บมจ.ภัทรลิสซิ่ง
PHATRA LEASING PLC.

252/6 29th Fl., Muang Thai Phatra Complex1,
Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th

Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

ประกาศ
นโยบายการรักษาความปลอดภัยระบบสารสนเทศ
(Information Technology Security Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานระบบสารสนเทศของ บริษัท ภัทรลิสซิ่ง จำกัด (มหาชน) ได้รับทราบถึงข้อปฏิบัติและข้อห้ามมิให้ปฏิบัติของผู้ใช้ระบบสารสนเทศ รวมถึงข้อปฏิบัติของผู้พัฒนาระบบสารสนเทศ และผู้ดูแลระบบสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบสารสนเทศ และให้การใช้ระบบสารสนเทศสอดคล้องตามบทบัญญัติของกฎหมาย และตรงตามวัตถุประสงค์ของบริษัท รวมถึงไม่กระทำการใดๆ ตามที่กฎหมายได้บัญญัติให้เป็นความผิด จึงได้จัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศนี้ขึ้นมา เพื่อให้ผู้ใช้ระบบสารสนเทศของบริษัทยึดถือเป็นแนวทางการใช้งานอย่างเคร่งครัด

2. ขอบเขตของประกาศ

นโยบายความมั่นคงปลอดภัยสำหรับระบบสารสนเทศนี้ ให้มีผลบังคับใช้กับผู้ใช้งานระบบสารสนเทศ ผู้พัฒนาระบบสารสนเทศ และผู้ดูแลระบบสารสนเทศ ของ “บริษัท ภัทรลิสซิ่ง จำกัด (มหาชน)” รวมถึงผู้ใช้งานที่เชื่อมต่อเข้ากับระบบอินเทอร์เน็ต โดยผ่านทางเครือข่ายของ บริษัท ภัทรลิสซิ่ง จำกัด (มหาชน) ทุกคน โดยไม่มียกเว้น

3. หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principle)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ในการธำรงไว้ซึ่งความลับ (Confidential) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิดและความน่าเชื่อถือ

4. คำจำกัดความ

4.1. **บริษัท (Company)** หมายถึง บริษัท ภัทรลิสซิ่ง จำกัด (มหาชน)

4.2. **หน่วยงานเทคโนโลยีสารสนเทศ** หมายถึง หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการระบบสารสนเทศของบริษัท ได้แก่ ฝ่ายพัฒนาเทคโนโลยีสารสนเทศ

4.3. **พนักงาน (Employee)** หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท

4.4. **ผู้ใช้งาน (User)** หมายถึง พนักงานของบริษัท รวมไปถึงบุคคลภายนอกบริษัทที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของบริษัท

4.5. **ผู้บังคับบัญชา** หมายถึงพนักงานซึ่งเป็นผู้บังคับบัญชาของหน่วยงานภายในตามโครงสร้างองค์กรของบริษัท

4.6. **ผู้มีอำนาจอนุมัติ** หมายถึง พนักงาน หรือผู้บริหารที่ได้รับมอบหมายให้มีอำนาจในการอนุมัติ เช่น กรรมการผู้จัดการ (MD) ผู้บริหารฝ่าย

4.7. **ระบบสารสนเทศ (Information System)** หมายถึง ระบบคอมพิวเตอร์ ระบบเครือข่ายติดต่อสื่อสาร ระบบเครือข่ายเชื่อมต่อเข้าระบบอินเทอร์เน็ต ระบบเก็บข้อมูล ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบสื่อสารข้อมูลทุกประเภท ข้อมูลอุปกรณ์สื่อสาร อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง หรืออุปกรณ์ใดๆ ที่เกี่ยวข้อง ที่เป็นกรรมสิทธิ์ของบริษัท ภัทรลิสซิ่ง จำกัด (มหาชน) และ/หรือที่ บริษัท ภัทรลิสซิ่ง จำกัด (มหาชน) ได้รับอนุญาตให้ใช้ได้ตามกฎหมาย

4.8. **ข้อมูล (Information)** หมายถึง ข้อความ ข่าวสาร ภาพ เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านกระบวนการใดๆ ทั้งที่อยู่ในรูปแบบอิเล็กทรอนิกส์ หรือที่อยู่ในรูปสื่อสิ่งพิมพ์

4.9. **ข้อมูลสำคัญ** หรือ **ข้อมูลที่เป็นความลับ (Sensitive Information)** หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัท มีพันธะผูกพันตาม ข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัทไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การ

252/6 29th Fl., Muang Thai Phatra Complex1,
Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

รั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง

4.10. **เจ้าของข้อมูล (Information Owner)** หมายถึง บุคคลหรือหน่วยงานภายในองค์กรที่ได้รับมอบหมายหรือมีหน้าที่รับผิดชอบในการจัดการและควบคุมข้อมูลสารสนเทศภายใต้ความดูแลของตน โดยมีอำนาจในการกำหนดสิทธิ์การเข้าถึงข้อมูล การใช้งาน การแบ่งปัน การเก็บรักษา และการทำลายข้อมูล รวมถึงการรับรองว่าข้อมูลนั้นได้รับการป้องกันและบริหารจัดการตามนโยบายของบริษัท และกฎหมายที่เกี่ยวข้องอย่างเหมาะสม

4.11. **Remote Access** หมายถึง การเข้าสู่ระบบสารสนเทศของบริษัทจากระยะไกล รวมถึงการเชื่อมต่อ VPN (Virtual Private Network)

4.12. **ผู้ดูแลระบบ (Administrator)** หมายถึง เจ้าหน้าที่ของบริษัท หรือผู้ได้รับการว่าจ้าง ซึ่งทำหน้าที่ดูแล และรักษาความปลอดภัยของระบบสารสนเทศ และเครือข่ายของบริษัท โดยเป็นผู้มีสิทธิเข้าถึงระบบสารสนเทศหลักของบริษัท

4.13. **ผู้พัฒนาระบบ (Developer)** หมายถึง เจ้าหน้าที่ของบริษัท หรือผู้ได้รับการว่าจ้าง ซึ่งทำหน้าที่รับผิดชอบในการพัฒนาโปรแกรม การใช้งาน และระบบสารสนเทศของบริษัท

4.14. **การรักษาความมั่นคงปลอดภัย** หรือ **ความมั่นคงปลอดภัย (Security)** หมายถึงกระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบสารสนเทศ และข้อมูลสารสนเทศที่เป็นระบบ และข้อมูลสำคัญ ให้พ้นจากความพยายามใดๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจของบริษัท ได้รับความเสียหาย

4.15. **บุคคลภายนอก (External Party)** หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ เช่น

- บริษัทคู่ค้า (Business Partner)
- ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource)
- ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier)
- ผู้ให้บริการต่างๆ (Service Provider)
- ที่ปรึกษา (Consultant)

4.16. **เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident)** หมายถึง เหตุการณ์ที่ส่งผลกระทบต่อการทำงานของระบบ หรือบริการสารสนเทศ เช่น ระบบล่ม ข้อมูลรั่วไหล การโจมตีทางไซเบอร์ หรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งต้องแก้ไขเพื่อคืนค่าการทำงานในทันที

4.17. **ปัญหาด้านระบบสารสนเทศ (IT Problem)** หมายถึง สาเหตุที่แท้จริงของเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งต้องได้รับการวิเคราะห์ และพิจารณาแนวทางแก้ไขเพื่อป้องกันการเกิดซ้ำในอนาคต

5. **ปัญญาประดิษฐ์ (AI: Artificial Intelligent)** หมายถึง เทคโนโลยีที่สามารถเรียนรู้ วิเคราะห์ และดำเนินการตามข้อมูลที่ได้รับ เช่น การวิเคราะห์ข้อมูลเชิงลึก การสร้างเนื้อหา หรือการให้คำแนะนำการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ (IT Security)

5.1. การบริหารจัดการทรัพย์สินด้านระบบสารสนเทศ (IT Asset Management)

5.1.1. ต้องจัดทำและเก็บทะเบียนทรัพย์สิน ซึ่งรวมถึงทรัพย์สินข้อมูล และเอกสาร (Information and Document Asset) ทรัพย์สินซอฟต์แวร์ (Software Asset) ทรัพย์สินอุปกรณ์ (Hardware Asset) ทรัพย์สินงานบริการ (Service Asset) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อทรัพย์สินอย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการทรัพย์สินให้สอดคล้องกับการดำเนินงานของบริษัท

5.1.2. ต้องมีการตรวจสอบทรัพย์สิน (Inventory Check) อย่างน้อยปีละ 1 ครั้ง หรือตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

252/6 29th Fl., Muang Thai Phatra Complex1, Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

5.1.3. การอนุญาตให้ใช้ทรัพย์สิน (Acceptable Use for Assets) จะต้องบันทึกเป็นเอกสาร และมีข้อบังคับการอนุญาตให้ใช้ข้อมูลและทรัพย์สินอย่างเหมาะสม

5.2. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

5.2.1. มีการตรวจสอบคุณสมบัติของผู้สมัครเข้าทำงาน เช่นตรวจสอบจากประวัติการทำงาน วุฒิการศึกษา จดหมายรับรอง หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และต้องจัดให้ผู้ใช้งานมีการลงนาม “ใบลงนามรับทราบ และยึดปฏิบัติ” (เอกสารแนบท้าย)

5.2.2. จัดอบรมให้ความรู้แก่ผู้ใช้งานทุกคนเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยด้านระบบสารสนเทศ มีการบันทึกข้อมูลการฝึกอบรมของบุคลากรทางด้านความมั่นคงปลอดภัย

5.2.3. ต้องมีการกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎและแนวปฏิบัติของบริษัท หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิด ที่ได้กระทำ และเป็นไปตามระเบียบบริษัท

5.2.4. สายงานบริหารทรัพยากรบุคคลและหน่วยงานต้นสังกัดของผู้ใช้งาน ต้องแจ้งให้หน่วยงานที่ เกี่ยวข้องทราบ เมื่อมีการลาออก แต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อทำการปรับปรุง ระงับยกเลิกบัญชีผู้ใช้ และยกเลิกสิทธิ์ในการเข้าถึงระบบและข้อมูล

5.3. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

5.3.1. ผู้ดูแลระบบมีหน้าที่ดูแลความปลอดภัยของห้องศูนย์คอมพิวเตอร์ (Datacenter room) ให้ดำเนินการได้อย่างต่อเนื่อง

5.3.2. มีการแยกห้องศูนย์คอมพิวเตอร์ออกจากสถานที่ทำงานทั่วไป และกั้นเป็นห้องต่างหาก มีการควบคุมการเข้า-ออกพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยให้เข้า-ออกได้

5.3.3. มีระบบไฟฟ้าสำรองภายในห้องศูนย์คอมพิวเตอร์เพื่อให้สามารถทำงานได้ตลอดเวลา และต้องมีการตรวจสอบระบบไฟฟ้าสำรองอย่างน้อยปีละ 2 ครั้ง เพื่อเป็นการลดความเสียหายที่อาจจะเกิดขึ้น

5.3.4. การเดินสายเคเบิลต่าง ๆ ต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการเดินสายนั้นต้องติดป้ายกำกับให้รู้ต้นทางปลายทางของสาย

5.3.5. ต้องบำรุงรักษาระบบสารสนเทศ ระบบเครือข่าย และเครื่องแม่ข่ายอย่างสม่ำเสมอหรือตามรอบระยะเวลาที่แนะนำโดยผู้ผลิตผู้ใช้งานต้องป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่เพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น

5.3.6. ควรกำหนดวิธีการกำจัดสื่อบันทึกข้อมูลที่มีข้อมูลของบริษัทอย่างเป็นลายลักษณ์อักษร เช่น การเผา ตัด หั่น หรือทำลายเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

5.4. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านระบบสารสนเทศ (IT Operations Security)

5.4.1. ต้องจัดทำคู่มือ และ/หรือ ขั้นตอนการปฏิบัติงานระบบสารสนเทศในหน่วยงาน เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติ และเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ โดยคู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง

5.4.2. ต้องมีการแบ่งแยกสภาพแวดล้อมของการพัฒนาระบบ (Development Environment) การทดสอบระบบ (Testing Environment) และระบบใช้งานจริง (Production Environment) ให้ปลอดภัยและถูกต้อง

5.4.3. ก่อนการตรวจรับระบบใหม่ควรกำหนดเกณฑ์การยอมรับอย่างชัดเจน (Acceptance Criteria) และดำเนินการทดสอบการยอมรับของผู้ใช้งาน (User Acceptance Testing - UAT)

การบริหารจัดการการตั้งค่าระบบ (System Configuration Management)

5.4.4. มีการตั้งค่าระบบที่มีความปลอดภัยของระบบงาน และอุปกรณ์เครือข่ายสื่อสารต่างๆ มีการสอบทานการตั้งค่าตามรอบระยะเวลา เพื่อให้สอดคล้องตามมาตรฐานของบริษัท

252/6 29th Fl., Muang Thai Phatra Complex1,
Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

5.4.5. การเปลี่ยนแปลงการตั้งค่าบนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการ การเปลี่ยนแปลงที่บริษัทกำหนด มีการสำรองการตั้งค่าของระบบทุกครั้งก่อนการดำเนินการเปลี่ยนแปลง เพื่อป้องกันความเสี่ยง หรือข้อผิดพลาดในการปฏิบัติงาน

5.4.6. ติดตั้งโปรแกรมรักษาความปลอดภัย Anti-Virus / Anti-malware โดยมีการปรับปรุงประสิทธิภาพของ การป้องกันโปรแกรมไม่ประสงค์ดี (Malware) สำหรับเครื่องแม่ข่ายให้เพียงพอและ เป็นปัจจุบัน เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ๆ

การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging)

5.4.7. มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารที่สำคัญด้วย วิธีการที่ปลอดภัย กำหนดให้บันทึกกิจกรรมการใช้งานของผู้ใช้งาน การให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด

5.4.8. มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารให้ตรงกับ เครื่องแม่ข่าย Network Time Protocol : NTP (clock synchronization) เพื่อให้ค่าเวลาในการบันทึก เหตุการณ์มีความถูกต้องในลักษณะ real-time ซึ่งเครื่องแม่ข่าย NTP ต้องรับสัญญาณนาฬิกาจากแหล่งที่มีความน่าเชื่อถือ

5.4.9. ข้อมูลการบันทึกเหตุการณ์ของอุปกรณ์สำคัญควรจัดเก็บไว้ที่เครื่องแม่ข่ายที่แยกเฉพาะ อย่างน้อย ครอบคลุม access log และ activity log โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอในการป้องกัน การเปลี่ยนแปลงแก้ไข หรือทำลาย

การบริหารจัดการ Patch (Patch Management)

5.4.10. กำหนดให้ผู้ดูแลระบบทำการติดตั้ง patch โดยประเมินจากการประเมินความเสี่ยงและการจัดลำดับความสำคัญของระบบ โดยจัดให้มีกระบวนการตรวจสอบ patch ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

5.4.11. การติดตั้ง patch บนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ บริษัทกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

5.4.12. มีการทบทวนและปรับปรุงกระบวนการบริหารจัดการ patch เพื่อให้มั่นใจได้ว่าบริษัทสามารถ ทดสอบและติดตั้ง patch ด้านการรักษาความปลอดภัย ได้ทันต่อสถานการณ์ที่เปลี่ยนไปและสามารถรองรับความเสี่ยงที่เพิ่มขึ้นได้อย่างรวดเร็ว

5.5. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (External Party Risk Management)

5.5.1. บริษัทต้องระบุ และจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่างหน่วยงานกับบุคคลภายนอก ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ กำหนดมาตรฐาน และระเบียบแนวปฏิบัติในการบริหารจัดการความเสี่ยงจากบุคคลภายนอก เพื่อให้มีการกำกับดูแลให้สอดคล้องกับการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศของบริษัท ตามหลักการดังนี้

- กำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างบริษัทและบุคคลภายนอกอย่างชัดเจนและ เป็นลายลักษณ์อักษร
- กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล จากบุคคลภายนอก
- รักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศของบริษัท และอ้างอิงมาตรฐานสากลที่ยอมรับ โดยทั่วไป และตามมาตรฐานหรือแนวทางที่บริษัทกำหนดโดยด้านการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ ครอบคลุม การรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และความพร้อมใช้งานด้านระบบสารสนเทศ (Availability)
- เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อบริษัทอย่างมีนัยสำคัญ เพื่อให้สามารถดำเนินธุรกิจ ได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการดำเนินธุรกิจ และการให้บริการแก่ลูกค้า

252/6 29th Fl., Muang Thai Phatra Complex1, Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

5.5.2. การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากบุคคลภายนอก ต้องมีการขออนุมัติอย่างเป็นทางการ และได้รับอนุมัติจากผู้มีอำนาจอนุมัติ หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

5.5.3. ผู้ดูแลระบบต้องให้สิทธิในการเข้าถึงข้อมูลต่อหน่วยงานหรือบุคคลภายนอกเท่าที่จำเป็นเท่านั้น

5.6. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

การรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

5.6.1. มีการจัดแบ่งเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบงาน ระดับความสำคัญ ของข้อมูลที่ถูกประมวลผล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่นๆ หรือจากภายนอกองค์กร และจัดให้มีการควบคุมการเชื่อมต่อระหว่างระบบงานอย่างเข้มงวด

5.6.2. มีการแบ่งแยกเครือข่ายส่วนที่เป็น Private Network และ Public Network ออกจากกัน

5.6.3. มีการจัดตั้งโซนเครือข่าย Demilitarized Zone (DMZ) เพื่อรองรับระบบงานที่ต้องมีการให้บริการ ติดต่อสื่อสาร หรือแลกเปลี่ยนข้อมูลกับภายนอก เช่น ระบบงาน Website ระบบงาน E-mail เป็นต้น โดยไม่จัดวางเครื่องแม่ข่าย ที่เป็นระบบฐานข้อมูลสำคัญไว้ในโซนดังกล่าว

5.6.4. ในจุดที่มีการแบ่งแยกเครือข่ายที่พิจารณาว่ามีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษา ความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุม คัดกรอง Traffic และการเข้าถึงเว็บไซต์ ที่ส่งผ่านระบบเครือข่าย การเฝ้าระวังการบุกรุก การป้องกันการบุกรุก และการตรวจจับไวรัส หรือมัลแวร์ต่างๆ ที่อาจบุกรุกเข้าสู่เครือข่าย

5.6.5. มีการจำกัดให้เฉพาะผู้ใช้งานที่ได้รับมอบอำนาจเท่านั้นที่สามารถเข้าถึงระบบเครือข่าย โดยจำกัดสิทธิ์ในการเข้าถึงระบบเครือข่ายให้อยู่ในส่วนที่มีความจำเป็น และเหมาะสมตามหน้าที่การทำงานเท่านั้น

5.6.6. การเปลี่ยนแปลงติดตั้งค่าต่างๆ ที่เกี่ยวกับอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย การเปลี่ยนแปลงต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงการตั้งค่าอุปกรณ์เครือข่าย และ อุปกรณ์รักษาความปลอดภัยเครือข่ายอย่างเป็นขั้นตอน พร้อมทั้งได้รับการอนุมัติดำเนินการจากผู้มีอำนาจอนุมัติ

5.6.7. มีการพิจารณาติดตั้ง Software และ Update Patch อย่างเหมาะสมแก่อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย ตามคำแนะนำของผู้ผลิต โดยการติดตั้งต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management) อย่างเป็นขั้นตอน

5.6.8. มีการเปลี่ยน Default Password ของอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย ให้เป็นไปตามนโยบายรหัสผ่าน

5.6.9. มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องประมวลผล ให้ตรงกับเครื่องแม่ข่าย NTP (Clock Synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์ (Log) มีความถูกต้องในลักษณะ Real-Time ซึ่งเครื่องแม่ข่าย NTP ต้องรับสัญญาณนาฬิกาจากสถาบันที่มีความน่าเชื่อถือ ยกตัวอย่างเช่น กรมอุทกศาสตร์ (กองทัพเรือ) หรือ สถาบันมาตรวิทยา (กระทรวงวิทยาศาสตร์และเทคโนโลยี)

5.6.10. สำหรับระบบงานที่ต้องมีการติดต่อสื่อสาร หรือแลกเปลี่ยนข้อมูลผ่านระบบ Internet ควรมี กระบวนการประเมินช่องโหว่ (Vulnerability Assessment) หรือทดสอบเจาะระบบเครือข่าย (Network Penetration Test) โดยผู้เชี่ยวชาญตามความเหมาะสมเมื่อมีการติดตั้ง Application ใหม่ หรือมีการเปลี่ยนแปลงความเสี่ยงทางระบบสารสนเทศที่มีนัยสำคัญ ตามดุลยพินิจของผู้ดูแลระบบ และได้รับการอนุมัติดำเนินการจากผู้มีอำนาจอนุมัติ

การควบคุมการเชื่อมต่อกับระบบเครือข่ายสื่อสารของบริษัท

5.6.11. ไม่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่นใด ที่บริษัทมิได้จัดหาให้มาเชื่อมต่อและใช้งานในระบบ เครือข่ายสื่อสารของบริษัท เว้นแต่ได้รับการพิจารณาอนุมัติจากผู้บังคับบัญชาหน่วยงานต้นสังกัด และผู้มีอำนาจอนุมัติของหน่วยงานเทคโนโลยีสารสนเทศ เป็นกรณีๆ ไป

5.6.12. การใช้งานการเชื่อมต่อเครือข่ายของบริษัท ต้องใช้หมายเลข IP Address ที่ผู้ดูแลระบบกำหนดให้ เท่านั้น

5.6.13. เครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่นใด ที่มีการเชื่อมต่อกับระบบเครือข่ายของบริษัท ต้องดำเนินการ ผ่านการควบคุมโดยระบบรักษาความปลอดภัยเครือข่ายของบริษัท และต้องมีการพิสูจน์ตัวตนก่อนเชื่อมต่อกับระบบเครือข่ายของบริษัท

252/6 29th Fl., Muang Thai Phatra Complex1,
Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

การควบคุมการการเชื่อมต่อมาจากเครือข่ายจากระยะไกล (Remote Access)

5.6.14. กรณีที่ต้องมีการเชื่อมต่อมาจากเครือข่ายจากระยะไกล (Remote Access) เพื่อทำการแก้ไขและ/หรือ ตั้งค่าพารามิเตอร์ของเครื่องแม่ข่าย อุปกรณ์เครือข่าย หรือโปรแกรมระบบงาน ควรมีการระบุตัวตน และพิสูจน์ตัวตนของบุคคลในลักษณะ Two-Factors Authentication และกระทำผ่านช่องทางที่มีความปลอดภัย เช่น SSH, VPN หรือ SSL/TLS เป็นต้น

5.6.15. ห้ามทำการเชื่อมต่อเพื่อเข้าถึงระบบเครือข่ายภายในองค์กรจากระยะไกลด้วยเครื่องคอมพิวเตอร์ สาธารณะ เช่น เครื่องคอมพิวเตอร์ในร้านอินเตอร์เน็ตคาเฟ่ เป็นต้น

5.6.16. ในการเข้าถึงระบบจากระยะไกล ห้ามใช้บริการเครือข่ายหรือโปรโตคอลที่ไม่มั่นคงปลอดภัย เช่น Telnet, FTP, NFS, Terminal services เป็นต้น ในกรณีที่จำเป็น ต้องมีการควบคุมโดยจำกัดโซนในการ เข้าถึง และการกำหนดสิทธิ์ในการใช้งาน

การควบคุมการเชื่อมต่อกับระบบไร้สาย (Wireless LAN)

5.6.17. กำหนดให้มีวิธีการในการพิสูจน์ตัวตน และการเข้ารหัสข้อมูลที่ปลอดภัยตามมาตรฐานสากล สำหรับ ระบบเครือข่ายไร้สายของบริษัท

5.6.18. มีอุปกรณ์ป้องกันเครือข่ายติดตั้งไว้ในระบบเครือข่ายไร้สาย เพื่อป้องกันการเข้าถึงเครือข่ายภายในของ บริษัทและจำกัดการติดต่อสื่อสารที่ไม่ได้รับอนุญาต (Unauthorized Traffic)

5.6.19. กำหนดให้มีการแยกเครือข่ายไร้สายสำหรับบุคคลภายนอกออกจากระบบเครือข่ายภายในของบริษัท ออกจากกันอย่างชัดเจน

5.6.20. ห้ามทำการเชื่อมต่อเพื่อเข้าถึงระบบเครือข่ายสาธารณะที่ไม่มีการรักษาความปลอดภัย เช่น Wi-Fi สาธารณะ

5.7. การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

5.7.1. การจัดเก็บรักษา และใช้งานข้อมูลต้องคำนึงความมั่นคงปลอดภัยของข้อมูลเป็นสำคัญ

- ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at endpoint) ให้มีการเข้ารหัสข้อมูลที่อยู่บนอุปกรณ์ พิจารณาจากเกณฑ์การประเมินความเสี่ยง และหลักเกณฑ์การจัดชั้นความลับของข้อมูล ด้วย เครื่องมือที่เหมาะสมในการดำเนินการ
- ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (Data in transit) ต้องมีการออกแบบและดำเนินการให้ มีการรับส่งข้อมูลผ่านเครือข่ายที่มีความปลอดภัย
- ข้อมูลที่อยู่บนระบบงาน และสื่อบันทึกข้อมูล (Data at rest) ให้มีการออกแบบ และดำเนินการให้มั่นใจว่าข้อมูลถูกจัดเก็บอย่างปลอดภัย มีการกำหนดสิทธิ์ในการเข้าใช้งานอย่างเหมาะสม

5.7.2. เจ้าของข้อมูล (Information Owner) จะต้องรับผิดชอบในการกำหนดสิทธิ์การเข้าถึงและการใช้งานข้อมูลอย่างปลอดภัย

5.7.3. การจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)

- สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media) ที่นำมาใช้งานภายในบริษัทต้อง ได้รับการอนุมัติจากผู้มีอำนาจอนุมัติ
- การนำข้อมูลออกจากบริษัท ต้องดำเนินการตามหลักเกณฑ์หรือนโยบายการใช้ข้อมูลสำคัญของบริษัท
- ห้ามนำสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ มาเชื่อมต่อโดยตรงกับเครื่องแม่ข่ายหรืออุปกรณ์ เว้นแต่ได้รับอนุมัติจากผู้มีอำนาจอนุมัติ และต้องดำเนินการตรวจเช็คไวรัสก่อนการเชื่อมต่อระบบ

5.7.4. การควบคุมดูแลรักษาความปลอดภัยสื่อบันทึกข้อมูลระหว่างขนส่ง (Physical Media Transfer)

- ต้องดำเนินการให้มีการควบคุมการเข้าถึงสื่อที่มี ข้อมูลสำคัญในระหว่างการขนส่ง
- จัดเก็บในบรรจุภัณฑ์ที่ปิดมิดชิด มีการป้องกันการเข้าถึง และป้องกันความเสียหาย

5.7.5. การทำลายข้อมูล (Information Disposal)

- ปฏิบัติตามมาตรฐาน และระเบียบวิธีปฏิบัติการทำลายข้อมูล (Information Disposal) ของบริษัท
- พิจารณาวิธีการทำลายข้อมูลให้สอดคล้องตามหลักเกณฑ์ของบริษัท โดยมีกระบวนการควบคุมการทำลายข้อมูล ที่ได้รับการอนุมัติจากผู้มีอำนาจอนุมัติก่อนดำเนินการ

252/6 29th Fl., Muang Thai Phatra Complex1, Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

- จัดให้มีการทำลายข้อมูลก่อนทุกครั้งเมื่อมีการยุติหรือยกเลิกการใช้งาน เช่น หมดอายุเสื่อมสภาพ หรือหมดสัญญาส่งคืน หรือถ่ายโอน หรือบริจาค หรือจัดจำหน่ายต่อ หรือไม่ใช้งานแล้ว
- การทำลายข้อมูลในสื่อสำรองบันทึกข้อมูลด้านระบบสารสนเทศ ที่หมดอายุการใช้งาน หรือตามที่กฎหมายกำหนด

ความปลอดภัยเกี่ยวกับข้อมูลของระบบสารสนเทศ

5.7.6. ผู้พัฒนาระบบต้องหลีกเลี่ยงการใช้ข้อมูลจริงในการทดสอบระบบ หากจำเป็นต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน และผู้พัฒนาระบบต้องควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง และควรเก็บ Source Code ไว้ในที่ ๆ ปลอดภัย

5.7.7. ต้องป้องกันการรั่วไหลของข้อมูลสารสนเทศ หรือลดโอกาสที่จะทำให้ข้อมูลสารสนเทศเกิดการรั่วไหลออกไปและต้องกำหนดมาตรการควบคุม และตรวจสอบการว่าจ้างให้พัฒนาระบบต้องมีความชัดเจน รวมถึงการรับรองคุณภาพของระบบและกำหนดขอบเขตในการว่าจ้างด้วย

การบริหารจัดการแลกเปลี่ยนข้อมูลและการเข้ารหัสข้อมูล (information Transfer and Cryptography)

5.7.8. กรณีที่มีการส่งข้อมูลที่เป็นความลับหรือความสำคัญผ่านช่องทางอิเล็กทรอนิกส์ หรือเคลื่อนย้ายสื่อ บันทึกข้อมูลที่มีความสำคัญ ผู้รับผิดชอบต้องดำเนินการเข้ารหัสข้อมูล เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ สามารถเข้าถึงข้อมูลได้

5.7.9. การส่งข้อมูลสำคัญกับบุคคลภายนอก ต้องกำหนดให้มีการเข้ารหัสข้อมูลสำคัญและช่องทางการสื่อสารที่ใช้ รับส่งข้อมูลสำคัญกับบุคคลภายนอกเป็นอย่างน้อย และได้รับการอนุมัติจากผู้มีอำนาจอนุมัติ

5.7.10. วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล เช่น การเข้ารหัสข้อมูลแบบสมมาตร (เช่น AES) การเข้ารหัสข้อมูลแบบอสมมาตร (เช่น Public Key Cryptography) เป็นต้น

5.7.11. กำหนดให้มีกระบวนการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key Management) ที่มีความรัดกุม ปลอดภัย

5.8. การควบคุมการเข้าถึง (Access Control)

5.8.1. **การบริหารจัดการบัญชีผู้ใช้ระบบ (User Access Management)**

- ในการเข้าใช้ระบบงานทุกครั้ง จะต้องมีการระบุตัวตนและพิสูจน์ตัวตนด้วยวิธีการที่เหมาะสม เช่น การใช้บัญชีผู้ใช้ (User ID) และรหัสผ่าน (Password) โดยจำกัดให้เฉพาะบุคคลที่ได้รับอนุญาต เท่านั้นที่สามารถเข้าถึงได้
- ในระบบงานที่มีความสำคัญควรมีการจัดทำตารางควบคุมการให้สิทธิ์ (Authorization Matrix) ที่สอดคล้องกับตำแหน่งหน้าที่งาน ตามหลักการตามความจำเป็นของหน้าที่รับผิดชอบ
- กำหนดให้มีขั้นตอนการร้องสิทธิ์การเข้าใช้ระบบและมีการอนุมัติโดยผู้ที่มีอำนาจอนุมัติทุกครั้งที่มี การเพิ่ม ยกเลิก และ/หรือ เปลี่ยนแปลง ทั้งบัญชีผู้ใช้งานและสิทธิ์ของผู้ใช้งาน
- เมื่อมีผู้ใช้งานลาออกจากงานหรือเปลี่ยนหน้าที่ความรับผิดชอบ กำหนดให้หน่วยงานต้นสังกัดและ สายงานบริหารทรัพยากรบุคคล ต้องแจ้งหน่วยงานเทคโนโลยีสารสนเทศทราบ เพื่อทำการปรับปรุง/ ยกเลิกบัญชีผู้ใช้งาน

5.8.2. **การบริหารจัดการรหัสผ่าน (Password Management)**

- รหัสผ่านควรมีความยาวไม่น้อยกว่า 8 ตัวอักษร
- รหัสผ่านควรประกอบด้วยตัวเลข ตัวอักษรใหญ่ อักษรเล็ก และ/หรือตัวอักขระพิเศษ
- กำหนดให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านทุกๆ 90 วัน ไม่ควรใช้ข้อความที่คาดเดาได้ง่าย เช่น ชื่อเล่น วันเดือนปีเกิด นามสกุล ทะเบียนรถยนต์ เป็นต้น
- รหัสผ่านถูกระงับการใช้ (Account Lock) เมื่อมีการใส่ผิด 3 ครั้งติดกัน
- รหัสผ่านไม่ควรซ้ำกับรหัสผ่านเดิมที่ใช้ 8 ครั้งที่ผ่านมา
- ต้องป้องกันรหัสผ่านไม่ให้ผู้อื่นทราบ และห้ามใช้รหัสผ่านร่วมกันกับผู้อื่น

5.8.3. **การบริหารจัดการเข้าถึงระบบงาน (System and application access control)**

- การบริหารสิทธิ์การเข้าถึงระบบของผู้มีหน้าที่ดูแลระบบงานประมวลผลหลัก ต้องมีการกำหนดสิทธิ์และแบ่งแยกหน้าที่ในการทำงานตามความจำเป็นและความเหมาะสม

252/6 29th Fl., Muang Thai Phatra Complex1,
Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

- การเข้าถึงระบบสารสนเทศทุกระบบต้องได้รับการพิสูจน์ และยืนยันตัวตนทุกครั้งอย่างน้อยด้วย Username และ Password ที่ได้รับจากผู้ดูแลระบบ ก่อนที่จะเข้าใช้งานได้ตามสิทธิ์ที่ได้รับ และหากเป็นระบบสำคัญ หรือเป็นการใช้งานจากระยะไกล (Remote Access) จะต้องกำหนดให้มีการยืนยันตัวตนแบบ 2 ขั้นตอน (Two-Factor Authentication)
- มีการระงับหรือยกเลิก Default Account ที่ไม่มีความจำเป็นในการใช้งานหรือไม่มีความจำเป็นต่อ การทำงานของระบบ เช่น Guest Accounts เป็นต้น
- มีการเปลี่ยน Default Password ของบัญชีผู้ใช้ที่มากับระบบงานให้เป็นไปตามมาตรฐานของบริษัท

5.9. การจัดหาและการพัฒนาระบบ (System Acquisition and Development)

5.9.1. ในการพัฒนาระบบจำเป็นต้องกำหนด และวางแผนความต้องการด้านความปลอดภัยอย่างรัดกุม ทั้งในระดับซอฟต์แวร์และฐานข้อมูล และควรเพิ่มระบบตรวจสอบกิจกรรม (Audit Logs) เพื่อบันทึกการเข้าถึงและการเปลี่ยนแปลงข้อมูลในระบบ

5.9.2. บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบควรเป็นไปตาม หลักการแบ่งแยกหน้าที่อย่างเหมาะสม (Segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถ ปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ควรแยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น

5.9.3. มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (Development Tools) และเครื่องมือแปลโปรแกรม (Compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยน หรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต

5.9.4. ผู้พัฒนาระบบต้องกำหนดมาตรฐาน และระเบียบวิธีปฏิบัติในการออกแบบ และพัฒนาระบบ โดยคำนึงถึงการรักษาความมั่นคงปลอดภัย ครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (Requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง รวมถึงจัดให้มีการลงนามในเอกสารที่เกี่ยวข้อง เพื่อป้องกันความผิดพลาดของการพัฒนาระบบ และการบำรุงรักษาในภายหลัง โดยกำหนดให้มีเอกสาร 4 รายการดังต่อไปนี้

- **เอกสารการวิเคราะห์ความต้องการ (Requirements Specification Document)**: เพื่อสรุปข้อกำหนดของระบบที่ต้องการ โดยจะรวมถึงฟังก์ชันการทำงานที่ระบบต้องมี
- **เอกสารออกแบบระบบ (System Design Document)**: จะอธิบายรายละเอียดเกี่ยวกับสถาปัตยกรรมของระบบ, การออกแบบฐานข้อมูล, การออกแบบอินเทอร์เฟซผู้ใช้, และโครงสร้างของโค้ด รวมถึงวิธีการที่ระบบจะเชื่อมต่อกับระบบอื่น ๆ
- **เอกสารการทดสอบ (Testing Document)**: เอกสารนี้จะรวมถึงแผนการทดสอบ, กรณีทดสอบ (Test Cases), และวิธีการในการทดสอบเพื่อให้มั่นใจว่าระบบที่พัฒนามีคุณภาพและตรงตามความต้องการ
- **เอกสารการใช้งาน (User Manual)**: เพื่อให้ข้อมูลแก่ผู้ใช้งานเกี่ยวกับวิธีการใช้งานระบบ โดยจะรวมถึงคำแนะนำในการใช้ฟังก์ชันต่าง ๆ และวิธีการแก้ไขปัญหาพื้นฐานที่อาจเกิดขึ้น

5.9.5. ผู้พัฒนาระบบต้องปฏิบัติตามมาตรฐานกระบวนการพัฒนาระบบ (Software Development Life Cycle (SDLC)) เพื่อทำให้กระบวนการพัฒนาซอฟต์แวร์มีระเบียบ และเป็นระบบมากขึ้น ช่วยให้สามารถวางแผน ควบคุม และประเมินผลการดำเนินงานได้ง่ายยิ่งขึ้น

5.9.6. เพื่อป้องกันความผิดพลาดของข้อมูลสารสนเทศ การสูญหายของข้อมูลสารสนเทศหรือการใช้งานผิดวัตถุประสงค์ ต้องมีการตรวจสอบข้อมูลนำเข้า ซึ่งผู้พัฒนาระบบต้องกำหนดกลไกว่าข้อมูลนำเข้านั้นมีความถูกต้อง และเหมาะสมก่อน ที่จะนำไปพัฒนาระบบต่อไป

5.9.7. กำหนดให้หน่วยงานที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการของหน่วยงาน ธุรกิจ (Business Requirement Confirmation)

5.9.8. ผู้พัฒนาระบบต้องใช้เครื่องมือ และวิธีการที่สามารถจัดการการเปลี่ยนแปลงในโค้ดอย่างมีประสิทธิภาพ เช่น การใช้ระบบ Version Control (เช่น Git, SVN) ที่ช่วยในการติดตามการเปลี่ยนแปลงทุกครั้งที่มีการแก้ไขโค้ด และสามารถย้อนกลับไป

252/6 29th Fl., Muang Thai Phatra Complex1, Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

ยังเวอร์ชั่นก่อนหน้าหากจำเป็น นอกจากนี้ยังต้องมีการสำรองข้อมูลอย่างสม่ำเสมอเพื่อป้องกันการสูญหายจากเหตุการณ์ที่ไม่คาดคิด เช่น ความผิดพลาดของฮาร์ดแวร์

5.9.9. มีการทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ (Unit test) ทดสอบการ ทำงานร่วมกันของระบบต่างๆ (System integration test) ทดสอบความพร้อมใช้งานตามกระบวนการและ ความต้องการของผู้ใช้งาน (User acceptance test) และทดสอบความปลอดภัยของระบบ (Security test) ตามกระบวนการรักษาความมั่นคงปลอดภัย ที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค (System Design Document) โดยเฉพาะช่องโหว่ที่อยู่ในระดับที่ระบุโดย Open Web Application Security Project (OWASP)

5.9.10. จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่างๆ ด้านประสิทธิภาพ ตามความต้องการ ของหน่วยงานธุรกิจ (Business Requirement) รวมถึงการควบคุมความมั่นคงปลอดภัยตามนโยบายหรือ มาตรฐานที่บริษัทกำหนด

5.9.11. มีการทดสอบบนสภาพแวดล้อมใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงของการเปลี่ยนแปลง บนระบบที่ให้บริการจริง

5.9.12. สำหรับการเปลี่ยนแปลงระบบมีการใช้งานหรือเชื่อมโยงกับระบบอื่นจำนวนมาก ควรจัดให้มีการ ทดสอบประสิทธิภาพ (Performance test) เพื่อให้มั่นใจได้ว่าระบบมีเสถียรภาพเพียงพอในการรองรับการทำงาน

5.9.13. สำหรับการเปลี่ยนแปลงระบบในส่วนที่เป็นการทำธุรกรรมสำคัญของระบบที่มีความสำคัญอย่างยิ่ง และมีการเชื่อมต่อกับเครือข่ายสาธารณะ ควรจัดให้มีการสอบทานคำสั่งในการเขียนโปรแกรม (Source code review)

5.9.14. ต้องมีการกำหนดมาตรฐานการเข้ารหัสข้อมูลต้องใช้เทคนิคการเข้ารหัสที่สอดคล้องกับมาตรฐานสากล เช่น AES-256, RSA, หรือเทคนิคที่ผ่านการรับรองด้านความปลอดภัยจากหน่วยงานที่เกี่ยวข้อง

5.9.15. สำหรับการบริหารจัดการกุญแจเข้ารหัสต้องกำหนดขั้นตอนในการสร้าง, แจกจ่าย, ใช้งาน, และเก็บรักษากุญแจเข้ารหัส โดยใช้ระบบหรือเครื่องมือที่มีความปลอดภัยสูงสำหรับการจัดการกุญแจ เช่น Cloud Key vault, Hardware Security Module (HSM) หรือ Key Management Service (KMS) และจำกัดสิทธิ์การเข้าถึงกุญแจเข้ารหัสเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

5.10. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านระบบสารสนเทศ (IT Incident and Problem Management)

การบริหารจัดการเหตุการณ์ผิดปกติด้านระบบสารสนเทศ (IT Incident Management)

5.10.1. ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท เช่น จุดอ่อนใด ๆ ให้แก่ผู้บังคับบัญชา หรือหน่วยงานเทคโนโลยีสารสนเทศทันทีที่พบ หรือสงสัยว่ามีสิ่งผิดปกติเกิดขึ้น และต้องกำหนดหน้าที่และความรับผิดชอบเพื่อ รับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท โดยต้องมีการบันทึกเหตุการณ์ พิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และ ค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย

5.10.2. ต้องเก็บรวบรวมหลักฐานตามกฎ หรือหลักเกณฑ์ เพื่อใช้สำหรับอ้างอิงในกระบวนการศาล หรือมาตรการที่เกี่ยวข้อง

5.10.3. ในกรณีเกิดปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการใช้งานระบบสารสนเทศ จนเป็นเหตุให้ บริษัทไม่สามารถให้บริการทางพื้นฐาน เช่น การบริการลูกค้า การรับชำระเงิน การวางบิล การโอนเงิน และ การชำระเงิน แก่ลูกค้าในวงกว้าง หรือเกิดเหตุการณ์ที่มีนัยสำคัญซึ่งอาจส่งผลกระทบต่อชื่อเสียงของบริษัท รวมถึงกรณีระบบสารสนเทศที่สำคัญของบริษัท ถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคาม ทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของบริษัททราบ ให้หน่วยงานเทคโนโลยีสารสนเทศรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้น ภายในไม่เกิน 24 ชั่วโมง นับแต่เกิดหรือรับรู้ปัญหาหรือเหตุการณ์ผิดปกติ และให้แจ้งสาเหตุและการแก้ไข ปัญหาเพิ่มเติมภายหลัง

การบริหารจัดการปัญหาด้านระบบสารสนเทศ (IT Problem Management)

5.10.4. มีมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการปัญหาด้านระบบสารสนเทศ เพื่อให้มีการนำ เหตุการณ์ผิดปกติที่ยังไม่ทราบสาเหตุที่แท้จริง (unknown root cause) เหตุการณ์ผิดปกติที่เกิดขึ้นซ้ำ (repeated incident) มาวิเคราะห์และพิจารณาแนวทางแก้ไขปัญหาจากสาเหตุที่แท้จริง (root cause)

บมจ.ภัทรลิสซิ่ง
PHATRA LEASING PLC.

252/6 29th Fl., Muang Thai Phatra Complex1, Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

5.10.5. มีกระบวนการหรือเครื่องมือในการบันทึกปัญหา หลักเกณฑ์ในการจัดประเภทปัญหา การจัดลำดับ ความสำคัญ วิเคราะห์ และจัดให้มีการติดตามการแก้ไขปัญหาเพื่อให้ปัญหาได้รับการแก้ไข

5.10.6. มีกระบวนการหรือเครื่องมือบันทึกปัญหาที่เคยเกิดขึ้น เพื่อให้เป็นแหล่งข้อมูลความรู้ให้สามารถสืบค้น เหตุการณ์ปัญหา และแนวทางการแก้ไขปัญหาได้ในภายหลังอย่างรวดเร็วและมีประสิทธิภาพ

5.11. การจัดทำแผนฉุกเฉินด้านระบบสารสนเทศ (Disaster Recovery Plan : DRP)

5.11.1. จัดทำระบบสำรองข้อมูลของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทสามารถให้บริการได้อย่างต่อเนื่อง และมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน พร้อมทั้งกำหนดหน้าที่ และความรับผิดชอบของผู้ดูแลระบบในการสำรองข้อมูลเพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

5.11.2. จัดให้มีการทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านระบบสารสนเทศประจำปี อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5.11.3. การจัดทำแผนฉุกเฉินด้านระบบสารสนเทศควร ครอบคลุมถึงการกำหนดระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และระยะเวลา สูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RP) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัท โดยจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการ เปลี่ยนแปลงอย่างมีนัยสำคัญ

5.11.4. จัดเตรียมทรัพยากรที่จำเป็น (redundancies) หรืออุปกรณ์ประมวลผลระบบสารสนเทศให้พร้อมต่อการใช้งาน และทบทวนปรับปรุงอย่างสม่ำเสมอ เพื่อให้มีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน โดยคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของระบบสารสนเทศ ความมั่นคงปลอดภัยด้านระบบสารสนเทศ เหตุการณ์ความเสียหายต่างๆ และความเสี่ยงที่ เกี่ยวข้องในการดำเนินธุรกิจของบริษัท ให้มีความต่อเนื่องในการให้บริการ

5.12. การปฏิบัติตามข้อกำหนด (Compliance)

5.12.1. ผู้ใช้งานทุกคนมีหน้าที่ต้องทำความเข้าใจ และปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด ทั้งนี้รวมถึงแต่ไม่จำกัดเฉพาะ

- นโยบายการรักษาความปลอดภัยระบบสารสนเทศ บริษัท ภัทรลิสซิ่ง จำกัด (มหาชน)
- นโยบายการสื่อสารผ่านสื่อสังคมออนไลน์ (Social network) บริษัท ภัทรลิสซิ่ง จำกัด (มหาชน)
- มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล บริษัท ภัทรลิสซิ่ง จำกัด (มหาชน)
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ 2560
- พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
- พระราชบัญญัติลิขสิทธิ์ พ.ศ 2537
- พระราชบัญญัติเครื่องหมายการค้า พ.ศ 2534
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5.12.2. ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบสารสนเทศของ บริษัท ถือเป็นทรัพย์สินของ บริษัท (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้บริษัท สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

5.12.3. ต้องกำหนดให้มีการป้องกันข้อมูล ที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและแนวปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญาและข้อกำหนดทางธุรกิจ รวมถึงต้องมีมาตรการป้องกันข้อมูลส่วนตัวตามที่ระบุไว้ในกฎหมาย แนวปฏิบัติและสัญญาที่เกี่ยวข้อง

252/6 29th Fl., Muang Thai Phatra Complex1, Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

5.12.4. ต้องกำหนดให้มีการป้องกัน สารสนเทศ ระบบสารสนเทศ ระบบเครือข่าย และเครื่องแม่ข่าย ไม่ให้ใช้งานไปในทางที่ผิดหรือโดยไม่มีสิทธิ และต้องกำหนดให้ใช้มาตรการเข้ารหัสข้อมูลโดยให้ยึดถือตามหรือสอดคล้องกับข้อตกลงทางกฎหมาย

5.12.5. การทบทวน ตรวจสอบการใช้งานระบบทุกระบบเป็นสิทธิที่บริษัทสามารถกระทำได้ หากบริษัทเห็นว่าจำเป็น โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า ต้องมีการตรวจสอบระบบว่ามีความมั่นคงปลอดภัยเพียงพอหรือไม่โดยใช้ซอฟต์แวร์ค้นหาช่องไหว่ และทดสอบการโจมตีระบบเพื่อตรวจข้อบกพร่องของระบบด้วยการรักษาความปลอดภัยในการใช้ทรัพย์สินสารสนเทศและอุปกรณ์ที่ใช้ในการปฏิบัติงาน

การเข้าถึงระบบงานและการพิสูจน์ตัวตน

5.12.6. ต้องออกจากระบบ (Log-out, Log-oft) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานานและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน

5.12.7. ต้องล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน

5.12.8. ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้งโดยใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย

5.12.9. ต้องระมัดระวังการโพสต์ข้อความ หรือการแสดงความคิดเห็นต่าง ๆ ผ่านสื่อโซเชียลมีเดีย (Social Media) ต่าง ๆ ที่อาจเข้าข่ายละเมิดบุคคลอื่นๆ หรืออันทำให้เกิดความเข้าใจผิดต่อบริษัทได้ และให้ปฏิบัติตามนโยบายการสื่อสารผ่านสื่อสังคมออนไลน์

5.12.10. ต้องระมัดระวังการได้รับข้อมูลปลอมต่างๆ หรือที่เรียกว่าการหลอกลวง “ฟิชชิ่ง” ซึ่งเป็นการหลอกให้ผู้ใช้งานคลิก หรือกรอกข้อมูล ต่างๆ ทั้งจากอีเมล เว็บ ไลน์ หรืออื่น ๆ อันมีเจตนาที่จะได้ข้อมูลสำคัญจากผู้ใช้งาน

5.12.11. ต้องตั้งรหัสผ่านให้ปลอดภัยจากการคาดเดา และเปลี่ยนรหัสผ่านทุก 90 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

5.12.12. ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่บริษัทกำหนด เพื่อใช้ในการเข้าถึงระบบสารสนเทศ ข้อมูลสารสนเทศ หรือข้อมูลของบริษัทเป็นความลับเฉพาะตนเองเท่านั้น ห้ามมิให้ผู้อื่นล่วงรู้ และใช้งานร่วมกัน

5.12.13. ผู้ใช้งานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอกจะต้องสื่อสาร และดำเนินการให้บุคคลภายนอกนั้นปฏิบัติตามนโยบายการใช้งานระบบสารสนเทศของบริษัทด้วย

5.12.14. บริษัทมีนโยบายให้ผู้ใช้งานใช้อุปกรณ์พกพาเฉพาะที่เป็นของบริษัท ในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทเท่านั้น หากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติ และหน่วยงานเทคโนโลยีสารสนเทศ

5.12.15. อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทจะต้องเป็นอุปกรณ์พกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย เช่น “Jail breaking” หรือ “Rooting” หรือ “Crack” ไม่ติดตั้ง Software ที่ละเมิดลิขสิทธิ์ รวมทั้งต้องกำหนดค่ารหัสผ่าน และเข้ารหัสข้อมูลหรืออุปกรณ์พกพาตามนโยบายที่หน่วยงานเทคโนโลยีสารสนเทศกำหนด ทั้งนี้ผู้ใช้งานต้องได้รับการพิจารณาอนุมัติจากผู้มีอำนาจอนุมัติของบริษัท เป็นกรณีไป

5.12.16. บริษัทขอสงวนสิทธิ์ในการตรวจสอบ ระงับ เพิกถอนการใช้งาน และลบข้อมูล ทั้งหมด (Wipe) บนอุปกรณ์พกพาทั้งที่เป็นของบริษัท และของส่วนตัวบุคคล ที่ใช้ในการเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัท หากเห็นว่าการใช้งานมีความเสี่ยงต่อโครงสร้างพื้นฐานต่อข้อมูลสารสนเทศของบริษัท

การบริหารจัดการทรัพย์สินสารสนเทศ

5.12.17. ผู้ใช้งานต้องใช้ทรัพย์สินสารสนเทศตามสิทธิ์ และหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย เพื่อรองรับการปฏิบัติงานในธุรกิจของบริษัทเท่านั้น

5.12.18. ผู้ใช้งานต้องไม่นำทรัพย์สินสารสนเทศ ระบบสารสนเทศของบริษัท รวมทั้งข้อมูลสารสนเทศของบริษัท หรือที่บริษัทครอบครอง ไปใช้นอกกิจการบริษัท หรือทำให้เกิดความเสียหายต่อบริษัท

252/6 29th Fl., Muang Thai Phatra Complex1,
Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

5.12.19. ผู้ใช้งานต้องไม่ให้บุคคลอื่นยืมทรัพย์สินสารสนเทศ ไม่ว่าในกรณีใดๆ เว้นแต่ได้รับการพิจารณาอนุมัติจากผู้มีอำนาจอนุมัติของบริษัท

5.12.20. ห้ามผู้ใช้งานวางทรัพย์สินสารสนเทศหรือข้อมูลสำคัญไว้ในที่ที่ไม่ปลอดภัยโดยไม่มีผู้ดูแล

5.12.21. ผู้ใช้งานต้องรับผิดชอบชดใช้ค่าเสียหาย ไม่ว่าจะเป็นการชำรุด สูญหาย ตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของผู้ใช้งาน

การใช้งานอุปกรณ์คอมพิวเตอร์

5.12.22. ผู้ใช้งานมีหน้าที่รับผิดชอบต่อการรักษาความปลอดภัยข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ ของผู้ใช้งาน รับผิดชอบต่อการใช้งานเครื่องคอมพิวเตอร์ และซอฟต์แวร์ที่ตนได้รับสิทธิใช้งาน รวมถึงการป้องกันมิให้บุคคลภายนอกหรือผู้ที่ไม่ได้รับสิทธิใช้เครื่องคอมพิวเตอร์ของตนเองโดยไม่ได้รับอนุญาต

5.12.23. ผู้ใช้งานต้องทำการล็อกอิน (Log in) ทุกครั้งที่มีการใช้งาน เมื่อเข้าใช้เครื่องคอมพิวเตอร์ ระบบงาน และระบบเครือข่ายโดยใช้บัญชีผู้ใช้ (User ID) และรหัสผ่าน (Password) ตามที่ตนได้รับสิทธิให้ใช้ เท่านั้น ทั้งนี้รหัสผ่าน (Password) ต้องเป็นไปตามนโยบายรหัสผ่าน (Password Policy)

5.12.24. ผู้ใช้งานต้องทำการล็อคหน้าจอ (Screen Lock) ทุกครั้งเมื่อไม่ได้ใช้งานเครื่องคอมพิวเตอร์ มากกว่า 15 นาที เพื่อป้องกันผู้ประสงค์ร้ายมาสวมสิทธิการใช้งานเครื่อง

5.12.25. ผู้ใช้งานต้องทำการปิดเครื่อง (Shut down) หรือ (Hibernate) เครื่องคอมพิวเตอร์และจอภาพทุกครั้งหลังใช้งานเสร็จแล้ว

5.12.26. การใช้สื่อบันทึกข้อมูลพกพา (Removable media) เช่น Universal Serial Bus (USB) หรือ External Hard disk เป็นต้น ต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติและหน่วยงานเทคโนโลยีสารสนเทศ พร้อมทั้งต้องมีการตรวจสอบไวรัสคอมพิวเตอร์ สปายแวร์ สแปมเมล์ ก่อนนำมาใช้งาน เพื่อป้องกัน การแพร่กระจายไวรัสคอมพิวเตอร์ในบริษัท

5.12.27. ผู้ใช้งานที่ใช้งานเครื่องคอมพิวเตอร์ประเภท Notebook / Tablet ต้องดำเนินการดังนี้

- ไม่วาง หรือฝากเครื่องคอมพิวเตอร์ Notebook / Tablet โดยไม่มีผู้ดูแลหรือไม่มีอุปกรณ์ในการ ป้องกันการสูญหาย
- ไม่เชื่อมต่อเครื่องคอมพิวเตอร์ Notebook/Tablet กับเครือข่ายสาธารณะที่ไม่มีระบบการรักษา ความปลอดภัยที่เพียงพอ (Unsecured)
- กำหนดให้ผู้ใช้งานที่มีความจำเป็นต้องเชื่อมต่อเข้ามายังระบบสารสนเทศของบริษัทจากภายนอก ต้องผ่านเครือข่าย VPN ที่บริษัทกำหนด

5.12.28. ห้ามผู้ใช้งาน ดำเนินการโยกย้ายอุปกรณ์ส่วนกลางจากสถานที่ตั้งที่กำหนด ไม่ว่าจะเป็นภายในชั้นเดียวกัน อาคารเดียวกัน หรือต่างอาคารต่างชั้น ตลอดจนกระทำการใดๆ อันเป็นเหตุให้อุปกรณ์ดังกล่าวไม่สามารถใช้งานได้

5.12.29. ห้ามดำเนินการถอดถอน หรือปรับแต่ง ต่อเติมเครื่องคอมพิวเตอร์และซอฟต์แวร์ โดยไม่ได้รับการอนุมัติจากผู้มีอำนาจอนุมัติ และหน่วยงานเทคโนโลยีสารสนเทศ

5.12.30. ไม่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่นใด ที่บริษัทมิได้จัดหาให้มาใช้งานในระบบเครือข่ายสื่อสาร ของบริษัท เว้นแต่ได้รับการอนุมัติจากผู้มีอำนาจอนุมัติ และหน่วยงานเทคโนโลยีสารสนเทศ เป็นกรณีไป

5.12.31. การใช้งานระบบ และอุปกรณ์คอมพิวเตอร์ เพื่อกิจธุระส่วนตัวนั้นอนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่กระทบหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของผู้ใช้งาน และการดำเนินงานของบริษัท

5.12.32. ไม่ให้มีการจัดเก็บข้อมูลสำคัญในเครื่องคอมพิวเตอร์ของผู้ใช้งาน แต่หากมีความจำเป็นต้องจัดเก็บ ผู้ใช้งานต้องจัดให้มีการรักษาความปลอดภัยที่รัดกุมเพียงพอ โดยการกำหนดสิทธิการเข้าถึง หรือการเข้ารหัส เป็นต้น

5.12.33. ไม่ดำเนินการคัดลอกส่วนหนึ่งส่วนใดของข้อมูลสำคัญของบริษัทหรือลูกค้าออกนอกบริษัท โดยไม่ได้รับอนุญาต การละเมิดจะถูกดำเนินการทางวินัยและทางกฎหมายขั้นสูงสุด

252/6 29th Fl., Muang Thai Phatra Complex1,
Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

5.12.34. ผู้ใช้งานต้องดำเนินการจำกัดการเข้าถึงพื้นที่จัดเก็บข้อมูลส่วนกลาง Shared Drive Shared Folder หรือ SharePoint ตามความจำเป็นในการใช้งาน และต้องบริหารจัดการเนื้อที่ในการจัดเก็บข้อมูลตามสิทธิ์ที่ได้รับและเพื่อการปฏิบัติงานเท่านั้น

การใช้งานทรัพย์สินด้านซอฟต์แวร์

5.12.35. บริษัทให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัทอนุญาตให้ใช้งานหรือที่ บริษัทมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น

5.12.36. ซอฟต์แวร์ที่ทางบริษัทได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งาน ทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่นโดยพละการ

5.12.37. ไม่ติดตั้งซอฟต์แวร์ที่เครื่องคอมพิวเตอร์อื่นใดที่บริษัทมิได้จัดหาให้ใช้งาน โดยการกระทำดังกล่าวถือ เป็นการละเมิดนโยบายของบริษัท ถึงแม้ซอฟต์แวร์ดังกล่าวจะเป็นซอฟต์แวร์ถูกกฎหมายก็ตาม และ หากซอฟต์แวร์ที่ติดตั้งเป็นซอฟต์แวร์ละเมิดลิขสิทธิ์ ผู้ใช้งานต้องรับผิดชอบตาม พรบ.ลิขสิทธิ์ และกฎหมายอื่นๆ ที่เกี่ยวข้องทั้งหมด

5.12.38. ซอฟต์แวร์ที่นำมาใช้ในการประมวลผล และจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัท ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติ อย่างเหมาะสมโดยหน่วยงานเจ้าของระบบและหน่วยงานเทคโนโลยีสารสนเทศ ก่อนนำมาติดตั้งใช้งานบนระบบสารสนเทศของบริษัท

5.12.39. ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปขององค์กร มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้อย่างเหมาะสม

5.12.40. ผู้ใช้งานต้องให้ความร่วมมือ และอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลระบบในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลของผู้ใช้งาน และเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา ผู้ดูแลระบบ

การบริหารจัดการข้อมูล

5.12.41. ผู้ใช้งานต้องปฏิบัติตามนโยบายที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูลตามที่บริษัทกำหนด

5.12.42. เอกสารสำคัญที่ผู้ใช้งานใช้งานร่วมกันควรกำหนดให้มีการใช้งาน Share Drive หรือ SharePoint ส่วนกลาง เพื่อลดความเสี่ยงจากการสูญหายของไฟล์ และสนับสนุนการเข้าถึงเอกสารอย่างสะดวกและรวดเร็ว

5.12.43. การใช้งาน Share Drive หรือ SharePoint ส่วนกลาง ต้องมีการกำหนดสิทธิ์การเข้าถึงให้เหมาะสมกับความจำเป็นของผู้ใช้งานที่เกี่ยวข้อง

5.12.44. การแชร์ไฟล์ผ่าน SharePoint หรือ OneDrive การแชร์ไฟล์ทั้งภายในบริษัทและบุคคลภายนอกควรมีการกำหนดสิทธิ์ที่ชัดเจน โดยระบุผู้รับอย่างเจาะจง พร้อมทั้งตั้งค่ารหัสผ่านหรือกำหนดวันหมดอายุของไฟล์ที่แชร์ เพื่อป้องกันการรั่วไหลของข้อมูลโดยไม่ได้รับอนุญาต

5.12.45. ผู้ใช้งานควรให้ความสำคัญกับการตรวจสอบสถานะการซิงค์ข้อมูลบน OneDrive ให้เป็นปกติเสมอ เพื่อลดความเสี่ยงจากการสูญหายของข้อมูล พร้อมทั้งแก้ไขปัญหาที่อาจเกิดขึ้นทันที เช่น ไฟล์ค้างหรือไม่ได้อัปโหลด รวมถึงดูแลพื้นที่จัดเก็บให้เพียงพอ เพื่อให้การใช้งานเป็นไปอย่างราบรื่นและปลอดภัย

5.12.46. ผู้ใช้งานต้องให้ความสำคัญและระมัดระวังต่อการจัดเก็บ และการใช้ข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของบริษัท หรือ เป็นข้อมูลของลูกค้า

5.12.47. ข้อมูลที่อยู่ภายในทรัพย์สินสารสนเทศของบริษัท ถือเป็นทรัพย์สินของบริษัท ห้ามไม่ให้ผู้ใช้งาน ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาต

5.12.48. ห้ามผู้ใช้งานจัดเก็บข้อมูลและแชร์ไฟล์บนเว็บไซต์ที่ให้บริการฝากข้อมูลสาธารณะ (Public File Sharing)

5.12.49. ไม่ให้มีการจัดเก็บข้อมูลสำคัญ หรือข้อมูลส่วนบุคคลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน แต่หากมีความ จำเป็นต้องจัดเก็บ ผู้ใช้งานต้องจัดให้มีการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น กำหนดสิทธิ การเข้าถึง มีการเข้ารหัสข้อมูล เป็นต้น

252/6 29th Fl., Muang Thai Phatra Complex1,
Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

5.12.50. ข้อมูล หรือข้อมูลส่วนบุคคลที่ใช้งาน และจัดเก็บ ต้องไม่เป็นข้อมูลที่ได้มาจากการละเมิดลิขสิทธิ์ ข้อมูล ที่ขัดต่อกฎหมาย ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน และการจัดเก็บข้อมูลส่วนบุคคล ในทรัพย์สินของบริษัท จะต้องไม่ก่อให้เกิดการรบกวนต่อการปฏิบัติงานหรือการใช้ระบบเทคโนโลยี สารสนเทศของบริษัท บริษัทมีสิทธิในการตรวจสอบการจัดเก็บข้อมูลหรือข้อมูลส่วนบุคคลได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

5.12.51. ผู้ใช้งานมีหน้าที่ในการดูแลรักษาและรับผิดชอบต่อข้อมูล หากผู้ใช้งานนำไปใช้ในทางที่ผิด หรือ นำไปเผยแพร่โดยไม่ได้รับอนุญาต หรือทำให้สูญหาย เสียหายโดยเจตนาไม่สุจริต เป็นเหตุให้เกิดความ เสียหายต่อบริษัทหรือบุคคลภายนอก ผู้ใช้งานจะต้องรับผิดชอบต่อความเสียหายนั้นเป็นการเฉพาะบุคคล

5.12.52. การเจตนาเข้าถึงระบบหรือการเข้าถึงข้อมูลส่วนบุคคล (Data Privacy) โดยไม่ได้รับอนุญาต การจงใจใส่ข้อมูลที่ผิดพลาด และการเจตนาเปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต ถือเป็นสิ่งต้องห้ามทั้งสิ้น การไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงด้านระบบสารสนเทศนี้ ถือว่ามีความผิดทางวินัย

การป้องกันโปรแกรมไม่ประสงค์ดี

5.12.53. เครื่องที่ใช้งานต้องมีการติดตั้งโปรแกรมรักษาความปลอดภัย Anti-virus / Anti-malware โดยมีการ ปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่ประสงค์ดี (Malware) ให้เพียงพอและเป็นปัจจุบัน เพื่อให้สามารถป้องกันภัยคุกคามใหม่ๆ ได้

5.12.54. ผู้ใช้งานต้องทำการตรวจสอบเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา หรืออุปกรณ์อื่นๆ ที่ผู้ใช้งานรับผิดชอบให้มีการตรวจสอบการอัปเดตซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ

5.12.55. ห้ามผู้ใช้งานดำเนินการถอดถอน ระงับการทำงาน หรือปรับแต่งโปรแกรมรักษาความปลอดภัย Anti-virus / Anti-malware จากเครื่องคอมพิวเตอร์ที่ใช้งาน

5.12.56. กำหนดให้ผู้ใช้งานมีการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี (Scan) เป็นประจำ สม่ำเสมอ ตามรอบระยะเวลาที่กำหนด ต้องทำการตรวจสอบข้อมูลที่ได้รับจากภายนอกบริษัททุกครั้ง ด้วยโปรแกรมรักษาความปลอดภัย Anti-Virus / Anti-malware

5.12.57. หากพบว่ามีการติดไวรัสคอมพิวเตอร์ ผู้ใช้ต้องไม่เชื่อมต่อเข้าสู่ระบบสารสนเทศของบริษัท และต้องแจ้งหน่วยงานเทคโนโลยีสารสนเทศทันที

การใช้งานอินเทอร์เน็ต

5.12.58. บริษัทจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินธุรกิจของบริษัท และอำนวยความสะดวกแก่ผู้ใช้งานในการปฏิบัติงาน การวิจัยการค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก

5.12.59. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัท และบุคคลผู้ที่เกี่ยวข้องกับบริษัทเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การ ใช้งานอินเทอร์เน็ตในทางที่ผิด ถือเป็นความผิดทางวินัยและอาจถูกดำเนินคดีตามกฎหมาย

5.12.60. การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง (Gateway) ที่ได้รับอนุญาต หรือผ่านเครื่อง คอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเท่านั้น ทั้งนี้บริษัทขอสงวนสิทธิ์ในการ ตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

5.12.61. ห้ามไม่ให้ผู้ใช้งานดำเนินการ ดังต่อไปนี้

- ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์เพื่อการกระทำผิดกฎหมาย หรือก่อความเสียหาย ให้แก่บริษัท หรือบุคคลอื่น
- ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์เพื่อขัดขวางการใช้งานของเครือข่ายคอมพิวเตอร์ของบริษัท หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของบริษัทไม่สามารถใช้งานได้ตามปกติ
- คลิกหน้าต่างโฆษณา หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมี โปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

252/6 29th Fl., Muang Thai Phatra Complex1, Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

- เข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
- แสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด บล็อก หรือ โซเชียลมีเดีย) ของผู้ใช้งาน ทั้งนี้ความเสียหายใดๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็น ดังกล่าวถือเป็นความรับผิดชอบของผู้ใช้งาน
- คัดลอกข้อมูล หรือเผยแพร่ ข้อมูล ที่ไม่เหมาะสม หรืออาจก่อให้เกิดความรุนแรง ทำลายชื่อเสียง ของบริษัทหรือของบุคคลภายนอก หยาบคาย ลามกอนาจาร ขัดต่อกฎหมาย ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน และความมั่นคงของประเทศ หรือกระทบต่อกิจการของบริษัท
- ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์ที่ไม่เหมาะสม เช่น เล่นการพนัน ละเมิดลิขสิทธิ์ หรือกระทำอื่นใดที่อยู่นอกเหนือขอบเขตจริยธรรม หรือ พฤติกรรมอันเหมาะสม
- ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์เพื่อการเปิดเผยที่เป็นความลับ ซึ่งได้มาจากการ ปฏิบัติงาน ทั้งข้อมูลของบริษัทและข้อมูลของลูกค้า
- ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์ในทางละเมิดทรัพย์สินทางปัญญาของบริษัท หรือบุคคลอื่น
- เปิดหรือใช้งานโปรแกรมสื่อสารข้อความทางอินเทอร์เน็ต (Messaging Chat) ทุกประเภท เว้นแต่ จะได้รับการอนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น

การใช้งานอีเมล และเครื่องมือสื่อสารของบริษัท

5.12.62. ผู้ใช้งานต้องใช้งานอีเมล และเครื่องมือสื่อสารของบริษัทตามสิทธิ์และหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย เพื่อรองรับการปฏิบัติงานในธุรกิจของบริษัทเท่านั้น ห้ามมิให้ใช้งานเพื่อวัตถุประสงค์อื่น

5.12.63. ผู้ใช้งานมีหน้าที่ในการดูแล รักษา ชื่อบัญชีและรหัสผ่าน ห้ามผู้ใช้งานนำบัญชีอีเมล และเครื่องมือสื่อสารของตนเองไปให้ผู้อื่นใช้งาน

5.12.64. ผู้ใช้งานอีเมล และเครื่องมือสื่อสารของบริษัทต้องคำนึงถึงการรักษาความมั่นคงปลอดภัยข้อมูล จัดให้มีการเข้ารหัสข้อมูลต้องปฏิบัติตามนโยบายการจัดชั้นข้อมูลของบริษัท

5.12.65. การส่งอีเมล ผู้ใช้งานต้องระบุชื่อผู้รับ หัวเรื่อง ให้ชัดเจน พร้อมทั้งตรวจสอบความถูกต้องของชื่อ ผู้รับ เนื้อหาและข้อมูลที่แนบไปกับอีเมล เพื่อเป็นการป้องกันการรั่วไหลของข้อมูล

5.12.66. ผู้ใช้งานใช้งานอีเมลกลาง ต้องดำเนินการตรวจสอบอีเมลกลางเป็นประจำ หากไม่มีความ จำเป็นต้องใช้งานให้ทำการขอยกเลิกการใช้อีเมลกลางนั้น

5.12.67. ผู้ใช้งานจะได้รับพื้นที่จัดเก็บอีเมลขนาด 50GB โดยผู้ใช้งานจะต้องดำเนินการลบอีเมลที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษา พื้นที่เก็บอีเมลให้เป็นไปตามขนาดที่บริษัทกำหนด

5.12.68. หากผู้ใช้งานได้รับอีเมลที่สงสัยว่าเป็นสแปม หรือมีความพยายามที่จะหลอกลวง ควรรายงานให้ผู้ดูแลระบบรับทราบ เพื่อทำการตรวจสอบและดำเนินการป้องกันไม่ให้เกิดความเสียหายต่อระบบของบริษัท

5.12.69. ห้ามไม่ให้ผู้ใช้งานดำเนินการ ดังต่อไปนี้

- ใช้ระบบอีเมลสาธารณะ (Public Email) หรือระบบอีเมลส่วนตัว เช่น Hotmail, Gmail, Yahoo mail เป็นต้น เว้นแต่ในกรณีที่ระบบอีเมลของบริษัทขัดข้องและต้องได้รับการพิจารณาอนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น
- ส่งอีเมล หรือเอกสารสำคัญของบริษัทต่อบุคคลภายนอก โดยไม่ได้รับอนุญาต
- คลิกลิงก์หรือเปิดไฟล์แนบที่มาจากแหล่งที่ไม่รู้จัก หรือไม่น่าเชื่อถือ โดยเฉพาะไฟล์ที่มีนามสกุล .exe, .vbs, .js, .zip และ .rar เนื่องจากอาจมีไวรัส หรือมัลแวร์ที่อาจจะทำให้ระบบสารสนเทศของบริษัทได้รับความเสียหาย
- ให้ข้อมูลข่าวสารแก่บุคคลอื่น โดยไม่ได้รับอนุญาตจากบริษัทหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว
- ส่งอีเมลที่มีลักษณะเป็นการผิดกฎหมาย ละเมิดสิทธิส่วนบุคคล หรือสื่อลามก ใช้ข้อความวาจา ที่ไม่สุภาพ ขัดต่อศีลธรรม ความสงบเรียบร้อย
- ระมัดระวังการเปิดเอกสารหรือไฟล์แนบที่ส่งมาทางอีเมล หรือคลิกลิงก์ที่แนบมาในอีเมล ที่ส่งมาจากบุคคลที่ไม่รู้จัก
- ใช้ระบบอีเมลของบริษัทเพื่อเผยแพร่ข้อมูลและโปรแกรมที่ไม่ประสงค์ดี มีลักษณะ เป็นอันตรายต่อผู้อื่น

252/6 29th Fl., Muang Thai Phatra Complex1, Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

- ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท
- ส่งอีเมลครั้งละจำนวนมาก เช่น ส่งหาผู้รับทุกคนในบริษัท (All Users) ผู้รับที่มีลักษณะ เป็นกลุ่ม รวมทั้งส่งไฟล์ที่มีขนาดใหญ่ เว้นแต่ได้รับการอนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น
- นำบัญชีอีเมลซึ่งเป็นของบริษัทไปเผยแพร่สู่บุคคลอื่น ไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในช่องทางสื่ออิเล็กทรอนิกส์ นำไปลงทะเบียนบริการต่างๆ เป็นต้น เว้นแต่การเผยแพร่นั้นจัดทำขึ้นเพื่อการดำเนิน ธุรกิจของบริษัท หรือได้รับการอนุมัติจากผู้มีอำนาจอนุมัติของบริษัทเท่านั้น

5.12.70. ผู้ใช้งานต้องร่างเนื้อหาของอีเมลด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนของบริษัท ผู้ใช้งานจะต้องใช้ข้อความที่สุภาพและเป็นทางการ ไม่ใช้ข้อความที่หยาบคาย ลามกอนาจาร การยั่วยุทางเพศ หลอกลวง ผิดกฎหมาย ละเมิดสิทธิ เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ หรือสร้างความรำคาญแก่ผู้อื่น หรืออีเมลที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมลที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด รวมทั้งแสวงหาผลประโยชน์ในเชิงธุรกิจส่วนตัว หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในการใช้อีเมล เนื้อหาที่ส่งผลเสียต่อบริษัท

การใช้อุปกรณ์ส่วนตัว (Bring Your Own Device : BYOD)

5.12.71. ห้ามผู้ใช้งานใช้อุปกรณ์ส่วนตัว ในการเข้าถึงระบบเครือข่ายสื่อสาร ระบบงานและข้อมูลของบริษัท หากมีความจำเป็นต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติของบริษัท เป็นกรณีๆ ไป

5.12.72. ผู้ใช้งานต้องทำการตรวจสอบ วิเคราะห์ และความเสี่ยงของอุปกรณ์ที่นำมาใช้งานในบริษัท โดยเครื่องคอมพิวเตอร์ ต้องติดตั้ง Anti-virus/ Anti-malware หรือโปรแกรมตามที่บริษัทกำหนด

5.12.73. ผู้ใช้งานต้องกำหนดรหัสผ่านเพื่อใช้ในการล็อค หรือปลดล็อคในการเข้าถึงอุปกรณ์ส่วนตัว

5.12.74. ห้ามผู้ใช้งานใช้อุปกรณ์โทรศัพท์เคลื่อนที่ (Tablet / Smartphone) ที่ถูกปรับแต่ง (Rooted หรือ Jail break) ลงทะเบียนใช้งานระบบเครือข่ายสื่อสาร ระบบงานและข้อมูลของบริษัท

5.13. การนำเทคโนโลยีปัญญาประดิษฐ์ (AI) เข้ามาใช้ในกิจการของบริษัท

เพื่อกำหนดแนวทางและข้อปฏิบัติในการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้ให้เกิดประสิทธิภาพสูงสุด โดยคำนึงถึงความปลอดภัย ความเป็นส่วนตัว และการดำเนินกิจการของบริษัท โดยมีรายละเอียดดังต่อไปนี้

5.13.1. ข้อมูลที่ AI ใช้ในการประมวลผลต้องได้รับการปกป้องและจัดการตามนโยบายความปลอดภัยของบริษัท

5.13.2. ห้ามผู้ใช้งานนำข้อมูลของบริษัท ไม่ว่าจะเป็นข้อมูลที่มีความลับ ข้อมูลทางธุรกิจ ข้อมูลส่วนบุคคล หรือข้อมูลใดๆ ที่ไม่ได้รับอนุญาต เข้าสู่ระบบ AI ใดๆ ทั้งสิ้น ไม่ว่าจะเป็นระบบที่พัฒนาโดยบริษัทหรือระบบของบุคคลที่สาม เว้นแต่ได้รับอนุมัติจากผู้มีอำนาจอนุมัติ

5.13.3. ห้ามใช้ AI ในการสร้างหรือเผยแพร่ข้อมูลที่ไม่เหมาะสม ผิดกฎหมาย หรืออาจก่อให้เกิดความเสียหายต่อชื่อเสียงของบริษัท

5.13.4. การนำ AI หรือ ข้อมูลที่สร้างจาก AI ต้องผ่านการทดสอบและตรวจสอบความถูกต้อง ก่อนนำมาใช้งานจริง และมีการติดตามประสิทธิภาพและความเสี่ยงอย่างต่อเนื่อง

5.13.5. การตัดสินใจที่มีผลกระทบสำคัญ เช่น การวิเคราะห์ข้อมูลทางธุรกิจ ต้องมีการตรวจสอบความถูกต้องของข้อมูลก่อนนำไปใช้

5.13.6. ข้อมูลส่วนบุคคลที่ใช้ในการประมวลผล AI ต้องได้รับความยินยอมจากเจ้าของข้อมูล ทั้งนี้ข้อมูลที่ใช้กับ AI ต้องผ่านการลบข้อมูลส่วนบุคคล (Data Anonymization) หากไม่จำเป็นต้องระบุข้อมูลดังกล่าวในการประมวลผล

5.13.7. ผู้ใช้งานต้องปฏิบัติตามข้อกำหนด และประกาศที่เกี่ยวข้องกับการใช้งาน AI ที่กำหนดโดยบริษัท ใช้งานเฉพาะ AI ที่บริษัทรับรอง หรือได้รับอนุมัติอย่างเป็นทางการจากผู้มีอำนาจอนุมัติ

252/6 29th Fl., Muang Thai Phatra Complex1,
Rachadaphisek Rd., Huaykwang, Bangkok 10320
www.pl.co.th
Tel. 0-2290-7575, 0-2693-2288
Fax. 0-2693-2298-99

5.13.8. ผู้ดูแลระบบ และผู้พัฒนาระบบ มีหน้าที่ติดตั้ง ตรวจสอบ และปรับปรุงให้สามารถเข้าใช้งาน AI ได้อย่างมีประสิทธิภาพ รวมถึงรักษาความปลอดภัยของระบบ AI

5.13.9. ผู้ใช้งานควรตรวจสอบข้อตกลงการให้บริการ (Terms of Service) และนโยบายความเป็นส่วนตัวของผู้ให้บริการ AI อย่างถี่ถ้วน

5.13.10. ผู้ใช้งานมีหน้าที่รายงานปัญหา หรือข้อผิดพลาดที่พบในการใช้งานระบบ AI ให้กับหน่วยงานที่เกี่ยวข้องโดยทันที

6. การบังคับใช้ การตักเตือน และการลงโทษ

การบังคับใช้

ผู้บังคับบัญชามีหน้าที่ในการควบคุมผู้ใต้บังคับบัญชา ให้ปฏิบัติตามเงื่อนไข นโยบายอย่างเคร่งครัด หากพบว่าผู้ใช้งานภายใต้การควบคุมได้กระทำความผิด ผู้บังคับบัญชามีหน้าที่ดำเนินการตามกฎระเบียบข้อบังคับของบริษัทอย่างเคร่งครัด การละเว้นการปฏิบัติหน้าที่ถือเป็นความผิดเช่นเดียวกับผู้กระทำผิด

การตักเตือน

ผู้ใช้งานที่ฝ่าฝืนนโยบายความมั่นคงปลอดภัยสำหรับระบบสารสนเทศฉบับนี้ แม้ว่าจะเจตนาหรือไม่เจตนา ไม่ว่าการฝ่าฝืนนั้นจะกระทำไม่สำเร็จก็ตาม

- ในกรณีที่เป็นการฝ่าฝืนไม่ร้ายแรง และยังไม่พบว่าเกิดความเสียหายใดๆ ให้ผู้ดูแลระบบทำการตักเตือนผู้ใช้งานให้ปฏิบัติให้ถูกต้อง และถ้าพบเห็นการกระทำซ้ำให้แจ้งผู้บังคับบัญชาของผู้ใช้งานรับทราบ
- ในกรณีที่เป็นการฝ่าฝืนร้ายแรง ผู้ดูแลระบบจะแจ้งสายงานบริหารทรัพยากรบุคคลเป็นผู้พิจารณาดำเนินการลงโทษ

การลงโทษ

ผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบายความมั่นคงปลอดภัยสำหรับระบบสารสนเทศฉบับนี้ แม้ว่าการฝ่าฝืนนั้น จะกระทำไม่สำเร็จก็ตามให้ถือว่ามีความผิดโดยสมบูรณ์

- การกระทำใดที่มีเจตนาฝ่าฝืน และ/หรือเป็นความผิดตามนโยบายความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของบริษัทฉบับนี้หรือฉบับอื่นที่จะมีการแก้ไขเพิ่มเติมต่อไปในภายภาคหน้ากำหนดไว้ ถือเป็นการกระทำที่ฝ่าฝืนข้อบังคับเกี่ยวกับการทำงานหรือระเบียบเกี่ยวกับการทำงานในกรณีร้ายแรง ให้ลงโทษผู้กระทำผิดตามระเบียบของบริษัท
- การกระทำใดที่เป็นความผิดตามที่กฎหมายได้บัญญัติไว้ ถือเป็นความผิดส่วนบุคคล ผู้กระทำผิดจะต้องพ้นสภาพความเป็นพนักงานของบริษัทและจะต้องชดใช้ค่าเสียหายที่เกิดขึ้นทั้งสิ้น พร้อมกับถูกดำเนินคดีจนถึงที่สุด