บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัยสารสนเทศ

(Information Security Policy)

ตามมติที่ประชุมคณะกรรมการบริษัท : ครั้งที่ 1/2567 วันที่ 27 กุมภาพันธ์ 2567

ใช้แทนฉบับลงวันที่ 1 มีนาคม 2565

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

ครั้งที่	รายละเอียด	วันที่มีผลบังคับใช้
01	นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)	30 ตุลาคม 2560
02	แก้ไขทั้งฉบับ	01 มีนาคม 2565
03	แก้ไขโลโก้บริษัท ตามมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2567	27 กุมภาพันธ์ 2567

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

สารบัญ

หน้า

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

สารบัญ

หน้า

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

1. ความมั่นคงปลอดภัยสารสนเทศ (Information Security)

1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์และขอบเขต

นโยบายความมั่นคงปลอดภัยสารสนเทศครอบคลุมถึงการปกป้องข้อมูลสารสนเทศขององค์กรเป็นหลัก เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยของข้อมูล ทำให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

เนื้อหานโยบายและการดำเนินการ

1.1.1 การจัดทำนโยบายความปลอดภัยสารสนเทศ (Policies for Information Security)

นโยบายความมั่นคงปลอดภัยสารสนเทศฉบับนี้ถูกจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์และขอบเขต ต้องได้รับการอนุมัติจากผู้บริหารหรือคณะกรรมการ มีการประกาศใช้และถือปฏิบัติทั่วทั้งองค์กร โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นขององค์กร ตั้งแต่ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูล และทรัพย์สินสารสนเทศขององค์กร

ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและทรัพย์สินสารสนเทศขององค์กร มีหน้าที่โดยตรงที่จะต้องสนับสนุนดำเนินการตามกฎระเบียบว่าด้วยการใช้งานระบบสารสนเทศขององค์กรอย่างปลอดภัย และให้ความร่วมมือในการดำเนินการตามนโยบายอย่างเคร่งครัด การฝ่าฝืนนโยบายนี้ถือเป็นความผิด โดยมีบทลงโทษตามระเบียบขององค์กร

ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้สารสนเทศจะต้องลงนามรับทราบกฎระเบียบว่าด้วยการใช้งานระบบสารสนเทศขององค์กรอย่างปลอดภัย เพื่อรับทราบเงื่อนไขการใช้งานระบบสารสนเทศ (IT-ARRF-03003)

1.1.2 การทบทวนนโยบายความปลอดภัยสารสนเทศ (Review of The Policies for Information Security)

หน่วยงานสารสนเทศ มีหน้าที่รับผิดชอบในการดูแลและสอบทานเนื้อหาของนโยบายอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลง และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความปลอดภัยทางด้านสารสนเทศขององค์กร เช่น การเปลี่ยนแปลงกลยุทธ์ หรือทิศทางด้านเทคโนโลยีสารสนเทศ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเปลี่ยนแปลงโครงสร้างองค์กรหรือโครงสร้างสารสนเทศ เป็นต้น

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

2. ความสอดคล้อง (Compliance)

2.1 นโยบายการทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้มีการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับนโยบาย และขั้นตอนปฏิบัติขององค์กร

2.1.1 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with Security Policies and Standards)

ผู้บริหารระดับสูงและหน่วยงานสารสนเทศ มีหน้าที่ต้องดำเนินการทบทวนความสอดคล้องของขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง ดังนั้นหัวข้อการประชุมและกำหนดระยะเวลาในการทบทวนเพื่อเป็นการตรวจสอบขั้นตอนต่างๆ ว่าได้มีการปฏิบัติตามครบถ้วนหรือไม่ ดังนี้

ขั้นตอนการดำเนินการ	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ
ทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศ	ปีละ 1 ครั้ง	ผู้บริหาร, แผนกเทคโนโลยีสารสนเทศ
ทบทวนระเบียบว่าด้วยการใช้ระบบสารสนเทศเพื่อความปลอดภัย	ปีละ 1 ครั้ง	ผู้บริหาร, แผนกเทคโนโลยีสารสนเทศ
ทบทวนรายการเอกสารสัญญา	ปีละ 1 ครั้ง	ผู้บริหาร, แผนกเทคโนโลยีสารสนเทศ
จัดทำงบประมาณ	ปีละ 1 ครั้ง	แผนกเทคโนโลยีสารสนเทศ
ทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศ	ปีละ 1 ครั้ง	แผนกเทคโนโลยีสารสนเทศ
ทบทวนและตรวจสอบ ตรวจนับทรัพย์สิน 100 %	ปีละ 1 ครั้ง	แผนกเทคโนโลยีสารสนเทศ
ทบทวนและตรวจสถานการณ์ทำงานของระบบสำรองข้อมูล	ปีละ 12 ครั้ง	แผนกเทคโนโลยีสารสนเทศ
ทบทวนและตรวจสอบการแก้ไขปัญหาในระบบสารสนเทศ	ปีละ 12 ครั้ง	แผนกเทคโนโลยีสารสนเทศ

3. การบริหารจัดการทรัพย์สิน (Asset Management)

3.1 นโยบายและหน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets Policy)

วัตถุประสงค์และขอบเขต

ทรัพย์สิน หมายถึง ทรัพย์สินที่เกี่ยวข้องกับข้อมูล เช่น ซอฟต์แวร์ หรือแม้แต่อุปกรณ์ที่เกี่ยวข้องในการประมวลผลต่างๆ นอกจากนี้องค์กรควรกำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน อย่างไรก็ดีเจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว เพื่อให้มีการระบุทรัพย์สินขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

เนื้อหานโยบายและการดำเนินการ

3.1.1 การจัดการบัญชีทรัพย์สิน (Inventory of Assets)

หน่วยงานสารสนเทศจะต้องดำเนินการจัดทำบัญชีทรัพย์สินที่เกี่ยวข้องกับข้อมูลขององค์กร โดยปฏิบัติตามคู่มือขั้นตอนการปฏิบัติงาน เรื่อง การบริหารจัดการเทคโนโลยีสารสนเทศ (IT-OP-01) และทำการตรวจสอบทรัพย์สินร่วมกับผู้ถือครองทรัพย์สินและหน่วยงานที่เกี่ยวข้องเพื่อปรับปรุงทะเบียนทรัพย์สินอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

3.1.2 ผู้ถือครองทรัพย์สิน (Ownership of Assets)

ในการจัดทำทะเบียนทรัพย์สินแต่ละหน่วยงาน จะต้องกำหนดเจ้าของทรัพย์สินที่มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินนั้น เจ้าของทรัพย์สินต้องสอบทานความถูกต้องของรายละเอียดของทรัพย์สินในทะเบียนทรัพย์สินตลอดจนการแจ้งถึงการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับทรัพย์สินให้ผู้ดูแลทรัพย์สินทราบ

3.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable Use of Assets)

กรณีพนักงานเข้าใหม่ จะต้องจัดทำใบรับและคืนทรัพย์สินสารสนเทศ/รับทราบเงื่อนไขการใช้งานระบบสารสนเทศ (IT-ARRF-03003) โดยระบุกฎเกณฑ์การใช้งานทรัพย์สินที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ซึ่งพนักงาน ผู้ใช้งานหรือหน่วยงานภายนอกต้องยินยอมทำตามข้อกำหนดในการใช้งานทรัพย์สินและข้อมูลสารสนเทศ

3.1.4 การคืนทรัพย์สิน (Return of Assets)

พนักงาน ผู้ใช้งานหรือหน่วยงานภายนอก ต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญาหรือสิ้นสุดข้อตกลงการจ้าง โดยจะต้องจัดทำใบรับและคืนทรัพย์สินสารสนเทศ/รับทราบเงื่อนไขการใช้งานระบบสารสนเทศ (IT-ARRF-03003) หรือ จัดทำแบบฟอร์มสำรวจทรัพย์สินของแผนกทรัพยากรบุคคล ที่เกี่ยวข้องกับหน่วยงานเทคโนโลยีสารสนเทศ พร้อมทั้งให้มีการตรวจสภาพทรัพย์สินจากแผนกสารสนเทศเสียก่อน หากผลการตรวจสอบพบว่ามีความชำรุดเสียหายหรือมีข้อมูลบางอย่างขาดหายไป ผู้ถือครองทรัพย์สินนั้นจะต้องรับผิดชอบตามข้อกำหนดที่ได้ตกลงไว้

3.1.5 การระบุสิทธิ์ในทรัพย์สินทางปัญญา (Intellectual Property Rights)

หน่วยงานสารสนเทศจะต้องจัดทำทะเบียนคุมซอฟท์แวร์ลิขสิทธิ์ (IT-SLL-T0303) เพื่อควบคุมลิขสิทธิ์ซอฟต์แวร์และสิทธิ์ในทรัพย์สินทางปัญญา (Intellectual Property Rights) ขององค์กร รวมถึงจะต้องจัดเก็บเอกสารหลักฐานแสดงสิทธิความเป็นเจ้าของที่ถูกต้องตามกฎหมาย

3.2 นโยบายการจัดการสื่อบันทึกข้อมูล (Media Handling Policy)

วัตถุประสงค์และขอบเขต

เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูลเพื่อป้องกันความเสียหายต่อการดำเนินธุรกิจอันเนื่องมาจากความเสียหายของสื่อบันทึกข้อมูลต่างๆ ควรได้รับการควบคุมและจัดการอย่างเหมาะสม

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

เนื้อหานโยบายและการดำเนินการ

3.2.1 การบริหารจัดการสื่อบันทึกข้อมูล (Management of Media)

ขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนที่องค์กรกำหนดไว้

1) การเบิกและจ่ายสื่อบันทึกข้อมูลจะต้องผ่านการอนุมัติจากผู้มีอำนาจของหน่วยงานผู้ใช้
2) สื่อบันทึกข้อมูลต้องมีการตรวจนับอย่างน้อยปีละ 1 ครั้ง

3.2.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างปลอดภัยเมื่อหมดความต้องการในการใช้งาน โดยปฏิบัติตามขั้นตอนการทำลายซึ่งกำหนดไว้ ดังนี้

1) ข้อมูลลำดับชั้นลับมากที่อยู่ในรูปเอกสารที่ต้องการทำลาย ต้องทำลายโดยการเข้าเครื่องย่อยกระดาษหรือด้วยวิธีการอื่นที่จะไม่สามารถนำข้อมูลนั้นกลับมาใช้ใหม่ได้
2) การทำลายสื่อบันทึกข้อมูลที่บันทึกข้อมูลลำดับชั้นลับมากขึ้นไป ต้องได้รับการอนุมัติจากผู้มีอำนาจพร้อมทั้งกำหนดวิธีการและขั้นตอนในการทำลาย และเก็บหลักฐานการทำลาย เพื่อใช้ในการตรวจสอบ

3.2.3 การขนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

สื่อบันทึกข้อมูลที่มีข้อมูล ต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาตหรือการนำไปใช้ผิดวัตถุประสงค์อันจะก่อให้เกิดความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

4. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

4.1 นโยบายพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Secure Areas Policy)

วัตถุประสงค์และขอบเขต

เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร เพื่อกำหนดพื้นที่ควบคุมความมั่นคงปลอดภัยภายในองค์กรและกำหนดมาตรการป้องกันที่เหมาะสมตามระดับของความเสี่ยงในแต่ละพื้นที่ โดยการควบคุมดังกล่าวเป็นการป้องกันสารสนเทศและระบบประมวลผลสารสนเทศขององค์กรขั้นพื้นฐานจากการเข้าถึงโดยไม่ได้รับการอนุญาต

เนื้อหานโยบายและการดำเนินการ

4.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

หน่วยงานได้จัดหาที่ตั้งห้องเซิร์ฟเวอร์ (Server) ที่มีสภาพแวดล้อมปลอดภัยจากภัยคุกคามภายนอก คือ อยู่ในสถานที่ที่เข้าถึงได้ยากจากบุคคลภายนอก อยู่บนอาคารสูงที่สามารถป้องกันเหตุจากน้ำท่วมได้ พื้นที่โดยรอบโปร่งและสามารถมองเห็นได้ชัดหากมีการเข้าถึงห้องเซิร์ฟเวอร์ (Server)

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

4.1.2 การรักษาความปลอดภัยสำนักงาน ห้องทำงานและอุปกรณ์ (Securing Office Room and Facilities)

องค์กรจะกำหนดรายชื่อผู้มีสิทธิ์ในการเข้าถึงห้องเซิร์ฟเวอร์ (Server) โดยหน่วยงานสารสนเทศจะต้องจัดทำเอกสารควบคุมสิทธิ์ในการเข้าห้องเซิร์ฟเวอร์ (Server) เพื่อให้ผู้บริหารอนุมัติ นอกจากนั้นกรณีมีบุคคลภายนอกที่ไม่เกี่ยวข้องจะเข้าไปกระทำการใดๆ ภายในห้องเซิร์ฟเวอร์จะต้องได้รับการอนุมัติก่อนทุกครั้ง พร้อมทั้งให้บันทึกรายละเอียดต่างๆ ในแบบฟอร์มการเข้า-ออก ห้องเซิร์ฟเวอร์ (Server) ของบุคคลภายนอก (IT-VLB-T0402) ให้อย่างครบถ้วน อีกทั้งจะต้องมีการจัดเตรียมอุปกรณ์รักษาความปลอดภัยในการเข้าถึงห้องเซิร์ฟเวอร์ (Server) ดังนี้

1) มีการติดตั้งกล้องวงจรปิด และบันทึกภาพภายในห้องเซิร์ฟเวอร์ (Server) ตลอดเวลาโดยสามารถดูข้อมูลย้อนหลังได้อย่างน้อย 20 วัน
2) ห้องระบบคอมพิวเตอร์ต้องมีการปิดล็อค เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าได้

4.1.3 การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against External and Environmental Threats)

การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ อุบัติเหตุ การโจมตีหรือการบุกรุกต้องมีการออกแบบและดำเนินการ ดังนี้

1) ห้องคอมพิวเตอร์เซิร์ฟเวอร์ (Server Room) ต้องมีระบบป้องกันอัคคีภัย ระบบปรับอากาศและความชื้น ระบบตัดกระแสไฟฟ้า
2) อุณหภูมิห้องเซิร์ฟเวอร์ ความเย็นควรอยู่ที่ 20-23 องศา

4.2 นโยบายเกี่ยวกับการจัดการอุปกรณ์ (Equipment Management Policy)

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อป้องกันการสูญหาย ความเสียหาย การขโมยหรือการที่เป็นอันตรายต่อทรัพย์สิน และป้องกันการหยุดชะงักต่อการดำเนินการขององค์กร อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายถือว่าเป็นอุปกรณ์ที่สำคัญต่อสารสนเทศและการดำเนินธุรกิจ ดังนั้น อุปกรณ์เหล่านี้ควรมีการป้องกันอันตรายจากสภาพแวดล้อมที่ไม่เหมาะสม รวมถึงการจำกัดการนำอุปกรณ์ดังกล่าวไปใช้นอกสถานที่

<u>เนื้อหานโยบายและการดำเนินการ</u>

4.2.1 การติดตามการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย (Server Monitor)

มีการตรวจสอบสถานะการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย ตามรอบของแผนการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ และควรต่อ MA Server กับผู้ให้บริการภายนอกเพื่อลดความเสี่ยงกรณีอุปกรณ์ชำรุดเสียหาย

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

4.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

อุปกรณ์ต้องได้รับการป้องกันการเสียหายจากกระแสไฟฟ้าขัดข้องและการหยุดชะงักอื่นๆ ดังนี้

1) อุปกรณ์คอมพิวเตอร์และเครือข่ายที่สำคัญต้องมีอุปกรณ์สำรองไฟฟ้าฉุกเฉิน (UPS) เพื่อให้ระบบทำงานต่อเนื่องเมื่อระบบไฟฟ้าขัดข้อง
2) ต้องทำการตรวจสอบอุปกรณ์สำรองไฟฟ้าฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าอุปกรณ์ดังกล่าวสามารถรองรับการทำงานได้เมื่อเกิดปัญหาไฟฟ้าขัดข้อง

5. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

5.1 นโยบายบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้มีการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ให้ระบบเครือข่ายมีความปลอดภัย และสามารถใช้เป็นสื่อกลางในการรับส่งข้อมูลต่างๆ ได้อย่างมีประสิทธิภาพ

เนื้อหานโยบายและการดำเนินการ

5.1.1 การควบคุมเครือข่าย (Network Controls)

เครือข่ายต้องมีการบริหารจัดการ และควบคุมเพื่อป้องกันสารสนเทศในระบบต่างๆ หัวหน้าหน่วยงานควบคุมระบบเครือข่ายต้องรับผิดชอบในการจัดให้มีการควบคุมการปฏิบัติการด้านเครือข่าย ดังต่อไปนี้

1) กำหนดและจัดทำแผนผังแสดงเครือข่ายสื่อสาร(Network Configuration) แสดงถึงข้อมูลเกี่ยวกับอุปกรณ์และคู่สายที่ใช้ในการสื่อสารของเครือข่ายทั้งหมดอย่างชัดเจน โดยจัดทำแผนผังเครือข่ายตำแหน่งเครื่องเซิร์ฟเวอร์
2) จัดให้มีการควบคุมการติดตั้งอุปกรณ์สื่อสารให้สอดคล้องกับแผนผังแสดงเครือข่ายสื่อสารที่จัดไว้
3) บำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ

5.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

ความมั่นคงปลอดภัยสำหรับการให้บริการเครือข่าย ต้องมีการระบุไว้ในข้อตกลงการให้บริการเครือข่ายอย่างชัดเจน

5.2 นโยบายการถ่ายโอนสารสนเทศ (Information Transfer Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนสารสนเทศภายในองค์กร และการถ่ายโอนสารสนเทศกับหน่วยงานภายนอกองค์กร

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

เนื้อหานโยบายและการดำเนินการ

5.2.1 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)

ข้อมูลสารสนเทศที่เกี่ยวข้องกับการส่งข้อความอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม

5.2.2 การตรวจสอบการใช้งานเครือข่าย (Network Monitoring)

หน่วยงานสารสนเทศต้องมีเครื่องมือสำหรับตรวจสอบการใช้งานเครือข่ายภายในองค์กร เพื่อเฝ้าระวังและจัดการกับเหตุการณ์ผิดปกติที่อาจจะเกิดขึ้นกับเครือข่าย

5.3 นโยบายด้านคอมพิวเตอร์พกพาและการปฏิบัติงานจากระยะไกล (Notebook Device and Teleworking Policy)

วัตถุประสงค์และขอบเขต

เพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกล เช่น การรีโมท (Remote) เข้ามาทำงานที่เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ (Server) จากทั้งภายในและภายนอกองค์กร

เนื้อหานโยบายและการดำเนินการ

5.3.1 การปฏิบัติงานจากระยะไกล (Remote Working)

เป็นการสนับสนุนสำหรับการปฏิบัติงานจากสถานที่หนึ่งในระยะไกล ซึ่งจำเป็นต้องมีมาตรการเพื่อป้องกันข้อมูลที่มีการเข้าถึงการประมวลผลหรือการจัดเก็บจากสถานที่ดังกล่าว ดังนี้

1) มีการระบุอย่างชัดเจนว่าใครสามารถที่จะ Remote เข้ามาทำงานได้
2) กรณีที่ต้องให้หน่วยงานภายนอก Remote เข้ามาใช้งานผ่านเครือข่าย ต้องมีการเฝ้าดูการทำงานตลอดเวลา และมีการเปลี่ยนแปลง Password ในการเข้าใช้ของหน่วยงานภายนอกทุกครั้ง หรือมีการกำหนด Expired User/Password

6. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

6.1 นโยบายเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้มีการป้องกันทรัพย์สินและสารสนเทศขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

เนื้อหานโยบายและการดำเนินการ

6.1.1 ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

กำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินและสารสนเทศขององค์กรกับผู้ให้บริการภายนอก โดยต้องมีการกำหนดข้อตกลงร่วมกับผู้ให้บริการภายนอกที่เป็นลายลักษณ์อักษร และหน่วยงานที่มีหน้าที่ดูและระบบสารสนเทศจะต้องจัดเก็บสัญญาการให้บริการให้ครบถ้วน

6.2 นโยบายการบริหารจัดการผู้ให้บริการภายนอก (Supplier Service Delivery Management Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงให้บริการของผู้ให้บริการภายนอก เพื่อจัดทำและรักษาระดับความปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่ได้จัดทำไว้

เนื้อหานโยบายและการดำเนินการ

6.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and Review of Supplier Services) องค์กรต้องมีการติดตาม ทบทวนและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

1) ต้องมีการตรวจสอบการให้บริการจากหน่วยงานภายนอก ผู้ทำหน้าที่ตรวจสอบจำเป็นต้องมีความรู้ความเข้าใจในเรื่องความปลอดภัยสารสนเทศ ตลอดจนเงื่อนไขและข้อตกลงต่าง ๆ
2) ในกรณีที่มีเหตุการณ์ที่กระทบต่อความปลอดภัยโดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการ เพื่อรักษาความถูกต้องทางด้านหลักฐานและดำเนินการทางกฎหมายในกรณีที่จำเป็น
3) กำหนดให้มีการตรวจประเมินผู้ให้บริการภายนอกเป็นประจำทุกปี โดยประเมินตามแบบฟอร์มของหน่วยงานจัดซื้อจัดจ้าง

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

7. การควบคุมการเข้าถึง (Access Control)

7.1 นโยบายการควบคุมการเข้าถึงระบบ (System and Application Access Control Policy)

วัตถุประสงค์และขอบเขต

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต และป้องกันการใช้งานจากผู้ที่ไม่มีสิทธิเข้าใช้งานในระดับระบบปฏิบัติการ (Operating System) หน่วยงานด้านสารสนเทศควรกำหนดสิทธิผู้ใช้งานและการบริหารรหัสผ่านสำหรับผู้ใช้งาน รวมถึงควรควบคุมเวลาในการเชื่อมต่อสู่ระบบข้อมูล

เนื้อหานโยบายและการดำเนินการ

การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง ผู้ดูแลระบบต้องจัดการอนุญาตให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิเข้าใช้งาน ดังต่อไปนี้

1) ผู้ใช้ทุกคนต้องมีรหัสผู้ใช้ (User-ID) เฉพาะบุคคล เพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้ได้
2) ผู้ใช้ควรออกจากระบบเครือข่าย (Log-off) ทันทีเมื่อใช้งานเสร็จหรือไม่มีความจำเป็นต้องใช้งานอีก
3) ผู้ใช้ควรติดตั้งโปรแกรมถนอมหน้าจอ (Screen Saver) ที่มีรหัสผ่านบนเครื่องคอมพิวเตอร์
4) หากไม่มีการใช้งานเป็นเวลานานผู้ใช้ต้องปิดเครื่องคอมพิวเตอร์ให้เรียบร้อย

7.2 นโยบายบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management Policy)

วัตถุประสงค์และขอบเขต

เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาตโดยอาศัยแบบฟอร์มการขอเปิด แก้ไข/เปลี่ยนแปลง และปิดสิทธิ์ผู้ใช้งาน (IT-ACP-T0703) สำหรับควบคุมสิทธิในกระบวนการที่เกี่ยวข้องกับผู้ใช้งานระบบ เริ่มตั้งแต่การขอใช้สิทธิไปจนถึงการยกเลิกสิทธิในกรณีที่ผู้ใช้งานนั้นไม่มีความจำเป็นต้องใช้อีกต่อไป รวมไปถึงการควบคุมสิทธิของผู้ใช้ซึ่งมีสิทธิพิเศษที่สามารถแก้ไขสิทธิต่างๆ ของระบบได้

เนื้อหานโยบายและการดำเนินการ

7.2.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and Deregistration)

กระบวนการลงทะเบียน และถอดถอนสิทธิผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตามเพื่อเป็นการให้สิทธิการเข้าถึง ดังต่อไปนี้

1) พนักงานทุกคนที่มีสิทธิเข้าใช้งานระบบข้อมูลต้องมีรหัสผู้ใช้เฉพาะบุคคลในการเข้าสู่ระบบ
2) รหัสผู้ใช้เป็นรหัสเฉพาะบุคคล โดยไม่มีการใช้รหัสผู้ใช้ร่วมกัน (Shared User ID) ในกรณีที่พนักงานลาออก รหัสผู้ใช้รายนั้นต้องไม่ถูกนำกลับมาใช้ใหม่
3) ในการร้องขอเพื่อเข้าใช้งานระบบใดๆ ผู้บังคับบัญชาสูงสุดในสายงานต้องทำการพิจารณาเพื่ออนุมัติเห็นชอบ
4) หน่วยงานสารสนเทศ ต้องดำเนินการร่วมกันกับหน่วยงานที่เกี่ยวข้องในการถอดถอนสิทธิของผู้ใช้ ที่ไม่มีความต้องการใช้ระบบอีกต่อไปโดยทันที

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

7.2.2 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

หน่วยงานสารสนเทศ ต้องมีการทบทวนสิทธิการเข้าถึงข้อมูลสารสนเทศร่วมกับหน่วยงานที่เกี่ยวข้อง อย่างน้อยปีละ 1 ครั้ง

7.3 นโยบายหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities Policy)

วัตถุประสงค์และขอบเขต

เพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต และมุ่งเน้นให้ผู้ใช้งานระบบสารสนเทศตระหนักถึงความปลอดภัยในการใช้งานระบบ โดยผู้ใช้ต้องให้ความร่วมมือด้านการใช้รหัสผ่านและต้องทราบถึงวิธีปฏิบัติเมื่อเสร็จภารกิจในการใช้งานระบบและอุปกรณ์

เนื้อหานโยบายและการดำเนินการ

การพิสูจน์ตัวตนและการใช้ข้อมูลซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information) ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูล การพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ ดังต่อไปนี้

1) รหัสผ่านสำหรับการเข้าสู่ระบบถือเป็นความลับ โดยผู้ใช้ต้องไม่แบ่งปันหรือเปิดเผยรหัสของตนให้บุคคลอื่นโดยเด็ดขาด
2) ผู้ใช้ควรกำหนดและใช้รหัสผ่านที่มีประกอบด้วยตัวเลข สัญลักษณ์และตัวอักษรรวมกันมากกว่า 6 ตัวอักษร
3) ผู้ใช้ควรเปลี่ยนรหัสผ่านของตนเองเป็นประจำทุกๆ 90 วัน ไม่ว่าจะมีการบังคับให้เปลี่ยนรหัสผ่านจากระบบหรือไม่ก็ตาม และผู้ใช้ควรไม่ตั้งรหัสผ่านซ้ำกับของเดิม
4) ผู้ใช้ต้องตรวจสอบว่าสิทธิที่ตนได้รับ ในการเข้าใช้ระบบเหมาะสมกับหน้าที่ที่ตนรับผิดชอบหรือไม่ ถ้าพบว่าสิทธิที่ได้รับไม่เหมาะสม ต้องแจ้งผู้บังคับบัญชาให้รับทราบเพื่อพิจารณาและปรับเปลี่ยนให้เกิดความเหมาะสมที่สุด

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

8. ความมั่นคงปลอดภัยด้านบุคลากร (Human Resources Security)

8.1 นโยบายความมั่นคงปลอดภัยด้านบุคลากร (Human Resources Security Policy)

วัตถุประสงค์และขอบเขต

เพื่อเป็นแนวทางการรักษาความปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการทรัพยากรบุคคล ให้รับทราบและเข้าใจข้อปฏิบัติการใช้สารสนเทศขององค์กรที่ถูกต้องเหมาะสม

เนื้อหานโยบายและการดำเนินการ

8.1.1 การสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

หน่วยงานสารสนเทศและหน่วยงานที่เกี่ยวข้อง ควรจัดให้พนักงานเข้ารับฟังการอบรมให้ตระหนักถึงความปลอดภัยสารสนเทศ อย่างน้อยปีละ 1 ครั้ง เพื่อรับทราบถึงนโยบายความปลอดภัยเพิ่มเติมขององค์กร เหตุการณ์ละเมิดความปลอดภัยและกรณีศึกษาใหม่ๆ ในขณะที่หน่วยงานด้านเทคโนโลยีสารสนเทศควรจะได้รับการฝึกอบรมจากหน่วยงานภายนอกอย่างน้อยปีละ 1 ครั้ง

8.1.2 กระบวนการทางวินัย (Disciplinary Process)

กระบวนการทางวินัยต้องกำหนดอย่างเป็นทางการ พนักงานทุกคนที่ใช้ข้อมูลสารสนเทศขององค์กรต้องลงลายมือชื่อรับทราบระเบียบว่าด้วยการใช้ระบบสารสนเทศขององค์กรอย่างปลอดภัย (IT-RIO-T0101) ในแบบฟอร์มใบรับและคืนทรัพย์สินสารสนเทศ/รับทราบเงื่อนไขการใช้งานระบบสารสนเทศ (IT-ARRF-03003) ซึ่งองค์กรต้องกำหนดระเบียบปฏิบัติและบทลงโทษสำหรับพนักงานที่ละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ

8.1.3 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

หน่วยงานสารสนเทศ ต้องติดตามและประสานงานหลังจากได้รับแจ้งจากแผนกทรัพยากรบุคคล เมื่อมีพนักงานสิ้นสุดสภาพการเป็นพนักงาน หรือเมื่อมีการเปลี่ยนตำแหน่งหรือสถานะการจ้างงาน ดังนี้

1) หน่วยงานทรัพยากรบุคคล แจ้งให้หน่วยงานสารสนเทศทราบทันทีที่มีการโอนย้าย ลาออก หรือพ้นสภาพการเป็นพนักงานขององค์กร เพื่อทำการถอดถอนสิทธิการเข้าใช้ระบบงานต่างๆ
2) หน่วยงานสารสนเทศ ปฏิบัติตามหัวข้อแบบสำรวจคืนทรัพย์สิน (IT-ARF-T0302) หรือแบบฟอร์มของหน่วยงานทรัพยากรบุคคล โดยทำการตรวจสอบทรัพย์สินของพนักงานและรายงานผลการตรวจสอบกลับมายังหน่วยงานทรัพยากรบุคคล

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

9. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

9.1 นโยบายการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ควรกำหนดหน้าที่ความรับผิดชอบ และกระบวนการด้านการจัดการและปฏิบัติงานของระบบที่ชัดเจน ซึ่งหน้าที่ความรับผิดชอบที่กำหนดนี้ควรพิจารณาถึงการแบ่งแยกหน้าที่อย่างเหมาะสม นอกจากกระบวนการทำงานปกติแล้วควรมีการกำหนดขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์กระทบความปลอดภัยเพื่อรองรับกับเหตุการณ์ดังกล่าว

เนื้อหานโยบายและการดำเนินการ

9.1.1 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

การใช้ทรัพยากรของระบบต้องมีการปรับปรุงเพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ หน่วยงานสารสนเทศต้องจัดทำแผนงบประมาณ เพื่อทำให้มีการจัดเตรียมคอมพิวเตอร์ ซอฟต์แวร์และอุปกรณ์ต่างๆ ที่คอยสนับสนุนการทำงานของหน่วยงานภายในองค์กร

9.2 นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี และเพื่อควบคุมป้องกันซอฟต์แวร์และข้อมูลสารสนเทศของบริษัทไม่ให้เกิดความเสียหาย

เนื้อหานโยบายและการดำเนินการ

9.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Protect against Malware)

มาตรการป้องกันและการตรวจหาจากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการที่เหมาะสม ดังนี้

1) หน่วยงานสารสนเทศ ต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ที่มีความน่าเชื่อถือในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ทุกเครื่อง และเครื่องเซิร์ฟเวอร์ (Server) โดยมีการ Update ให้ทันสมัยอยู่ตลอดเวลา
2) หน่วยงานสารสนเทศ ต้องกำหนดให้โปรแกรมป้องกันไวรัส (Antivirus) ทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะการใช้ระบบด้วย
3) ไฟล์ที่แนบมากับอีเมลหรือจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตต้องมีการตรวจหาไวรัส (Virus) ก่อนนำไปใช้งาน
4) ห้ามพนักงานดำเนินการใดๆ ที่เกี่ยวกับการพัฒนาไวรัส (Virus) ซอฟต์แวร์ที่เป็นอันตรายหรือเก็บไว้เป็นเจ้าของ กรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกที่อนุญาตให้นำมาใช้ ผู้ใช้ต้องตรวจสอบไวรัส (Virus) ก่อนใช้งานทุกครั้ง

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

9.3 นโยบายการสำรองข้อมูล (Data Backup Policy)

วัตถุประสงค์และขอบเขต

เพื่อป้องกันการสูญหายของข้อมูล และเพื่อให้ข้อมูลสารสนเทศถูกต้องสมบูรณ์พร้อมใช้งานเสมอ

เนื้อหานโยบายและการดำเนินการ

9.3.1 การสำรองข้อมูล (Data Backup)

ข้อมูลสำหรับสารสนเทศต้องมีการดำเนินการสำรองไว้ และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอ ดังนี้

1) มีการจัดเตรียมแผนในการสำรองข้อมูล และมีการปรับปรุงทบทวนแผนทุกปี
2) มีการจัดทำคู่มือในการสำรองข้อมูลและการกู้คืนข้อมูล
3) หน่วยงานสารสนเทศทำตรวจสอบการสำรองข้อมูลในระบบทุกวันว่ามีสถานะเป็นอย่างไร พร้อมทั้งบันทึกรายละเอียดการสำรองข้อมูลลงในแบบฟอร์มที่กำหนด
4) หน่วยงานสารสนเทศควรทำการทดสอบกู้ข้อมูลสำรองระบบงานหลัก อย่างน้อยปีละ 1 ครั้ง โดยทดสอบตามแผนการกู้คืน
5) คอมพิวเตอร์ส่วนบุคคลที่พนักงานเบิกใช้งาน ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลไฟล์ที่สำคัญและมีมาตรการห้ามนำข้อมูลที่เป็นความลับของบริษัทไปเผยแพร่ มิฉะนั้นจะมีบทลงโทษตามกฎระเบียบของบริษัท

9.4 นโยบายการบันทึกข้อมูลจราจรสารสนเทศและการเฝ้าระวัง (Logging and Monitoring Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐานการใช้สารสนเทศขององค์กร

เนื้อหานโยบายและการดำเนินการ

9.4.1 การบันทึกข้อมูลจราจรสารสนเทศ (Logging)

ข้อมูลจราจรสารสนเทศ (Log) แสดงเหตุการณ์ซึ่งบันทึกกิจกรรมของผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบและเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึก จัดเก็บและทบทวนอย่างสม่ำเสมอ อุปกรณ์บันทึกข้อมูลจราจรสารสนเทศ (Log) ต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต

9.5 นโยบายการควบคุมการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ (Control of Operational Software Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้ระบบให้ปฏิบัติการมีการทำงานที่ถูกต้องและเป็นไปในทิศทางที่บริษัทกำหนด

เนื้อหานโยบาย และการดำเนินการ

9.5.1 การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ (Installation of Software on Operational Systems)

ซอฟต์แวร์บนคอมพิวเตอร์ทุกเครื่อง จะต้องถูกติดตั้งหรืออยู่ในการควบคุมโดยหน่วยงานสารสนเทศเท่านั้น

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

9.6 นโยบายการบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management Policy)

วัตถุประสงค์และขอบเขต

เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค และป้องกันข้อผิดพลาดต่างๆ ที่อาจจะเกิดขึ้น

เนื้อหานโยบายและการดำเนินการ

9.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิค จุดอ่อนต่อช่องโหว่ระบบสารสนเทศขององค์กร ควรมีการเก็บรวบรวมเพื่อประเมินและเตรียมมาตรการที่เหมาะสมเพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง หน่วยงานสารสนเทศควรรายงานผู้บริหารเมื่อพบช่องโหว่ทางด้านเทคนิคพร้อมเสนอแนวทางแก้ไขและป้องกัน

10. การจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information management for Business Continuity Plan)

10.1 นโยบายความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity Policy)

วัตถุประสงค์และขอบเขต

เพื่อป้องกันและรับมือกับความเสี่ยงต่อการหยุดชะงักของระบบสารสนเทศต่อการดำเนินธุรกิจขององค์กร อันเนื่องมาจากภัยคุกคามต่อการทำงานของระบบ ไม่ว่าจะด้วยการโจมตีด้านเครือข่าย อุบัติเหตุ ภัยธรรมชาติหรือจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ล่วงหน้า ซึ่งก่อให้เกิดความเสียหายต่อองค์กร

ดังนั้นจึงควรจัดทำแผนบริหารจัดการความต่อเนื่อง ในการดำเนินธุรกิจเพื่อลดความรุนแรงของผลกระทบจากเหตุการณ์ดังกล่าวให้อยู่ในระดับที่ยอมรับได้ และเพื่อให้สามารถดำเนินธุรกิจหลักขององค์กรต่อไปได้

เนื้อหานโยบายและการดำเนินการ

10.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity)

องค์กรต้องกำหนดหัวข้อด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสภาพการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดภัยพิบัติ โรคระบาดฯ เพื่อคงไว้ซึ่งความต่อเนื่องทางธุรกิจ ดังต่อไปนี้

1) การวิเคราะห์และการประเมินความเสี่ยงที่กระทบต่อการดำเนินธุรกิจขององค์กร
2) การจัดทำกลยุทธ์เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ โดยต้องมีความสอดคล้องกับเป้าหมายทางธุรกิจขององค์กร
3) การฝึกอบรมพนักงาน เพื่อให้ตระหนักถึงความมั่นคงปลอดภัยและเข้าใจในแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมทั้งสามารถปฏิบัติตามได้อย่างถูกต้อง
4) กำหนดหน้าที่ความรับผิดชอบในการประสานงาน การพัฒนาและการทบทวนปรับปรุงแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศประจำปี

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

10.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity)

องค์กรต้องมีการกำหนด คู่มือการบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (IT-BCP-T1001) และมีการทบทวนปรับปรุงกระบวนการ เพื่อให้เกิดความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศตามที่กำหนดไว้ เมื่อมีสถานการณ์ความเสียหายอย่างใดอย่างหนึ่งเกิดขึ้น ดังนี้

1) ควรมีการสื่อสารไปยังพนักงานทุกคน เพื่อทราบถึงแผนการดำเนินการเมื่อเกิดเหตุฉุกเฉิน
2) ควรมีการทดสอบและซักซ้อมแผนตามระยะเวลาที่กำหนด
3) หน่วยงานสารสนเทศต้องกำกับดูแลในการนำแผนงานไปใช้

10.1.3 การตรวจสอบ การทบทวนและการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review and Evaluate Information Security Continuity)

องค์กรต้องมีการตรวจสอบมาตรการบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นมีความถูกต้องและครบถ้วน

10.2 นโยบายการเตรียมการอุปกรณ์ประมวลผลสำรอง (Backup Processing Device Policy)

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศสำหรับกรณีฉุกเฉิน

<u>เนื้อหานโยบายและการดำเนินการ</u>

10.2.1 สภาพพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้กรณีอุปกรณ์ประมวลผลหลักได้รับความเสียหาย

11. การจัดหา การพัฒนาและการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

11.1 นโยบายความมั่นคงปลอดภัยของระบบสารสนเทศ (Security Requirements of Information Systems Policy)

<u>วัตถุประสงค์และขอบเขต</u>

เพื่อให้ความมั่นคงปลอดภัยของระบบสารสนเทศเป็นองค์ประกอบสำคัญขององค์กร และทำให้มั่นใจได้ว่าการพัฒนาระบบงานมีการคำนึงถึงความปลอดภัยและมีกระบวนการควบคุมที่เพียงพอ องค์กรต้องมีการกำหนดให้มีการพิจารณาถึงความต้องการด้านความปลอดภัยของระบบงาน ก่อนที่จะมีการพัฒนาระบบงาน

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

เนื้อหานโยบายและการดำเนินการ

11.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

ความมั่นคงปลอดภัยสารสนเทศ ต้องครอบคลุมถึงการพัฒนาระบบใหม่หรือการปรับปรุงระบบเดิมที่มีอยู่แล้ว ดังนี้

1) องค์กรต้องร่วมกันวิเคราะห์และกำหนดความต้องการด้านความปลอดภัยสารสนเทศ ก่อนที่จะทำการพัฒนาหรือจัดหาระบบงาน ซึ่งถือเป็นส่วนหนึ่งของการพัฒนาหรือจัดหาระบบงาน
2) ความต้องการที่เกิดขึ้นต้องได้รับการอนุมัติจากผู้มีสิทธิ์อนุมัติของหน่วยงานที่ร้องขอ ก่อนส่งมายังหน่วยงานสารสนเทศเพื่อวิเคราะห์ความเป็นไปได้ในการพัฒนาหรือเปลี่ยนแปลงระบบและนำเสนอผู้บริหารเพื่อพิจารณาต่อไป

11.2 นโยบายสำหรับกระบวนการพัฒนาและสนับสนุน (Development and Support Processes Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบและดำเนินการพัฒนาอย่างเป็นระบบ

เนื้อหานโยบายและการดำเนินการ

11.2.1 ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)

การเปลี่ยนแปลงระบบ ต้องมีการควบคุมโดยหน่วยงานสารสนเทศ และจะต้องทำการระบุขั้นตอนการเปลี่ยนแปลงอย่างชัดเจน

11.2.2 การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)

แผนการทดสอบและเกณฑ์การทดสอบที่เกี่ยวข้องเพื่อรองรับระบบ ต้องมีการจัดทำเพื่อรองรับระบบที่ปรับปรุงจากระบบเดิมและระบบใหม่ ดังนี้

1) กำหนดให้มีการตรวจสอบความถูกต้องของผลลัพธ์ข้อมูลที่ได้จากระบบคอมพิวเตอร์ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องสมบูรณ์
2) ผู้ร้องขอจะต้องเป็นผู้ทดสอบและตรวจรับระบบงาน

11.3 นโยบายสำหรับการทดสอบข้อมูล (Test Data Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้มีการป้องกันข้อมูลสำหรับการทดสอบ กับข้อมูลที่นำมาใช้จริงออกจากกัน

เนื้อหานโยบายและการดำเนินการ

11.3.1 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments)

สภาพแวดล้อมสำหรับการพัฒนา การทดสอบและการให้บริการต้องมีการจัดทำแยกกันเพื่อลดความเสี่ยงของการเข้าถึงข้อมูลหรือการเปลี่ยนแปลงสำหรับการให้บริการโดยไม่ได้รับอนุญาต

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

1) ในการพัฒนาระบบต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับระบบที่ใช้ในการพัฒนา (Development System) และระบบที่ใช้งานจริง (Production System)
2) ควรมีระเบียบปฏิบัติที่ชัดเจนในการโอนย้ายโปรแกรมที่พัฒนาเสร็จแล้วไปยังระบบที่ใช้งานจริง

12. โครงสร้างความปลอดภัยสารสนเทศ (Organization of Information Security)

12.1 นโยบายโครงสร้างภายในองค์กร (Internal Organization Policy)

วัตถุประสงค์และขอบเขต

เพื่อให้การจัดการความปลอดภัยสารสนเทศเป็นไปอย่างมีระบบและมีความชัดเจนตั้งแต่ระดับบริหารจนถึงระดับปฏิบัติการ องค์กรจึงต้องจัดทำโครงสร้างความปลอดภัยสารสนเทศรวมถึงการกำหนดบทบาทและหน้าที่ในการบริหารจัดการความปลอดภัยของสารสนเทศภายในองค์กร

เนื้อหานโยบายและการดำเนินการ

12.1.1 กำหนดบทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

ผู้บริหารควรให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความปลอดภัยสารสนเทศ โดยอนุมัติให้มีการจัดตั้งโครงสร้างบุคคลากรด้านความปลอดภัยสารสนเทศ โดยอ้างอิงตามผังโครงสร้างองค์กร

12.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

- ประธานเจ้าหน้าที่บริหาร อนุมัตินโยบายต่างๆ ด้านสารสนเทศและอนุมัติโครงการที่เกี่ยวข้องกับสารสนเทศ
- รองประธานเจ้าหน้าที่บริหาร หรือ ผู้มีอำนาจอนุมัติในสายงานไอที.ตามผังโครงสร้างองค์กร อนุมัติเห็นชอบนโยบายต่างๆ ด้านสารสนเทศและอนุมัติเห็นชอบโครงการที่เกี่ยวข้องกับสารสนเทศตามอำนาจอนุมัติ
- แผนกเทคโนโลยีสารสนเทศ จัดตั้งขึ้นเพื่อป้องกันความเสียหายระบบสารสนเทศขององค์กรอันเกิดจากภัยคุกคามด้านสารสนเทศ เพื่อให้เกิดความปลอดภัยในระดับที่สอดคล้องกับเป้าหมายทางธุรกิจขององค์กร

12.2 นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)

วัตถุประสงค์และขอบเขต

เพื่อกำหนดเกณฑ์ในการจัดลำดับชั้นความลับของข้อมูลและเพื่อให้ข้อมูลได้รับการป้องกันอย่างเหมาะสมตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น

เนื้อหานโยบายและการดำเนินการ

12.2.1 ชั้นความลับของสารสนเทศ (Information Classification)

สารสนเทศต้องมีการจัดชั้นความลับโดยพิจารณาจากด้านกฎหมาย คุณค่าและระดับความสำคัญ หากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต หน่วยงานสารสนเทศต้องจัดทำเอกสารแสดงขั้นความลับสารสนเทศ (IT-CI-T1201) เพื่อให้หน่วยงานต่างๆ ลงทะเบียนรับทราบตามลำดับชั้นที่กำหนดไว้ ดังนี้

1) ชั้นที่ 1 ข้อมูลเปิดเผยได้
ข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501

2) ชั้นที่ 2 ข้อมูลใช้ภายในองค์กรเท่านั้น

เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่าสามารถเปิดเผยให้พนักงานทุกคนภายในองค์กรทราบได้ แต่ไม่สามารถเปิดเผยต่อบุคคลภายนอกองค์กรได้เพราะอาจสร้างความเสียหายให้กับองค์กร

3) ชั้นที่ 3 ข้อมูลลับ

เป็นข้อมูลภายในองค์กรที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้พนักงานทุกคนได้ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ควรทราบ

4) ชั้นที่ 4 ข้อมูลลับมาก

เป็นข้อมูลใช้ภายในองค์กรแต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้ใช้บางกลุ่มขององค์กร ส่วนใหญ่เป็นผู้บริหารเท่านั้น และไม่สามารถเปิดเผยต่อบุคคลภายนอกได้เนื่องจากข้อมูลประเภทนี้มีความจำเป็นต่อการปฏิบัติงานขององค์กรและจะเป็นประโยชน์ในเชิงการค้าต่อคู่แข่งหรือทำให้เกิดผลเสียหายต่อองค์กรหากมีการรั่วไหลของข้อมูล

5) ชั้นที่ 5 ข้อมูลลับที่สุด

ข้อมูลใช้ภายในองค์กรแต่เป็นข้อมูลลับ ซึ่งใช้งานโดยผู้บริหารระดับสูงขององค์กรเท่านั้นและเป็นการใช้เพื่อการวินิจฉัยและตัดสินใจที่สำคัญขององค์กรไม่สามารถเปิดเผยต่อบุคคลภายนอกได้เลย เนื่องจากข้อมูลประเภทนี้มีความจำเป็นต่อการปฏิบัติงานขององค์กร จะเป็นประโยชน์ในเชิงการค้าต่อคู่แข่งหรือทำให้เกิดผลเสียหายร้ายแรงต่อองค์กร การนำข้อมูลในชั้นนี้ไปเปิดเผยต่อบุคคลภายนอกไม่สามารถทำได้เว้นแต่มีการบังคับตามกฎหมาย

โดยให้มีผลตั้งแต่วันที่ 27 กุมภาพันธ์ 2567 เป็นต้นไป ตามมติที่ประชุมคณะกรรมการบริษัท : ครั้งที่ 1/2567

PSG Corporation Public Company Limited I 11/1 AIA Sathorn Tower, 21st Floor, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 I Tel. 02 018 7190 - 8 I Fax. 02 018 7199
บริษัท พีเอสจี คอร์ปอเรชั่น จำกัด (มหาชน) I 11/1 อาคารเอไอเอ สาทร ทาวเวอร์ ชั้น 21 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 I www.psgcorp.co.th I TAX ID 0107548000501