นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศ และระบบเครือข่าย และคอมพิวเตอร์ของ บริษัท พรอดดิจิ จำกัด (มหาชน) เป็นไปอย่างเหมาะสม มีความมั่นคง ปลอดภัย และ สามารถสนับสนุนการดำเนินงานของบริษัทฯ ได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ กฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัทฯ ทางบริษัทฯ จึงกำหนดนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

วัตถุประสงค์

เพื่อสร้างความตระหนักด้านความปลอดภัยในระบบสารสนเทศของบริษัทฯ มุ่งเน้นการกำกับดูแล การดำเนินงาน เพื่อบริหารจัดการให้ระบบสารสนเทศ มีความถูกต้องสมบูรณ์ พร้อมใช้งานอยู่เสมอ และเผยแพร่ความรู้ ความเข้าใจ ให้กับผู้ใช้งานทุกระดับภายในบริษัทฯ รวมถึงสร้างการรับรู้ถึงผลกระทบที่จะเกิดขึ้นจากเหตุการณ์ภัยคุกคาม หรือการเข้าถึงข้อมูลของบริษัทฯ เพื่อให้พนักงานทุกระดับปฏิบัติตามนโยบายที่บริษัทฯ กำหนดไว้อย่างเคร่งครัด

ขอบเขต

ครอบคลุมการใช้งานด้านระบบสารสนเทศทั้งหมดของบริษัทฯ ทั้งในส่วนของสำนักงานใหญ่และสาขา รวมถึงการขยายสาขา บริษัทย่อย บริษัทในเครือ ที่อาจเกิดขึ้นในอนาคต

ขั้นตอนการปฏิบัติ

1. สื่อสารผ่านช่องทางต่างๆ ภายในบริษัทฯ เพื่อให้พนักงานทุกระดับรับทราบนโยบายฯ และถือปฏิบัติตามหน้าที่ของตนอย่างเหมาะสม พร้อมทั้งปกป้องข้อมูลของบริษัทฯ โดยพนักงานต้องลงนามในข้อตกลงการรักษาความลับของบริษัทฯ และจัดให้มีการทบทวนความเข้าใจของผู้ใช้งานเกี่ยวกับการใช้งานระบบสารสนเทศของบริษัทฯ
2. แผนกไอทีจัดทำคู่มือการใช้งานระบบต่างๆ ที่เกี่ยวข้องกับการทำงาน เพื่อลดความเสี่ยงต่อระบบสารสนเทศของบริษัทฯ
3. แผนกไอทีจะต้องติดตามการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ เพื่อปรับปรุงพัฒนาระบบ ให้สามารถป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ให้มีประสิทธิภาพ และสอดคล้องกับสถานการณ์ที่เป็นปัจจุบัน

4. แผนกไอทีมีการคัดเลือกผู้ให้บริการคลาวด์เซิร์ฟเวอร์ (Cloud Server) สำหรับอีเมลโฮสติ้ง (Email Hosting) และ เว็บโฮสติ้ง (Web Hosting) ที่น่าเชื่อถือ และมีแผนรองรับความเสี่ยงจากภัยคุกคามทางไซเบอร์ และความรับผิดชอบต่อผู้รับบริการ
5. แผนกไอทีกำหนดให้มีแผนการบำรุงรักษาดูแลขีดความสามารถของอุปกรณ์ไอทีทั้งฮาร์ดแวร์ (Hardware) และ ซอฟต์แวร์ (Software) เป็นประจำทุกปี
6. แผนกไอทีมีการจัดหาระบบ Firewall และ Antivirus ตลอดจนเครื่องมือป้องกันต่อต้านภัยคุกคามประเภทอื่นๆ ที่มีประสิทธิภาพ และมีการอัพเดทอยู่เสมอ เพื่อปกป้องข้อมูลสำคัญในระบบสารสนเทศของบริษัทฯ
7. แผนกไอทีมีการจัดทำการสำรองข้อมูล (Backup) ของบริษัทฯ มีการตรวจสอบการสำรองข้อมูล และทดสอบผลการสำรองข้อมูลอย่างต่อเนื่อง
8. แนวทางการคัดเลือกผู้ขายและผู้ให้บริการที่ได้กำหนดไว้ตาม TOR ทางแผนกไอทีจะต้องตรวจสอบระยะเวลาการประกันสินค้า และระยะเวลาการให้บริการ โดยการสอบทานการประกันสินค้าและการให้บริการของผู้ขายและผู้ให้บริการ ให้เป็นไปตามเงื่อนไขทางการค้า หรือ บันทึกข้อตกลงทางการค้าที่ได้กำหนดไว้
9. พนักงานไอทีควรจะได้รับการอบรมและพัฒนาอย่างต่อเนื่อง เพื่อพัฒนาขีดความสามารถของตนเกี่ยวกับด้านเทคโนโลยีสารสนเทศ และให้ทันต่อปัญหาภัยคุกคามทางไซเบอร์ รวมถึงเทคโนโลยีการป้องกันความเสี่ยงอย่างต่อเนื่อง
10. พนักงานทุกคนจะต้องปฏิบัติตามหลักการใช้อีเมล (Email) และการเข้าถึงอินเทอร์เน็ต (Internet) ของบริษัทอย่างถูกต้อง
11. ห้ามพนักงานทุกระดับใช้โปรแกรมคอมพิวเตอร์ที่ไม่เกี่ยวข้องกับภารกิจของบริษัท ในเครื่องคอมพิวเตอร์ของบริษัทฯ โดยทางแผนกไอทีต้องทำการสำรวจเครื่องคอมพิวเตอร์ของพนักงานเป็นประจำอย่างสม่ำเสมอ
12. หากพนักงานคนใดไม่ปฏิบัติตามนโยบายฯ จะได้รับการลงโทษ เสมือนเป็นการกระทำผิดทางวินัยของบริษัทฯ

การตอบสนองเหตุการณ์

การตอบสนองเหตุการณ์ หมายถึง การดำเนินการเมื่อเกิดภัยคุกคามต่อระบบสารสนเทศ โดยการตอบสนองคือ แผนกไอทีจะต้องดำเนินการยับยั้งการโจมตีของภัยคุกคาม กู้คืนระบบ และแจ้งให้ผู้บริหารรับทราบโดยเร็วที่สุด พร้อมทั้งกำหนดวิธีการปรับปรุงและพัฒนาระบบสารสนเทศของบริษัทฯ เพื่อป้องกันและลดความเสี่ยง ที่อาจจะเกิดขึ้นอีกในอนาคต

แผนกไอทีต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และ ภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ตามแผนบริหารภาวะวิกฤตของบริษัทฯ การให้ความรู้ วิธีการปฏิบัติที่ถูกต้องแก่ผู้ใช้งานระบบ และหากเกิดปัญหาในด้านระบบจะต้องแจ้งให้แผนกไอทีได้รับทราบ รวมถึงในกรณีที่พบเหตุการณ์ภัยคุกคามต่อระบบสารสนเทศ หรือเหตุการณ์ด้านความปลอดภัยอื่นๆ และต้องให้ความร่วมมือใน

การปฏิบัติตามมาตรการต่างๆที่ทางแผนกไอทีได้กำหนดไว้อย่างสม่ำเสมอ อีกทั้งผู้บริหารจะต้องให้ความสำคัญในแผนการพัฒนาระบบ การกำหนดบทบาทหน้าที่ความรับผิดชอบอย่างชัดเจน

การเก็บรักษาข้อมูล

(1) แผนกไอทีมีหน้าที่สอบถามความประสงค์ในการใช้ข้อมูล เพื่อนำมาจัดทำมาตรฐานและข้อกำหนดในการเก็บรักษาข้อมูลที่จะนำมาใช้ภายในบริษัทฯ

(2) การจัดประเภทของข้อมูลรวมถึงเอกสารบันทึกลูกค้า ข้อมูลการทำธุรกรรม ข้อความอีเมล ต้องจัดระเบียบข้อมูล เพื่อให้สามารถนำมาใช้ภายหลังได้อย่างสะดวก

(3) การเก็บรักษาข้อมูลควรระบุประเภทข้อมูลที่ธุรกิจต้องเก็บรักษา และระยะเวลาการเก็บรักษา การสร้างพื้นที่จัดเก็บเพิ่มขึ้น ในกรณีที่พื้นที่จัดเก็บมีแนวโน้มจะไม่เพียงพอ

การสร้างความปลอดภัยของระบบสารสนเทศด้านบุคลากร

เพื่อให้ผู้ใช้งานเข้าใจ นโยบาย หน้าที่ และ ความรับผิดชอบ ในการใช้งานระบบสารสนเทศของบริษัทฯ

(1) ต้องกำหนดหน้าที่ และ ความรับผิดชอบ ด้านความปลอดภัยระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร สำหรับบุคคล หรือ หน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน

(2) ต้องให้ผู้ใช้งานและหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

(3) หลังจากมีการเปลี่ยนแปลง หรือ ยกเลิกการจ้างงาน หรือ สิ้นสุดโครงการ ต้องยกเลิกการเข้าถึงข้อมูลในระบบสารสนเทศทันที

การกำหนดช่องทางการแจ้งเบาะแส

หากพบเห็นมีข้อสงสัย หรือ รับทราบข้อมูลใดๆ ที่เกี่ยวกับการกระทำผิดในด้านระบบสารสนเทศภัยคุกคามฯ การโจรกรรมข้อมูลที่เกี่ยวข้องสามารถแจ้งมายังแผนกไอที ซึ่งเป็นผู้ดูแลระบบโดยตรงของบริษัทให้รับทราบ เพื่อดำเนินการตรวจสอบต่อไป

……..