการทดสอบแผนฉุกเฉิน รวมถึงสถานที่ และอุปกรณ์ เครื่องมือต่างๆ และงบประมาณที่ต้องใช้ด้วย ต้อง กำหนดแผนงาน แนวทาง และระยะเวลาในการ ทบทวน และปรับปรุงแผน อย่างชัดเจนเพื่อให้แผนนั้นมีความทันสมัย

ความพร้อม ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity) ควรวางแผนด้าน ความพร้อมของ ICT นำไปปฏิบัติดูแลรักษาและทดสอบโดยอิงตามวัตถุ ประสงค์ความต่อเนื่องทางธุรกิจและ ข้อกำหนดความต่อเนื่องของ ICT และควบคุมข้อกำหนดให้ เทคโนโลยีสารสนเทศ และการสื่อสารของบริษัทฯ พร้อมสำหรับการหยุดชะงักที่อาจเกิดขึ้น เพื่อ ให้ข้อมูล และสินทรัพย์ ที่จำเป็นพร้อมใช้งานเมื่อจำเป็น ซึ่งรวม ถึงการวางแผนความพร้อม การนำไปใช้งาน การบำรุงรักษา และการทดสอบ

บริษัทฯ มีการกำหนดกระบวนการ ขั้นตอนการวางแผนซึ่งคำนึงถึงความเสี่ยง และ ความต้องการทางธุรกิจในการกู้คืน บริษัทฯ มีการกำหนดการบำรุงรักษาสำหรับเทคโนโลยีสาร สนเทศ และขั้นตอน การทดสอบสำหรับการกู้คืนจากความเสียหายและ/หรือ แผนความต่อเนื่อง ทางธุรกิจ โดยแผนดังกล่าวได้รับการอนุมัติจากกรรมการผู้จัดการ

บริษัทฯ มีการจัดทำเอกสารผ่านการวิเคราะห์ผลกระทบทางธุรกิจ กลยุทธ์ความต่อเนื่อง ทางธุรกิจ และแผนความต่อเนื่องทางธุรกิจ พร้อมกับการจัดทำรายงานการทดสอบความต่อเนื่อง ทางธุรกิจ โดยมีการทบทวนและทดสอบความต่อเนื่องทางธุรกิจอย่างน้อยปีละ 1 ครั้ง

5.31 กฎหมายข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับและข้อผูกพันตามสัญญา (Regal, statutory, regulatory and contractual requirement)

5.31.1 การระบุข้อกำหนด และความต้องการในสัญญาจ้างในการใช้งานระบบเทคโนโลยีสาร สนเทศ (Identification of Applicable Legislation and Contractual Requirements)

ผู้ใช้งานทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบายกฎ ระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศที่ กำหนดขึ้นอย่างเคร่งครัดโดย Information Technology Director เป็นหนึ่งในคณะกรรมทำงาน Compliance ซึ่งมีการประชุมเป็นประจำ โดยมีรายการดังต่อไปนี้เป็นอย่างน้อยตามบันทึกพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
2) พระราชบัญญัติลิขสิทธิ์
3) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
4) พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์
5) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน)

5.31.2 การควบคุมการเข้ารหัส (Regulation of cryptographic controls)
ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

5.32 ทรัพย์สินทางปัญญา (Intellectual Property Rights)

5.32.1 ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทาง ปัญญาที่บริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) จัดหามาให้ใช้งาน

5.32.2 ต้องมีการบริหารจัดการ และควบคุมดูแลการใช้งานซอฟต์แวร์ให้เป็นไปตามลิขสิทธิ์ ที่ได้รับ

5.32.3 ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำหรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือ เอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนเครื่องคอม พิวเตอร์ แท็ปแล็ต หรือสมาร์ทโฟนของ บริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) โดยเด็ดขาด

5.33 การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

ต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบ หรือ ข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล

5.34 ความเป็นส่วนตัว และการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personally Identifiable Information : PII)

กำหนดให้มีการคุ้มครองข้อมูลส่วนบุคคล โดยให้สอดคล้องกับกฎหมาย และข้อกำหนดตาม สัญญาต่างๆ ของบริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน)

5.35 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent Review of Information Security)

ต้องมีการทบทวนวิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติ ของบริษัทฯ เช่น ทบทวนวัตถุประสงค์ มาตรการ นโยบาย วิธีปฏิบัติงานต่างๆ ให้ถูกต้อง และเป็น ปัจจุบันตามรอบระยะเวลาที่กำหนดอย่างน้อยปีละ 1 ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง

5.36 การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความปลอดภัยสารสนเทศ (Compliance with policies, rules and Security Standards for information security)

5.36.1 การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)

1) ต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัย สารสนเทศและระยะเวลาที่กำหนดไว้

2) ต้องมีการตรวจสอบ และทบทวนเอกสารนโยบาย มาตรการ วิธีการปฏิบัติงานรวมถึงแบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนด หรือ เมื่อมีการเปลี่ยนแปลง

5.36.2 การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)
ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งานหรือให้บริการอยู่แล้วตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

5.37 เอกสารขั้นตอนการปฏิบัติงาน (Document Operating Procedures)

5.37.1 ต้องจัดทำเอกสารแนวปฏิบัติที่เหมาะสมสำหรับแต่ละระบบเทคโนโลยีสารสนเทศที่อยู่ในความรับผิดชอบของตนและประกาศให้ผู้ปฏิบัติงานทราบ

คู่มือและแนวปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนและผู้รับผิด ชอบการปฏิบัติงานนั้นๆ โดยแนวปฏิบัติงานและเอกสารเกี่ยวข้องทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้งรวมถึงมีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบเทคโนโลยีสารสน เทศถูกเข้าถึงโดยมิได้รับอนุญาต

A6 มาตรการควบคุมด้านบุคลากร (People Control)

6.1 การสรรหาบุคลากร (Screening)

6.1.1 ฝ่ายทรัพยากรมนุษย์ต้องทำการตรวจสอบประวัติในการรับบุคลากรโดยให้บุคลากรที่จะ เข้ามาปฏิบัติงานจัดส่งหลักฐานของบุคลากร เช่น บัตรประชาชน สำเนาทะเบียนบ้าน เป็นต้น เพื่อให้ตรวจสอบก่อนที่จะรับเข้ามาปฏิบัติงาน และตรวจสอบประวัติอาชญากรรม จากสำนักงานตำรวจแห่งชาติ

6.1.2 ฝ่ายทรัพยากรมนุษย์ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นผู้บริหารเจ้าหน้าที่ชั่วคราว หรือนักศึกษาฝึกงานโดยต้องไม่มีประวัติในการบุกรุก แก้ไขทำลายหรือโจรกรรมข้อมูลในระบบ เทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน

6.1.3 ฝ่ายทรัพยากรมนุษย์ต้องจัดให้มีการลงนามในสัญญาไม่เปิดเผยความลับ (Non-Disclosure Agreement : NDA) ก่อนการเข้าปฏิบัติงานภายในบริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน)

6.1.4 ผู้ให้บริการภายนอกที่เข้ามาดำเนินกิจกรรมภายในบริษัทฯ จะต้องลงนามในสัญญา ไม่ เปิดเผยความลับ (Non-Disclosure Agreement: NDA) หรือข้อตกลงเกี่ยวกับความมั่นคง ปลอดภัยสารสนเทศ (Security in Third Party Agreements) ก่อนการเข้าปฏิบัติงาน ภายในบริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน)

6.2 ข้อกำหนดและเงื่อนไขของการจ้างงาน (Terms and Conditions of Employment)

ฝ่ายทรัพยากรมนุษย์ต้องทำข้อตกลงในสัญญาจ้างงานกับพนักงานพร้อมระบุหน้าที่รับผิดชอบที่ชัดเจน ทั้งความรับผิดชอบโดยทั่วไปตามตำแหน่ง และความรับผิดชอบทางด้านความมั่นคงปลอดภัย ทางด้านสารสนเทศ

6.2.1 เพื่อให้การบริหารจัดการ Login หรือ User ID เป็นไปอย่างถูกต้อง และปัจจุบันฝ่ายทรัพยากรมนุษย์ต้องแจ้งให้ฝ่าย เทคโนโลยีสารสนเทศ ทราบทันทีเมื่อมีเหตุ ดังนี้

1) การว่าจ้างงาน
2) การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่ และลูกจ้าง หรือ การถึงแก่กรรม
3) การโยกย้ายหน่วยงาน
4) การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

6.3 การสร้างความตระหนัก การให้ความรู้ และการอบรมให้ความรู้ด้านความมั่นคงปลอดภัย สารสนเทศ (Information Security Awareness, Education and Training)

6.3.1 ผู้ปฏิบัติงานของบริษัททุกคนต้องได้รับการอบรมให้ความรู้โดยเนื้อหาที่แต่ละบุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคลเพื่อเป็นการสร้างความตระหนักและฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

6.3.2 ต้องจัดอบรมให้ความรู้พนักงานเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัย และการเปลี่ยนแปลงที่เกิดขึ้นด้านสารสนเทศ

6.3.3 พนักงานใหม่ทุกคนต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

6.3.4 ต้องดำเนินการจัดทำร่างแผนการฝึกอบรมประจำปีโดยให้มีการให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ปฏิบัติงานใน บริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) อย่างน้อยปีละ 1 ครั้ง

6.4 กระบวนการทางวินัย (Disciplinary Process)

ผู้บริหารสูงสุดต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบ ปฏิบัติ แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุ ในแต่ละข้อกฎหมายนั้นๆ

6.5 ความรับผิดชอบหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน (Responsibilities after Termination or Change of Employment)

6.5.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

1) ต้องมีการกำหนดและสื่อสารให้พนักงานหรือผู้ทำสัญญาได้รับทราบรวมทั้งมีการควบคุมให้ปฏิบัติตามข้อกำหนดในสัญญา

2) ฝ่ายทรัพยากรมนุษย์มีหน้าที่ดูแลหากมีการแต่งตั้งโยกย้าย ปลด หรือเปลี่ยนแปลงตำแหน่งใดๆ ที่เกี่ยวข้องกับความรับผิดชอบในบริษัทฯ

3) ฝ่ายทรัพยากรมนุษย์แจ้งเรื่องผู้ใช้งานที่สิ้นสุดสภาพการจ้างงาน หรือเปลี่ยนหน้าที่ความรับผิดชอบให้ฝ่ายเทคโนโลยีสารสนเทศ เพื่อดำเนินการเพิกถอนสิทธิ หรือเปลี่ยนแปลงสิทธิ และฝ่ายเทคโนโลยีสารสนเทศดำเนินการยกเลิกสิทธิ ดังนี้

(1) Account บนระบบ Microsoft Active Directory / เครื่องสแกนบัตรพนักงาน (Access Card) จะถูกดำเนินการยกเลิกสิทธิของพนักงานที่จะพ้นสภาพภายในเวลาเที่ยงคืนของวันสุดท้ายที่พนักงานจะยังคงมีสถานภาพการเป็นพนักงานของบริษัทฯอยู่

(2) กรณียกเลิกสิทธิเร่งด่วนจะดำเนินการทันทีที่ได้รับแจ้ง

6.6 การรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or Non-Disclosure Agreements)

ต้องมีการจัดทำข้อตกลง หรือสัญญาการรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) อย่างเป็นลายลักษณ์อักษรกับพนักงานภายในบริษัท และ ผู้ให้บริการภายนอกเพื่อป้องกันความปลอดภัยของข้อมูล มีการทบทวนอย่างเหมาะสม และจัดทำเป็น ลายลักษณ์อักษร

6.7 การปฏิบัติงานจากระยะไกล (Teleworking)

6.7.1 ต้องมีการกำหนดให้ผู้ปฏิบัติงานใน บริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) และผู้ให้บริการภายนอกที่ต้องการเชื่อมต่อระบบเทคโนโลยีสารสนเทศจากระยะไกลต้องมีการระบุตัวตนของผู้เข้าใช้ระบบ และอุปกรณ์ที่ใช้ในการเข้าระบบเทคโนโลยีสารสนเทศ ควรอยู่ภายใต้การควบคุมหรือดูแลโดยบริษัทฯ

6.7.2 ผู้ปฏิบัติงานใน บริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) และผู้ให้บริการภายนอกที่ ต้องการเข้าระบบเทคโนโลยีสารสนเทศจากระยะไกลหรือภายนอก บริษัทฯ ต้องเชื่อมต่อ เครือข่าย เพื่อใช้งานผ่านเครือข่ายเสมือน (Virtual Private Network : VPN) ที่บริษัทฯ กำหนดไว้เท่านั้น

6.7.3 หากเชื่อมต่อด้วยอุปกรณ์ที่เป็นของส่วนตัวต้องมีการป้องกันไวรัส และการใช้งาน ไฟร์วอลล์ตามที่บริษัทฯ กำหนด

6.7.4 กำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ และยกเลิกการปฏิบัติจากระยะไกล

6.8 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information Security Event Reporting)

6.8.1 พนักงานที่พบเห็นเหตุการณ์ (Event) หรืออุบัติการณ์ (Incident) ที่เกี่ยวข้องกับความ มั่นคงปลอดภัยสารสนเทศ ต้องแจ้งผู้มีหน้าที่เกี่ยวข้องโดยเร็วที่สุด เพื่อให้ผู้เกี่ยวข้อง ดำเนินการตรวจสอบ และแก้ไขได้ทันเวลา เช่น ไวรัสคอมพิวเตอร์ ข้อมูลสารสนเทศ สูญหาย ระบบคอมพิวเตอร์ล้มเหลว เป็นต้น

6.8.2 การรายงานจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Weaknesses) ต้องมีมาตรการควบคุมพนักงานผู้ทำสัญญาจ้างที่ใช้งานระบบ และผู้ให้บริการสารสนเทศของบริษัทต้องทำการจดบันทึก และรายงานข้อสังเกต หรือ จุดอ่อนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่น่าสงสัยใดๆ ในระบบหรือบริการ ต่างๆ

A7 มาตรการทางกายภาพ (Physical Controls)

ความมั่นคงปลอดภัยทางด้านกายภาพ และสิ่งแวดล้อมของบริษัทฯ (Physical and Environmental Security)

7.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

7.1.1 การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

1) ต้องมีการกำหนดว่าพื้นที่หรือบริเวณใดที่ต้องรักษาความมั่นคงปลอดภัย (Secure areas) เช่น ห้องระบบเครือข่าย (Network Room) เป็นต้น

2) มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่

7.2 การควบคุมการเข้า-ออกที่ถูกควบคุม (Physical Entry)

7.2.1 มีการติดตั้งเครื่องสแกนลายนิ้วมือ หรือล็อกประตู

7.2.2 มีการติดตั้ง CCTV ให้ครอบคลุมพื้นที่ที่ถูกควบคุม

7.2.3 กำหนดรายชื่อผู้มีสิทธิเข้าพื้นที่ควบคุม และทบทวนรายชื่อผู้มีสิทธิอย่างน้อยปีละ 1 ครั้ง

7.2.4 การกำหนดพื้นที่สำหรับบุคคลภายนอกใช้รับส่งสิ่งของ (Delivery and Loading Areas)

1) ต้องมีการจัดพื้นที่หรือบริเวณส่งสินค้า (Loading Areas) หากเป็นไปได้ควรแบ่งแยกพื้นที่ที่เกี่ยวกับการทำงานเพื่อหลีกเลี่ยงการเข้าถึงของ บุคคลภายนอก

2) ต้องตรวจสอบวัสดุหรือสินค้าก่อนนำเข้าพื้นที่ควบคุม

7.3 การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ (Securing Offices Rooms and Facilities)

มีการจัดแบ่งและบริหารพื้นที่ที่เป็นสำนักงานห้องทำงานและสิ่งอำนวยความสะดวกตามมาตรา ฐานความปลอดภัยในสำนักงาน

7.4 การเฝ้าติดตามความมั่นคงปลอดภัยสารสนเทศ (Physical security monitoring)

บริษัทฯ มีการกำหนดการควบคุมและตรวจสอบพื้นที่ที่ละเอียดอ่อนเพื่อให้ผู้ที่ได้รับอนุญาต เท่านั้นที่สามารถเข้าถึงได้ ซึ่งรวมถึงสำนักงาน และ ห้องระบบเครือข่าย (Network Room) ของบริษัทฯ มีการกำหนดกระบวน การและกำหนดว่าใครเป็นผู้รับผิดชอบในการตรวจสอบพื้นที่ที่ละเอียดอ่อน และช่องทางการสื่อสารใด ที่จะใช้เพื่อรายงานเหตุการณ์ เช่น วิธีรายงานและจัดการกับเหตุการณ์ความ ปลอดภัยทางกายภาพ

7.5 การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อมอื่นๆ (Protecting Against Physical and Environmental Threats)

ต้องมีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ อัคคีภัย ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์ และธรรมชาติ พร้อมทั้งให้มีการทดสอบระบบรักษาความปลอดภัยอย่างน้อยปีละ 1 ครั้ง

7.6 การปฏิบัติงานบริเวรที่ต้องรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

7.6.1 บุคคลภายนอกหรือผู้ให้บริการภายนอกที่มีความจำเป็นต้องเข้า-ออกพื้นที่ควบคุมต้องได้รับอนุญาตก่อนเข้า

7.6.2 มีการบันทึกการเข้า-ออกพื้นที่ควบคุม และบันทึกวัตถุประสงค์ในการเข้าพื้นที่ควบคุม

7.6.3 บุคคลภายนอกหรือผู้ให้บริการภายนอกต้องไม่พกพาอาวุธ วัตถุต้องห้าม หรือวัสดุที่อาจเป็นเชื้อเพลิง ยกเว้นเครื่องใช้สำนักงานเข้ามาภายในพื้นที่ควบคุม

7.6.4 ห้ามถ่ายภาพ ห้ามสูบบุหรี่ ห้ามนำอาหาร และเครื่องดื่มเข้ามาในพื้นที่ควบคุม

7.7 การจัดระเบียบโต๊ะทำงาน และหน้าจออุปกรณ์สารสนเทศ (Clear Desk and Clear Screen)

7.7.1 ข้อมูลความลับหรือข้อมูลที่มีความสำคัญที่บันทึกอยู่ในรูปแบบกระดาษหรือที่จัดเก็บในสื่อบันทึกข้อมูลทาง อิเล็กทรอนิกส์ต้องมีการจัดเก็บอย่างปลอดภัยเมื่อไม่มีความจำเป็นในการใช้งาน

7.7.2 เมื่อไม่ได้ใช้งานต้องล็อกหน้าจอคอมพิวเตอร์ด้วยรหัสผ่าน หรือระบบการยืนยันตัวตนอื่นๆ

7.7.3 เอกสารที่มีชั้นความลับ หรือเอกสารสำคัญต้องไม่วางทิ้งไว้บนโต๊ะทำงานg ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

7.8 การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and production)

7.8.1 การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Siting and Protection)

1) ต้องจัดตั้งอุปกรณ์หรือเครื่องมือไว้ในสถานที่ที่ปลอดภัย รวมทั้งมีการป้องกันภัย หรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์ และอุปกรณ์สนับสนุนการทำงาน เช่น ติดตั้งสายนำสัญญาณ เครื่องปรับอากาศ เครื่องสำรองไฟฟ้า เพื่อให้สามารถทำงานได้อย่าง ต่อเนื่องและราบรื่น

2) ต้องจัดวางอุปกรณ์สารสนเทศในตำแหน่งที่เหมาะสมเพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจากบุคคลภายนอก

7.9 ความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศที่ใช้งานอยู่นอกหน่วยงาน (Security of Asset Off-Premises)

7.9.1 การนำอุปกรณ์สารสนเทศไปใช้งานนอกสำนักงานต้องได้รับอนุญาตก่อนนำอุปกรณ์ออก ไปใช้งาน

7.9.2 ไม่ทิ้งอุปกรณ์หรือทรัพย์สินสารสนเทศโดยไม่มีผู้ดูแล

7.9.3 ผู้ใช้งานที่นำอุปกรณ์ไปใช้งานนอกสำนักงานมีความตระหนักพึงระวังรักษาข้อมูลเครื่องคอมพิวเตอร์หรือ อุปกรณ์ซึ่งเป็นทรัพย์สินของบริษัทเสมือนเช่นทรัพย์สินของตนเอง

7.10 สื่อบันทึกข้อมูล (Storage Media)

7.10.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

1) การบริหารจัดการสำหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ต้องมีการจัดทำขั้นตอนสำหรับบริหารจัดการสื่อบันทึกข้อมูลโดยต้องมีความสอดคล้องกับวิธี หรือ ขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทฯ กำหนดไว้

2) สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต

7.10.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

1) การทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของ ข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม

2) การทำลายข้อมูลที่อยู่ภายในสื่อบันทึกข้อมูลจะต้องได้รับการควบคุมด้วยขั้นตอนการปฏิบัติที่เป็นทางการ เพื่อให้มั่นใจว่าข้อมูลจะไม่ถูกทำลายโดยไม่ได้รับอนุมัติ

7.10.3 การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

พนักงานในบริษัทฯทุกระดับต้องไม่นำทรัพย์สินและอุปกรณ์ออกภายนอกบริษัทโดยไม่ได้รับการพิจารณาจากหัวหน้าหน่วยงานหรือผู้มีอำนาจ

7.10.4 การนำสินทรัพย์ของบริษัทฯ ออกนอกหน่วยงาน (Removal of Asset)

1) ห้ามนำทรัพย์สินหรืออุปกรณ์สารสนเทศไปใช้งานนอกหน่วยงานโดยไม่ได้รับอนุญาต

2) ให้มีการบันทึกการนำทรัพย์สินหรืออุปกรณ์สารสนเทศก่อนนำออกและบันทึกการส่งคืนเพื่อเก็บเป็นหลักฐานป้องกันการสูญหาย

7.11 การดูแลอุปกรณ์ต่างๆ (Supporting Utilities)

7.11.1 ต้องมีระบบสนับสนุนการทำงานของระบบควบคุมอุณหภูมิ และความชื้นของบริษัทที่ เพียงพอต่อการใช้งาน เช่น ระบบกระแสไฟฟ้า การควบคุมอุณหภูมิ เครื่องปรับอากาศ ระบบไฟฟ้าหลักและสำรอง เป็นต้น

7.11.2 ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบ และอุปกรณ์สนับสนุนต่างๆ เช่น ระบบกระแสไฟฟ้า ระบบไฟฟ้าสำรอง ระบบควบคุมอุณหภูมิ ระบบความชื้น และระบบ ปรับอากาศ เป็นต้น เพื่อป้องกันการล้มเหลวของระบบเทคโนโลยีสารสนเทศอันส่งผลต่อ ความต่อเนื่องในการดำเนินธุรกิจ

7.12 การเดินสายไฟ และสายเคเบิล (Cabling Security)

ต้องกำหนดให้มีการป้องกันการเดินสายไฟฟ้าสายสื่อสารหรือสายเคเบิ้ลต้องได้รับการป้องกันจากการ เข้าถึงโดยไม่ได้รับอนุญาตหรือทำให้เกิดความเสียหายกับสายสัญญาณและส่งผลต่อการทำงาน ทำให้เกิดการหยุดชะงักซึ่งต้องคำนึงถึงสิ่งเหล่านี้

7.12.1 จัดให้มีการเดินสายไฟฟ้าสายสื่อสารหรือสายสัญญาณอื่นๆจากภายนอกอาคารผ่านลอด เข้ามาทาง ฝ้าเพดาน หรือใต้ดินเพื่อเข้ามาที่ตัวอาคารเพื่อป้องกันการเข้าถึงสายสัญญาณโดยผู้ไม่ประสงค์ดี

7.12.2 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของบริษัทฯในลักษณะที่ผ่านเข้าไปในบริเวณที่มีบุคคลภายนอก สามารถเข้าถึงได้ซึ่งอาจลักลอบดักจับข้อมูลในสายสัญญาณได้

7.12.3 บริเวณที่มีการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารและมีการติดตั้งตู้พักสายต้องล็อกไว้ ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่ หรือบุคคลที่มีสิทธิ เท่านั้น

7.12.4 ต้องกำหนดให้มีการร้อยสายสัญญาณต่างๆเข้าไปในท่อเพื่อป้องกันการดักแอบจับ สัญญาณ การถูกสัตว์กัดแทะ หรือการตัดสายสัญญาณซึ่งทำให้เกิดความเสียหายได้

7.12.5 ต้องกำหนดให้มีการเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกัน การแทรกแซง ของสัญญาณซึ่งกันและกัน

7.12.6 ต้องกำหนดให้มีการจัดทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อให้สามารถ ค้นหาเส้นสายสัญญาณที่ต้องการได้โดยง่าย เช่น ในการแก้ไขปัญหาที่เกิดจากสาย สัญญาณมีปัญหา เป็นต้น

7.12.7 ต้องกำหนดให้มีการทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้องรวมทั้ง ปรับปรุงให้ทันสมัยเสมอ

7.12.8 ต้องกำหนดให้มีการปิดล็อกห้องที่มีสายสัญญาณสื่อสารต่าง ๆเพื่อป้องกันการเข้าถึงโดยบุคคลภายนอก หรือบุคคลที่ไม่มีสิทธิ

7.13 การดูแลรักษาอุปกรณ์ (Equipment Maintenance)

ต้องกำหนดให้มีการดูแล และบำรุงรักษาอุปกรณ์อย่างถูกต้องสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงอย่างน้อยปีละ 1 ครั้ง

7.14 การจัดการอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้ใหม่ (Secure Disposal or Re-use of Equipment)

7.14.1 ต้องกำหนดให้มีวิธีการในการตรวจสอบอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เพื่อป้องกันการรั่วไหล หรือการเปิดเผยข้อมูลดังกล่าวก่อนนำ อุปกรณ์ไปแจกจ่าย

7.14.2 ก่อนนำอุปกรณ์กลับมาใช้ใหม่ให้ทำลายข้อมูลทั้งหมดที่อยู่ในสื่อบันทึกข้อมูลก่อนนำไปใช้

A8 มาตรการควบคุมทางด้านเทคโนโลยี (Technological Control)

8.1 การใช้อุปกรณ์ (User endpoint devices)

8.1.1 นโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile Device Policy)

1) ผู้ปฏิบัติงานในบริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) ควรมีความตระหนักถึง การป้องกันดูแลรักษาอุปกรณ์สื่อสารประเภทพกพาทั้งทางกายภาพและข้อมูลสำคัญที่อยู่ภายในอุปกรณ์โดยทางกายภาพให้ทำการล็อกอุปกรณ์ไว้กับโต๊ะหรือนำไปเก็บ ไว้ในตู้ที่สามารถล็อกได้ส่วนข้อมูลสำคัญที่อยู่ภายในอุปกรณ์ให้มีการป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับ อนุญาตซึ่งทำได้โดยการเข้ารหัสข้อมูลเพื่อเข้าถึงข้อมูลสำคัญ ที่อยู่ภายในอุปกรณ์และรวมไปถึงให้มีการสำรองข้อมูลสำคัญที่อยู่ภายในอุปกรณ์ไว้ อย่างสม่ำเสมอด้วย

2) ผู้ปฏิบัติงานในบริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) ต้องทำการขออนุญาตก่อนที่จะนำอุปกรณ์สื่อสารประเภทพกพาของตนเอง เช่น เครื่องคอมพิวเตอร์แบบพกพา / Notebook / Tablet / Smartphone อุปกรณ์สื่อสาร เคลื่อนที่อื่นๆ ที่เชื่อมต่อเข้ากับเครือข่ายของบริษัทฯ รวมทั้งควรมีความตระหนักเพื่อให้มีความระมัดระวัง หากอุปกรณ์สื่อสารประเภทพกพาของบริษัทฯ ออกไปเชื่อมต่อกับเครือข่ายภายนอก

8.1.2 การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment)

1) ผู้ใช้งานต้องป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์ระบบเทคโนโลยีสารสนเทศเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ไม่มีผู้ดูแล

2) ผู้ใช้งานต้องออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นการปฏิบัติงานและปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการปฏิบัติงานประจำวัน

3) ผู้ดูแลระบบคอมพิวเตอร์กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจอ (Screen Saver) แบบที่มีรหัสป้องกันทุก 10 นาที หรือล็อกหน้าจอเมื่อไม่มีการใช้งาน

8.2 การบริหารจัดการสิทธิ์ตามระดับสิทธิ์การเข้าถึง (Privileged Access Right)

8.2.1 บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับสูง เช่น Root หรือ Administrator หรือเทียบเท่าต้องได้รับการพิจารณามอบหมายแก่ผู้ปฏิบัติงาน ตามความจำเป็นและ มีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสม กับการทำงานเท่านั้น

8.2.2 กรณีมีความจำเป็นต้องให้สิทธิในระดับสูงแก่ผู้ปฏิบัติการหรือบุคคลภายนอกต้องมีการ พิจารณาการควบคุมอย่างรัดกุม โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

1) ต้องได้รับความเห็นชอบและอนุมัติจากเจ้าของระบบสารสนเทศนั้น ๆ
2) ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
3) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
4) ต้องมีการเปลี่ยนรหัสผ่านหลังเสร็จสิ้นการใช้งาน

8.3 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

8.3.1 ต้องมีการควบคุมการใช้งานสารสนเทศในระบบเทคโนโลยีสารสนเทศ ได้แก่ กำหนด สิทธิในการใช้งาน เช่น เขียนอ่านลบได้เป็นต้นกำหนดกลุ่มของผู้ใช้ที่สามารถใช้งาน ได้ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้น มีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

8.3.2 บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศ ในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและ มีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

8.3.3 บุคคลภายนอกต้องจะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ ก่อนที่ปฏิบัติงาน

8.4 การควบคุมการเข้าถึงซอร์สโค้ด (Access to Source Code)

8.4.1 ผู้พัฒนาระบบเทคโนโลยีสารสนเทศต้องจัดเก็บรหัสต้นฉบับ (Source Code) และคลัง โปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มี ความมั่นคงปลอดภัย

8.4.2 ผู้พัฒนาระบบเทคโนโลยีสารสนเทศต้องไม่เก็บรหัสต้นฉบับ (Source Code) ของ โปรแกรมที่อยู่ระหว่างการทดสอบไว้รวมกับรหัสต้นฉบับที่ใช้งานจริง

8.5 ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure authentication)

ควรกำหนดคุณสมบัติ หรือวิธีการล็อกอินเข้าใช้ระบบให้มีความปลอดภัย (Secure Log-on) เมื่อมีระบบใหม่ที่ได้รับการอนุมัติให้จัดหา และติดตั้งพิจารณากำหนดคุณสมบัติ เช่น

8.5.1 การไม่แสดงชื่อหรือรายละเอียดของระบบจนกว่าจะล็อกอินสำเร็จ

8.5.2 การไม่มี หรือ การไม่แสดงฟังก์ชั่นให้การช่วยเหลือ (Help Menu) ในระหว่างที่ทำ การล็อกอิน

8.5.3 การบันทึกข้อมูลความสำเร็จ หรือการล้มเหลวในการล็อกอินแต่ละครั้งของผู้ใช้งาน (เพื่อใช้ในการตรวจสอบในภายหลัง)

8.5.4 การไม่แสดงข้อมูลรหัสผ่านให้เห็นบนหน้าจอในขณะที่ผู้ใช้งานใส่ข้อมูลรหัสผ่านของตน

8.6 การบริหารจัดการขีดความสามารถของทรัพยากรสารสนเทศ (Capacity Management)

8.6.1 ต้องมีการติดตามสภาพการใช้งานและวิเคราะห์ขีดความสามารถของทรัพยากรสารสน เทศปัจจุบันอย่าง สม่ำเสมอตามความเหมาะสมของทรัพยากรชนิดต่าง ๆเพื่อวางแผน บริหารทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม

8.6.2 ต้องมีการวางแผนบริหารทรัพยากรสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจาก ความต้องการใช้งานทรัพยากรสารสนเทศในอนาคต (อาทิ ความต้องการใน 1 ปี ที่จะถึง เช่น CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น เป็นต้น) สภาพการใช้งาน ทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี

8.7 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

8.7.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

1) เครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แบบพกพาต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสที่ได้รับการอัพเดตข้อมูลปัจจุบัน

2) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัสต้องมีการอัพเดทข้อมูลล่าสุด อยู่เสมอ

8.8 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical Vulnerability)

8.8.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

1) ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

2) ต้องอัพเดทระบบซอฟต์แวร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ อย่างสม่ำเสมอรวมถึงต้องกำหนดและจำกัดรายการของซอฟต์แวร์ที่ติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่าย

8.8.2 การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งานหรือให้บริการอยู่แล้ว ตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่า ระบบสามารถถูกบุกรุกได้หรือไม่การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไป

อย่างปลอดภัยหรือไม่รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

8.9 การจัดการการตั้งค่า (Configuration Management)

ต้องกำหนดให้บริษัทฯ ต้องบริหารจัดการวงจรทั้งหมดของการกำหนดค่าความปลอดภัยสำหรับ เทคโนโลยีสารสนเทศ เพื่อให้แน่ใจว่ามีระดับความปลอดภัยที่เหมาะสม และเพื่อหลีกเลี่ยงการเปลี่ยน แปลงที่ไม่ได้รับอนุญาต ซึ่งรวมถึงการกำหนด Configuration การนำไปใช้ การมอนิเตอร์ และการ ทบทวน

บริษัทฯ มีการจัดทำกระบวนการ สำหรับการเสนอ ตรวจสอบ และอนุมัติการกำหนดค่าความ ปลอดภัยตลอดจนกระบวนการสำหรับจัดการและตรวจสอบ การกำหนด ค่าต้องมีการทบทวนการ เปลี่ยนแปลงการกำหนดค่าทั้งหมดอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

8.10 การลบข้อมูล (Information deletion control)

ควรลบสารสนเทศที่จัดเก็บไว้ในระบบสารสนเทศอุปกรณ์หรือสื่อจัดเก็บข้อมูลอื่นๆ ทิ้งเมื่อไม่ต้อง การใช้อีกต่อไป และเพื่อป้องกันการเปิดเผยสารสนเทศที่ละเอียดอ่อนโดยไม่จำเป็นและเพื่อให้สอดคล้องกับ ข้อกำหนด พรบ. คุ้มครองข้อมูลส่วนบุคคลสำหรับการลบข้อมูลสารสนเทศ

เมื่อใช้บริการระบบคลาวด์ บริษัทฯ ควรทวนสอบว่าวิธีการลบที่ผู้ให้บริการคลาวด์ให้มานั้น สามารถยอมรับได้หรือไม่และหากเป็นกรณีเช่นนี้บริษัทฯควรใช้หรือขอให้ผู้ให้บริการคลาวด์ลบสารสน เทศ กระบวนการลบเหล่านี้ควรเป็นแบบอัตโนมัติตามนโยบายหากมีและนำไปใช้ได้บันทึกสามารถ ติดตามหรือทวนสอบว่ามีกระบนการลบสารสนเทศเกิดขึ้นทั้งนี้ขึ้นอยู่กับความละเอียดอ่อนของสารสนg เทศที่ถูกลบ

เพื่อหลีกเลี่ยงการเปิดเผยสารสนเทศที่ละเอียดอ่อนโดยไม่ได้ตั้งใจเมื่ออุปกรณ์ถูกส่งกลับไปให้ผู้g ขายควรคุ้มครองข้อมูลสารสนเทศที่ละเอียดอ่อนโดยการนำที่เก็บข้อมูลฮาร์ดดิสก์ไดรฟ์ และหน่วย ความจำออกก่อนที่จะส่งอุปกรณ์ออกนอกบริษัทฯ

8.11 การซ่อนข้อมูล (Data Marking)

8.11.1 ควรใช้การปิดบังข้อมูลตามนโยบายเฉพาะหัวข้อของบริษัทฯเกี่ยวกับการควบคุมการเข้าถึงและข้อกำหนดทางธุรกิจเฉพาะหัวข้ออื่นๆ ที่เกี่ยวข้องโดยคำนึงถึงกฎหมายที่บังคับใช้ และเพื่อจำกัดการเปิดเผยข้อมูลที่ละเอียดอ่อน รวมถึงข้อมูลส่วนบุคคลที่สามารถระบุ ตัวตนได้และเพื่อให้เป็นไปตามข้อกำหนดทางกฎหมาย พรบ. คุ้มครองข้อมูลส่วนบุคคล ระเบียบข้อบังคับและสัญญา

8.11.2 ในกรณีที่มีความกังวลเรื่องการคุ้มครองข้อมูลที่ละเอียดอ่อน (Sensitive persernal data) บริษัท ฯ ควรพิจารณาซ่อนข้อมูลดังกล่าวโดยใช้มาตรการทางเทคนิคต่างๆ เช่น การปิด บังข้อมูลโดยขีดฆ่าบนเอกสาร การแฝงข้อมูล (Pseudonymization) การทำข้อมูลนิรนาม (Anonymization)

8.11.3 เมื่อใช้เทคนิคการแฝงข้อมูลหรือเทคนิคการทำข้อมูลนิรนามควรทวนสอบว่าเพียงพอและเหมาะสมการทำให้ข้อมูลไม่เปิดเผยตัวตนควรพิจารณาองค์ประกอบทั้งหมดของข้อมูลที่ละเอียดอ่อนเพื่อให้มีประสิทธิภาพตัวอย่าง เช่น หากพิจารณาอย่างไม่ถูกต้องก็จะ สามารถระบุตัวตนของบุคคลได้แม้ว่าข้อมูลที่สามารถระบุตัวบุคคลนั้นได้โดยตรงนั้น จะ ไม่ได้ระบุชื่อก็ตามโดยการมีข้อมูลเพิ่มเติมซึ่งทำให้ สามารถระบุตัวบุคคลได้ทางอ้อม

8.12 การป้องกันข้อมูลรั่วไร (Data Leakage prevent control)

ต้องมีมาตรการป้องกันการรั่วไหลของข้อมูลต่างๆ เพื่อหลีกเลี่ยงการเปิดเผยข้อมูลที่ละเอียดอ่อน โดยไม่ได้รับอนุญาต และหากเกิดเหตุการณ์การรั่วไหลของข้อมูลและสามารถที่จะตรวจจับได้อย่างทัน ท่วงที ซึ่งรวมถึงข้อมูลในระบบเทคโนโลยีสารสนเทศ เครือข่าย หรืออุปกรณ์อื่นๆ

บริษัทฯ มีการกำหนดกระบวนการจัดการชั้นความลับของข้อมูล และประเมินความเสี่ยงด้านเทค โนโลยีสารสนเทศ และตรวจสอบช่องโหว่ที่มีโอกาสเกิดการรั่วไหลของข้อมูล และมีมาตรการปกป้อง ข้อมูล

8.13 การสำรองข้อมูล (Information backup)

8.13.1 การสำรองข้อมูล (Information Backup)

1) ต้องกำหนดความถี่ในการทำการสำรองข้อมูลขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล

2) ต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพสามารถใช้งานได้ตลอดเวลา

3) ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบเทคโนโลยีสารสนเทศ

4) ต้องมีกระบวนการสำรองข้อมูลและการกู้ข้อมูลของทุกระบบต้องมีการทำเอกสารและมีการตรวจ สอบและทดสอบเป็นระยะๆเพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่าง สมบูรณ์

5) กระบวนการในการเก็บข้อมูลระหว่างสถานที่ระบบคอมพิวเตอร์และสถานที่เก็บข้อมูลต้องได้รับ การตรวจสอบอย่างน้อยปีละ 1 ครั้ง

8.14 การเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancy of information processing facilities)

สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)

8.14.1 อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรง ตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนด

8.14.2 กำหนดให้ทดสอบระบบปฏิบัติงานสำรองอย่างสม่ำเสมอเพื่อมั่นใจได้ว่าจะสามารถทำงานทดแทนระบบหลักได้เมื่อมีความจำเป็นต้องใช้งาน

8.15 การบันทึกข้อมูลล็อก และการเฝ้าระวัง (Logging and Monitoring)

8.15.1 การบันทึกข้อมูลเหตุการณ์ (Event Logging).

1) ระบบคอมพิวเตอร์หรือระบบระบบเครือข่ายต้องมีการเก็บบันทึกข้อมูลล็อกต้องบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบเทคโนโลยีสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่างๆ เพื่อประโยชน์ในการสืบสวน สอบสวนในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง รวมทั้งให้มีการวิเคราะห์ข้อมูลล็อก ดังกล่าวอย่างสม่ำเสมอ และจัดการแก้ไขข้อผิดพลาดอย่างเหมาะสม

2) ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องจัดให้มีขั้นตอนการเฝ้าติดตามสังเกตการใช้ งานระบบเทคโนโลยี สารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกต ดังกล่าวอย่างสม่ำเสมอ

3) ผู้ดูแลระบบเทคโนโลgสารสนเทศ ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นระยะเวลาไม่น้อยกว่า 90 วัน

8.15.2 การป้องกันข้อมูลล็อก (Protection of Log Information)

ต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการ ใช้งานสารสนเทศเพื่อป้องกันการเปลี่ยนแปลง หรือการแก้ไขโดยไม่ได้รับอนุญาต

8.15.3 ข้อมูลล็อกของผู้ดูแลระบบ และเจ้าหน้าที่ปฏิบัติการ (Administrator and Operator Logs)

ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบเทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ รวมถึงอุปกรณ์คอมพิวเตอร์ และเครือข่าย

8.16 การเฝ้าติดตามกิจกรรม (Monitoring activities)

8.16.1 บริษัทฯ มีกระบวนการสอบทานและพิจารณาการดำเนินงานตามระบบการควบคุมภายใน ที่กำหนดขึ้นของหน่วยงานว่าอยู่ในระดับที่เหมาะสมเป็นไปตามวัตถุประสงค์การควบคุม ภายในอย่างมีประสิทธิภาพ ประสิทธิผล คุ้มค่า และมีการปรับปรุงให้สอดคล้องกับ สถานการณ์ปัจจุบั

8.16.2 ควรเฝ้าติดตามเครือข่ายระบบและแอปพลิเคชันเพื่อหาพฤติกรรมที่ผิดปกติและการ ดำเนินการหมาะสมเพื่อ ประเมินอุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศ ที่อาจเกิดขึ้นและเพื่อตรวจจับพฤติกรรมที่ผิดปกติและอุบัติการณ์ด้านการรักษาความ ปลอดภัยของสารสนเทศที่อาจเกิดขึ้น

8.16.3 ควรกำหนดขอบเขตและระดับการเฝ้าติดตามตามข้อกำหนดทางธุรกิจและการรักษา ความปลอดภัยของ สารสนเทศและคำนึงถึงกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง ควรดูแลเก็บรักษาบันทึกการเฝ้าติดตามตาม ระยะเวลาการเก็บรักษาที่กำหนดไว้

8.17 การตั้งเวลาให้ถูกต้อง (Clock Synchronization)

จะต้องตั้งแหล่งเทียบเวลานาฬิกา เช่น โปรโตคอลเวลาเครือข่าย (Network Time Protocol) ให้เป็นไปตามมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อให้เวลาที่ปรากฏในปูม เหตุการณ์ (Log) ที่ได้จากระบบเทคโนโลยีสารสนเทศ และอุปกรณ์เครือข่ายคอมพิวเตอร์เป็นเวลา ถูกต้องตรงกัน และสามารถนำไปใช้ในการตรวจสอบได้

8.18 การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

8.18.1 ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิดในการใช้โปรแกรมอรรถประโยชน์ที่อาจ ละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องกำหนดให้มีการควบคุมการใช้ โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องการเข้าถึงโดย ผู้ที่ไม่ได้รับอนุญาต ได้แก่

1) ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
2) จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
3) ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ผู้ใช้งานระบบ เป็นต้น

8.19 การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems)

8.19.1 ต้องควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี ซอฟต์แวร์อุดช่องโหว่ลงใน เครื่องแม่ข่ายที่ให้บริการอยู่โดยต้องมีการทดสอบซอฟต์แวร์เหล่านั้นก่อนเพื่อให้มั่นใจว่าจะไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

8.19.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

1) ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญาที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด

2) ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

8.20 ความมั่นคงปลอดภัยระบบเครือข่าย (Network Security)

8.20.1 การควบคุมการเข้าถึงเครือข่าย (Network Control)

1) ผู้ดูแลระบบเครือข่ายต้องจำกัดการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศที่เชื่อมต่อ อยู่กับระบบเครือข่ายโดยกำหนดให้ผู้ใช้งานในเครือข่ายสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศ ผ่านทางระบบการพิสูจน์ตัวตน

2) ผู้ดูแลระบบเครือข่ายต้องทดสอบความปลอดภัยทุกครั้งที่จะเชื่อมต่อกับระบบเครือข่ายของบุคคลภายนอก เพื่อให้มั่นใจว่าไม่มีการเข้าถึงทรัพยากรที่ไม่ได้รับอนุญาต

3) ผู้ดูแลระบบเครือข่ายต้องควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดย ไม่ได้รับอนุญาต

4) การเข้าถึงอุปกรณ์เครือข่ายเพื่อการตรวจสอบและปรับแต่งระบบทั้งทางกายภาพและการเข้าถึง จากระยะไกลต้องมีการควบคุม และทำได้เพียงแต่เฉพาะผู้ดูแลระบบเครือข่ายที่ได้รับอนุญาต

5) ในกรณีที่ต้องกำหนดสิทธิการเข้าถึงแบบชั่วคราวแก่บุคคลภายนอก

6) ผู้ดูแลระบบเครือข่ายต้องให้มีผู้ควบคุมตรวจสอบ และยกเลิกสิทธิการเข้าถึงทันที ที่ปฏิบัติงานเสร็จ

7) ผู้ดูแลระบบเครือข่ายต้องตรวจสอบ และปิดพอร์ตของอุปกรณ์เครือข่ายที่ไม่ใช้งาน

8) การให้บริการทางเครือข่ายสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบเครือข่ายต้องอนุญาตเฉพาะพอร์ต (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

9) ผู้ดูแลระบบเครือข่ายต้อง Update Security Patch ของอุปกรณ์เครือข่ายอย่างสม่ำเสมอ

10) ผู้ดูแลระบบเครือข่ายต้องจัดทำแผนผังเครือข่าย (Network Diagram) ซึ่งมีรายละเอียด เกี่ยวกับขอบเขตของระบบเครือข่ายภายในบริษัทฯ พร้อมทั้งปรับปรุงให้ เป็นปัจจุบันอยู่เสมอ

11) ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องกับกฎหมาย

8.21 ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

8.21.1 ผู้ใช้งานต้องใช้บริการระบบเครือข่ายตามที่ผู้ดูแลระบบเครือข่ายอนุญาตเท่านั้น

8.21.2 ผู้ใช้งานต้องใช้ระบบเครือข่ายที่ไม่กระทบต่อประสิทธิภาพการใช้งานเครือข่ายโดยรวม เช่น การรับ-ส่งไฟล์ขนาดใหญ่ การดาวน์โหลด หรือการอัปโหลดไฟล์ที่มีขนาดใหญ่ เป็นต้น

8.21.3 ห้ามผู้ใช้งานอุปกรณ์เครือข่ายเชื่อมต่อกับระบบเครือข่ายของบริษัทก่อนได้รับอนุญาต จากผู้ดูแลระบบเครือข่าย

8.21.4 ห้ามใช้เครือข่ายเพื่อกระทำสิ่งที่ผิดกฎหมาย

8.21.5 ผู้ใช้งานต้องเข้าใช้ระบบเครือข่ายด้วยบัญชีผู้ใช้งานของตนเองเท่านั้น

8.21.6 ห้ามเผยแพร่ข้อมูลของผู้อื่นหรือของหน่วยงาน โดยไม่ได้รับอนุญาต

8.21.7 ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ จากภายนอกเข้า กับระบบคอมพิวเตอร์ และระบบเครือข่ายโดยเด็ดขาดหากมีความจำเป็นต้องใช้งาน ต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

8.21.8 ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่าง เช่น Router Switch Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับ อนุญาตเด็ดขาด

8.22 การจัดแบ่งเครือข่ายภายในสำนักงานฯ (Segregation in Network)

8.22.1 กลุ่มที่ให้บริการระบบเทคโนโลยีสารสนเทศเป็นระบบเครือข่ายที่สามารถเข้าถึง และ ใช้งานโดยผู้ใช้งาน เช่น ระบบอินทราเน็ต ระบบจดหมายอิเล็กทรอนิกส์ เป็นต้น

8.22.2 กลุ่มที่ให้บริการระบบเทคโนโลยีสารสนเทศ เป็นระบบเครือข่ายที่เข้าถึง และใช้งาน โดยระบบเทคโนโลยีสารสนเทศ ซึ่งต้องไม่ถูกเข้าถึงจากผู้ใช้งานโดยตรง เช่น ระบบฐาน ข้อมูล ระบบ Directory Service ระบบ Domain Name System (DNS) ระบบ Printer Service เป็นต้น

1) กลุ่มที่ให้บริการผู้ใช้งานเป็นระบบเครือข่ายที่สามารถเข้าถึง และใช้งานโดยเครื่องคอมพิวเตอร์ของผู้ใช้งาน

2) กลุ่มที่ให้บริการผู้ใช้งานแบบไร้สายเป็นเครือข่ายสามารถเข้าถึง และใช้งานโดย เครื่องคอมพิวเตอร์พกพา แท็บเล็ต และสมาร์ทโฟนของผู้ใช้งาน

3) ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และโซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของ

เครือข่ายภายใน และเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

8.23 การกรองเว็ป (Web Filtering)

บริษัทฯ มีการควบคุมการเข้าถึง กรองข้อมูล/บล็อกและจำกัดสิทธิการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัยหรือเว็บเสี่ยงแบบอัตโนมัติ ผู้ใช้งานไม่สามารถทราบได้ว่าเว็บไซต์ไหนปลอดภัย หรือเว็บไซต์ ไหนเป็นอันตราย ฝ่ายเทคโนโลยีสารสนเทศจะเป็นผู้ตรวจสอบและกำหนดนโยบายการกรองเว็ป (Web Filtering) และทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

8.24 การกำหนดการควบคุมการเข้ารหัสข้อมูล (Use of Cryptography)

8.24.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

1) เมื่อต้องการป้องกันความลับของข้อมูล หรือสารสนเทศด้วยวิธีการเข้ารหัสลับ ผู้ปฏิบัติงานใน บริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) ต้องใช้เทคนิค หรือ ขั้นตอนวิธีที่ได้กำหนดไว้ในมาตรฐาน การบริหารจัดการความมั่นคงปลอดภัย สารสนเทศ

2) ระบบเครือข่ายคอมพิวเตอร์ภายในบริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) เมื่อต้องการป้องกันความลับของข้อมูลที่สื่อสารภายในด้วยวิธีการเข้ารหัสลับการควบคุมนั้นต้องใช้ เทคนิคหรือขั้นตอนวิธีที่ได้กำหนดไว้ในมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

8.24.2 การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management)

กุญแจรหัสลับที่ใช้ในการเข้ารหัสลับสำหรับระบบเครือข่ายคอมพิวเตอร์ภายใน บริษัท เคซีจี คอร์ปอเรชั่น จำกัด (มหาชน) ต้องได้รับการควบคุมดูแลการกำหนดกุญแจรหัสลับ การจัดเก็บกุญแจรหัสลับ การเปลี่ยนกุญแจรหัสลับ และการครอบครองกุญแจรหัสลับ

8.25 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

8.25.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)

ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และมีการปฏิบัติตามนโยบายหรือข้อกำหนดที่ บริษัทฯ กำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ควรคำนึงความปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนาตรวจพบช่วงโหว่ และต้องสามารถแก้ไขช่องโหว่ที่ตรวจพบได้

8.26 ข้อกำหนดความมั่นคงปลอดภัยของแอปพลิเคชัน (Application Security Requirement)

8.26.1 ของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing Application Services on Public Networks)

สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะต้อง ได้รับการป้องกัน และการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

8.26.2 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting Application Services Transactions)

สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศต้องได้รับการป้องกันจากการรับ ส่ง ข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความ การเปิดเผยข้อมูล การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

8.27 สถาปัตยกรรมระบบและหลักการวิศวกรรมระบบความมั่นคงปลอดภัย (Security system architecture and Engineering Principles)

8.27.1 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรมระบบต้องมีการกำหนดขึ้นมาเป็นลาย ลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ

8.28 Secure coding

8.28.1 หลักการเข้ารหัสที่ปลอดภัยในการพัฒนาซอฟต์แวร์และเพื่อตรวจสอบให้แน่ใจว่ามีการ เขียนซอฟต์แวร์อย่าง ปลอดภัยโดยลดจำนวนช่องโหว่ด้านการรักษาความปลอดภัยของ สารสนเทศที่อาจเกิดขึ้นในซอฟต์แวร์

8.28.2 บริษัทฯ ควรกำหนดกระบวนการทั่วทั้งบริษัทฯ เพื่อให้มีการกำกับดูแลดีสำหรับการเข้า รหัสที่ปลอดภัย ควรสร้างและใช้พื้นฐานการรักษาความปลอดภัยขั้นต่ำ นอกจากนี้ควร ขยายกระบวนการและ การกำกับดูแลดังกล่าวให้ครอบคลุมส่วนประกอบของซอฟต์แวร์ จากบุคคลภายนอกและซอฟต์แวร์แบบโอเพ่นซอร์ส

8.28.3 บริษัทฯ ควรเฝ้าติดตามภัยคุกคามในโลกแห่งความเป็นจริงและคำแนะนำล่าสุดและสารสนเทศเกี่ยวกับช่องโหว่ของซอฟต์แวร์เพื่อเป็นแนวทางในหลักการการเข้ารหัสที่ปลอดภัยของบริษัทฯ ผ่านการปรับปรุงและการเรียนรู้อย่างต่อเนื่อง ซึ่งสามารถช่วยให้มั่นใจว่ามีการนำแนวปฏิบัติการเข้ารหัสปลอดภัยมาใช้ต่อสู้กับภูมิทัศน์ภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว

8.28.4 ควรใช้หลักการการเข้ารหัสปลอดภัยทั้งสำหรับการพัฒนาใหม่และในสถานการณ์ที่นำ กลับมาใช้ใหม่ หลักการเหล่านี้ควรนำไปใช้กับกิจกรรมการพัฒนาทั้งภายในบริษัทฯ และสำหรับผลิตภัณฑ์และบริการที่บริษัทฯ มอบให้ผู้อื่น การวางแผน และข้อกำหนด เบื้องต้น

8.29 การทดสอบด้านความมั่นคงปลอดภัยการพัฒนาระบบงาน (Security Testing in development and Acceptance)

8.29.1 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing)

1) ระบบที่พัฒนาขึ้นมาควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยโดยต้องมีการทดสอบอยู่ ในช่วงระหว่างการพัฒนา

2) ผู้พัฒนาระบบสารสนเทศต้องมีการตรวจสอบข้อมูลนำเข้าระบบสารสนเทศ

3) ผู้พัฒนาระบบสารสนเทศต้องมีวิธีการตรวจสอบการประมวลผลข้อมูลสารสนเทศ (Checks and Controls) ว่ามีข้อผิดพลาดหรือไม่

4) ผู้พัฒนาระบบสารสนเทศต้องมีวิธีการตรวจสอบการส่งข้อมูลในระบบสารสนเทศเพื่อให้แน่ใจว่า ข้อมูลในระบบสารสนเทศมีความปลอดภัย และมีความถูกต้องสมบูรณ์

8.29.2 การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)

1) มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบโดยต้องมีการจัดทำทั้งสำหรับระบบใหม่ และระบบที่ปรับปรุง

2) ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือ ทรัพยากรสารสนเทศอื่นๆ ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ทำการทดสอบ ระบบก่อนที่จะตรวจรับระบบนั้น และให้มีการเซ็นชื่อ เจ้า หน้าที่ทำการทดสอบและลายเซ็นผู้ส่งมอบ

8.30 การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (Outsourced Development)

ในการทำสัญญาว่าจ้างการพัฒนาระบบสารสนเทศต้องมีความชัดเจนและครอบคลุมถึงสัญญา ทางด้านลิขสิทธิ์ซอฟต์แวร์การใช้ระบบการตรวจสอบระบบโดยละเอียดก่อนติดตั้งใช้งานจริงรวมถึง การรับรองคุณภาพของระบบและการกำหนดขอบเขตในการจ้างพัฒนาระบบสารสนเทศ

8.31 การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนา ทดสอบ และ สภาพแวดล้อมในการปฏิบัติงาน (Separation of Development, Test and Production development)

8.31.1 การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนา ทดสอบ และ สภาพแวด ล้อมในการปฏิบัติงาน (Separation of Development, Testing and Operational Environment) ต้องมีการแยกระบบสารสนเทศสำหรับการทดสอบ (Development) และ การใช้งานจริง (Production) เช่น ระบบคอมพิวเตอร์และเครือข่ายออกจากกันเพื่อลด ความเสี่ยง ในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบ สารสนเทศโดยไม่ได้รับอนุญาต

8.31.2 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)

ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามนโยบาย หรือข้อกำหนด ที่บริษัทฯ กำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ควรคำนึง ความปลอด ภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการ หลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนาตรวจพบช่วงโหว่ และต้องสามารถแก้ไขช่องโหว่ที่ ตรวจพบได้

8.32 การบริหารการเปลี่ยนแปลง (Change Management)

8.32.1 การบริหารการเปลี่ยนแปลง (Change Management)

1) ก่อนทำการเปลี่ยนแปลงกับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบคอม พิวเตอร์ซอฟต์แวร์หรือฐานข้อมูลโดยผู้ดูแลระบบฯหรือผู้ให้บริการภายนอกต้องดำเนินการขอ อนุมัติ การดำเนินการเปลี่ยนแปลงจากฝ่ายเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

2) การเปลี่ยนแปลงกับระบบเครือข่ายระบบคอมพิวเตอร์ซอฟต์แวร์หรือฐานข้อมูลโดยผู้ให้บริการภาย นอกต้องได้รับการควบคุมดูแลจากผู้ดูแลระบบเทคโนโลยีสารสนเทศ

3) ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องแจ้งให้ผู้ใช้งานทราบก่อนทุกครั้งก่อนทำการเปลี่ยนแปลงระบบ

4) ผู้ดูแลระบบเทคโนโลยีสารสนเทศหรือผู้ให้บริการภายนอกต้องมีการประเมินผลกระทบของการเปลี่ยนแปลงระบบก่อนที่จะทำการเปลี่ยนแปลงนั้นเพื่อป้องกันผลกระทบกับการทำงานของระบบที่ใช้ ดำเนินงานอยู่ในปัจจุบัน

5) ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องบันทึกรายละเอียดการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ

6) ผู้ดูแลระบบเทคโนโลยีสารสนเทศหรือผู้ให้บริการภายนอกต้องมีการทดสอบการเปลี่ยนแปลงนั้นก่อนเสมอ โดยเฉพาะอย่างในกรณีเป็นระบบเทคโนโลยีสารสนเทศ ที่สำคัญ

7) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ หรือผู้ให้บริการภายนอกต้องกำหนดแผนย้อนคืน (Fallback Plan) เพื่อรองรับหากการเปลี่ยนแปลงไม่เป็นไปตามที่คาดคิด

8) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ หรือผู้ให้บริการจากภายนอกต้องกำหนดระยะเวลาในการติดตามการเปลี่ยนแปลงนั้นเพื่อตรวจสอบผลกระทบที่อาจเกิดขึ้นกับระบบหลังจากการเปลี่ยนแปลง

8.32.2 กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)

ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไข ซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น

1) คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ
2) ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
3) ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
4) เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
5) ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

8.32.3 การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes)

เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบ และทดสอบซอฟต์แวร์ต่าง ๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงาน และความมั่นคงปลอดภัย

8.32.4 การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages).

เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็นและ การเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบ และจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้

8.33 ข้อมูลสำหรับการทดสอบ (Test information)

8.33.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

1) ห้ามมิให้ใช้ข้อมูลในระบบที่ใช้ปฏิบัติงานจริงที่ประกอบด้วยข้อมูลส่วนบุคคลหรือ ข้อมูลที่มีชั้นความลับในการทดสอบระบบใด ๆทั้งนี้หากมีความจำเป็นต้องใช้ข้อมูล เหล่านี้จะต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน และต้องมีมาตรการในการป้องกัน การทำสำเนาข้อมูลโดยไม่ได้รับอนุญาต

2) เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันทีและทำการบันทึกไว้เป็น หลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบแจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

8.34 การปกป้องระบบสารสนเทศระหว่างการทดสอบประเมิน (Protection of information systems during audit testing)

8.34.1 การวางแผนการตรวจสอบระบบเทคโนโลยีสารสนเทศทั้งหมด (Information System Audit Controls)

ต้องวางแผนการตรวจสอบระบบโดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อ ระบบและกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด

ประกาศ ณ วันที่ 5 มิถุนายน 2568

-ณัฐชัย วีระกุล-
นายณัฐชัย วีระกุล
รองกรรมการผู้อำนวยการสายงานกลยุทธ์องค์กร
บริษัท เคซีจี คอร์ปอเรชั่นจำกัด (มหาชน)