UNIVENTURES

นโยบายรักษาความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศ

ประกาศ
เรื่อง นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัท ยูนิเวนเจอร์ จำกัด (มหาชน) (“บริษัท” หรือ “UV”) จัดเตรียมระบบเทคโนโลยีสารสนเทศ (“ระบบไอที”) ซึ่งประกอบด้วย ระบบงาน ระบบเครือข่าย และระบบข้อมูลของบริษัทและบริษัทย่อย (รวมเรียกว่า “กลุ่มบริษัท”) ตลอดจนเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง เพื่อให้พนักงานของกลุ่มบริษัทใช้ในการทำงานตามหน้าที่ที่ได้รับมอบหมาย เพิ่มความสะดวกรวดเร็วในการทำงาน ใช้ในการค้นหาข้อมูลและติดต่อสื่อสารทั้งภายในและภายนอกองค์กร ทั้งนี้ เพื่อให้การใช้งานระบบไอทีของกลุ่มบริษัทเป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และเกิดประโยชน์สูงสุด บริษัทจึงจัดทำนโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (“นโยบาย IT Security”) ของกลุ่มบริษัทขึ้น รายละเอียดดังนี้

1. วัตถุประสงค์ของการใช้นโยบาย
    - 1.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบไอทีของกลุ่มบริษัท
    - 1.2 เพื่อให้ใช้งานระบบไอทีของกลุ่มบริษัทได้อย่างมีประสิทธิภาพและประสิทธิผลสูงสุด
    - 1.3 เพื่อเผยแพร่ให้พนักงานทุกคนของกลุ่มบริษัทรับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด
    - 1.4 เพื่อกำหนดมาตรฐาน แนวปฏิบัติ และวิธีปฏิบัติให้แก่ผู้บริหารและพนักงานผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกลุ่มบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบไอทีของกลุ่มบริษัท
2. นโยบายการรักษาความมั่นคงปลอดภัยระบบไอทีฉบับนี้ กำหนดประเด็นสำคัญไว้ดังนี้
    - 2.1 การควบคุมการเข้าถึงและการรักษาความปลอดภัย
        - 2.1.1 การควบคุมการเข้าถึงและการใช้งานระบบไอที
        - 2.1.2 การบริหารจัดการสิทธิในการเข้าถึง
        - 2.1.3 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
        - 2.1.4 การควบคุมการเข้าถึงห้องเซิร์ฟเวอร์
        - 2.1.5 การรักษาความปลอดภัยของห้องเซิร์ฟเวอร์
        - 2.1.6 การบริหารจัดการด้านความมั่นคงปลอดภัยของระบบเครือข่าย
        - 2.1.7 การบริหารจัดการด้านความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย
        - 2.1.8 การควบคุมการเข้าถึงระบบปฏิบัติการ โปรแกรมประยุกต์ และโปรแกรมอรรถประโยชน์
        - 2.1.9 การรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์
        - 2.1.10 หน้าที่ความรับผิดชอบของผู้ใช้งาน
    - 2.2 การสำรองข้อมูลและการเตรียมความพร้อมรับมือกับสถานการณ์ฉุกเฉินและภัยคุกคามทางไซเบอร์
        - 2.2.1 การจัดทำระบบสำรองข้อมูลที่สำคัญในระบบไอที
        - 2.2.2 สถานที่ในการจัดเก็บสำรองข้อมูล
        - 2.2.3 การกำหนดรอบระยะเวลาในการสำรองข้อมูล และการตรวจสอบ
        - 2.2.4 การทดสอบระบบสำรองข้อมูล
        - 2.2.5 การกำหนดหน้าที่ความรับผิดชอบของผู้ดูแลระบบการสำรองข้อมูล
        - 2.2.6 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานต่อข้อมูล
        - 2.2.7 การจัดเตรียมความพร้อมต่อสถานการณ์ฉุกเฉิน
        - 2.2.8 การกำหนดหน้าที่ความรับผิดชอบของทีมบริหารสถานการณ์ฉุกเฉิน
        - 2.2.9 การรับมือต่อภัยคุกคามทางไซเบอร์
        - 2.2.10 การกำหนดหน้าที่ความรับผิดชอบของทีมรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์

2.3 การตรวจสอบ การประเมินความเสี่ยง และการควบคุมข้อมูลภายใน

2.4 การสร้างความตระหนักและระเบียบการรักษาความมั่นคงปลอดภัยในระบบไอทีของกลุ่มบริษัท

2.5 การปฏิบัติเกี่ยวกับโปรแกรมคอมพิวเตอร์ที่กลุ่มบริษัทหรือพนักงานจัดหา สร้างสรรค์ พัฒนา

3. การกำหนดผู้รับผิดชอบ

3.1 กำหนดให้ผู้บริหารสูงสุดของกลุ่มบริษัทเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือระบบข้อมูลสารสนเทศเกิดความเสียหาย หรือเกิดอันตรายใดๆ แก่กลุ่มบริษัทหรือผู้ใด เนื่องจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายฉบับนี้

3.2 กำหนดให้ผู้บริหารระดับสูงฝ่ายเทคโนโลยีสารสนเทศของกลุ่มบริษัท เป็นผู้รับผิดชอบในการสั่งการตามนโยบาย IT Security ของกลุ่มบริษัท

3.3 กำหนดให้ผู้อำนวยการ ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบติดตาม กำกับดูแล มอบหมายงานตามนโยบาย IT Security นี้

3.4 กำหนดให้ฝ่ายเทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย เป็นผู้ควบคุมตรวจสอบหรือให้คำเสนอแนะแก่พนักงานระดับปฏิบัติการหรือผู้หรือผู้ที่ได้รับระบบไอทีของกลุ่มบริษัท เพื่อให้การปฏิบัติตามนโยบายฉบับนี้เป็นไปอย่างมีประสิทธิภาพ ทั้งนี้ กำหนดให้มีการทบทวนนโยบายและแนวปฏิบัติอย่างน้อยปีละ 1 ครั้ง และหากมีการเปลี่ยนแปลง ให้ประกาศให้พนักงานกลุ่มบริษัทรับทราบทุกครั้ง

4. เพื่อให้เกิดความตระหนักในภัยคุกคามทางไซเบอร์และผลกระทบที่เกิดจากการใช้งานระบบไอทีโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ กำหนดให้ฝ่ายเทคโนโลยีสารสนเทศสร้างความรู้ความเข้าใจแก่พนักงานกลุ่มบริษัท ดังนี้

4.1 จัดอบรมให้ความรู้ความเข้าใจในหน้าที่ความรับผิดชอบของพนักงานหรือผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยในระบบไอทีของกลุ่มบริษัท

4.2 เผยแพร่นโยบายฉบับนี้ทางอินทราเน็ตของกลุ่มบริษัทเพื่อให้พนักงานทุกคนสามารถเข้าถึงได้

5. นโยบายฉบับนี้ถือเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยระบบไอทีของกลุ่มบริษัท เพื่อใช้เป็นแนวทางสำหรับการดำเนินงานต่างๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของกลุ่มบริษัทเกิดความปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง ทั้งนี้ กำหนดให้กลุ่มบริษัทและพนักงานกลุ่มบริษัททุกคนต้องถือปฏิบัติอย่างเคร่งครัด

ทั้งนี้ ให้ถือปฏิบัติตั้งแต่วันที่ในประกาศนี้เป็นต้นไป

ประกาศ ณ วันที่ 4 กันยายน 2567

-นายกำพล ปุญโสณี-

(นายกำพล ปุญโสณี)
กรรมการผู้จัดการใหญ่

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัทจัดให้มีนโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (นโยบาย IT Security) ของกลุ่มบริษัทขึ้น เพื่อควบคุมดูแลและกำหนดมาตรฐานสำหรับการใช้งานระบบไอที เพื่อให้กลุ่มบริษัทและพนักงานของกลุ่มบริษัทถือปฏิบัติ ดังนี้

หมวด 1 การควบคุมการเข้าถึงและการรักษาความปลอดภัย

ข้อ 1.1 การเข้าใช้งานระบบไอทีของกลุ่มบริษัท ต้องมีการควบคุม จำกัดสิทธิในการเข้าถึง จากฝ่ายเทคโนโลยีสารสนเทศ ("ฝ่ายไอที") โดยให้เป็นไปตามความจำเป็นในการดำเนินงาน มีความเหมาะสมแบบเป็นลำดับขั้นและตามสิทธิที่พึงมีในการเข้าถึงเท่านั้น ตลอดจนมีการดูแล จัดเก็บ ป้องกันระบบงานและข้อมูลที่สำคัญตามนโยบายดังกล่าวนี้ รวมทั้งถูกต้องตามกฎหมายที่เกี่ยวข้องและมีการเก็บหลักฐานการร้องขอสิทธิ สามารถตรวจสอบได้

ข้อ 1.2 การเข้าสู่ระบบไอทีของกลุ่มบริษัท ต้องมีการลงทะเบียนผู้ใช้งาน ซึ่งผ่านการพิสูจน์ตัวตน โดยการใช้บัญชีชื่อและรหัสผ่านในโดเมนบริษัทของตนเองเท่านั้น ห้ามมิให้พนักงานใช้ชื่อบัญชีชื่อของตนเองในโดเมนร่วมกับพนักงานผู้อื่น และต้องมีการกำหนดรหัสผ่านอย่างปลอดภัย เพื่อให้สามารถยืนยันตัวตนในการใช้ระบบงาน สามารถระบุผู้รับผิดชอบต่อการบันทึกรายการนั้นๆ ในระบบงานได้ และใช้เพื่อกำหนดการเข้าถึงข้อมูลแบบเป็นลำดับขั้นตามสิทธิที่พึงมีในการเข้าถึง ตลอดจนใช้เพื่อระบุตัวตนในการใช้งานเส้นทางจราจรในระบบเครือข่ายของกลุ่มบริษัท

ข้อ 1.3 การเข้าถึงข้อมูลตามระดับชั้นความสำคัญและการจัดเก็บข้อมูลสารสนเทศในระบบงาน ต้องมีการจัดลำดับชั้นความสำคัญ มีการแบ่งประเภทของข้อมูลออกตามหน้าที่ ภารกิจ ฝ่ายงานหรือหน่วยงาน มีการกำหนดวิธีการบริหารจัดการและการดูแลปกป้องข้อมูลแต่ละประเภท รวมถึงการเข้าถึงและดูแลปกป้องข้อมูลส่วนบุคคลที่มีความอ่อนไหว (ตามคำนิยามในกฎหมายคุ้มครองข้อมูลส่วนบุคคล) และให้มีการกำหนดขั้นตอนและวิธีปฏิบัติกับข้อมูลสำคัญ ก่อนการจำหน่ายออก หรือการเปลี่ยน หรือนำอุปกรณ์กลับมาใช้งานใหม่

ข้อ 1.4 การควบคุมการเข้าถึงห้องเซิร์ฟเวอร์ เพื่อควบคุมรักษาความปลอดภัยของระบบงาน ระบบเครือข่าย และข้อมูลของกลุ่มบริษัท โดยกำหนดให้จำกัดการเข้าถึงห้องที่มีการติดตั้ง และจัดเก็บอุปกรณ์ที่ใช้ในระบบเครือข่าย หรืออุปกรณ์ที่ใช้กับระบบไอทีของกลุ่มบริษัท ในกรณีผู้ไม่มีหน้าที่เกี่ยวข้องจำเป็นต้องเข้าถึงห้องดังกล่าว จะต้องมีการจัดเก็บบันทึกรายชื่อ เวลา และระบุเหตุผลที่ต้องเข้าสู่พื้นที่ดังกล่าว เพื่อใช้ในการตรวจสอบในภายหลังได้ และต้องมีผู้มีหน้าที่รับผิดชอบห้องเซิร์ฟเวอร์เป็นผู้คอยดูแลควบคุมการเข้าเยือนในพื้นที่ดังกล่าว

ข้อ 1.5 การรักษาความปลอดภัยของห้องเซิร์ฟเวอร์ กำหนดให้มีการติดตั้งระบบดับเพลิงชนิดที่ใช้กับอุปกรณ์คอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ในห้องดังกล่าว เพื่อทำความเสียหายต่ออุปกรณ์ให้น้อยที่สุดเมื่อมีความจำเป็นต้องใช้งาน มีการติดตั้งระบบสำรองเครื่องปรับอากาศ และระบบสำรองไฟฟ้าฉุกเฉินให้เพียงพอตามระดับความสำคัญของระบบงานต่างๆ และกำหนดให้มีรอบการบำรุงรักษาอุปกรณ์ เพื่อให้ระบบงานและระบบเครือข่ายสามารถให้บริการได้อย่างต่อเนื่อง

ข้อ 1.6 การควบคุมการเข้าถึงเครือข่ายทั้งจากเครือข่ายภายในและเครือข่ายภายนอก กำหนดให้ผู้ที่จะเข้าใช้งานต้องได้รับการอนุมัติจากฝ่ายไอทีก่อน ต้องมีขั้นตอนการพิสูจน์ยืนยันตัวตน (Authentication) โดยมีการใส่บัญชีชื่อ (Username) เพื่อแสดงตัวตนด้วยชื่อผู้ใช้งานและใส่รหัสผ่านในโดเมนก่อนเข้าใช้งาน และให้มีการบังคับเส้นทางเชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัทกับระบบอินเทอร์เน็ตให้ผ่านระบบควบคุม ระบบตรวจสอบ และระบบรักษาความปลอดภัยตามที่กลุ่มบริษัทกำหนด และมีการออกแบบระบบเครือข่ายโดยแบ่งเขตแดน (Zone) ในการใช้งานเพื่อให้สามารถป้องกันภัยคุกคามได้อย่างปลอดภัย มีประสิทธิภาพ และสามารถตรวจสอบได้ในกรณีที่มีเหตุการณ์ผิดปกติเกิดขึ้น

ข้อ 1.7 การควบคุมการเข้าถึงเครือข่ายไร้สาย เพื่อป้องกันการเข้าถึงระบบไอทีของกลุ่มบริษัท ต้องมีขั้นตอนการพิสูจน์ยืนยันตัวตน (Authentication) โดยมีการใส่บัญชีชื่อ (Username) เพื่อแสดงตัวตนด้วยชื่อผู้ใช้งาน และใส่รหัสผ่านในโดเมนก่อนเข้าใช้งาน หรือในกรณีเป็นผู้มาติดต่องานกับกลุ่มบริษัท (Guest) จำเป็นต้องมีการขออนุมัติใช้งาน ผ่านระบบลงทะเบียนขอใช้งานระบบเครือข่ายไร้สายของกลุ่มบริษัท (Guest Wi-Fi) หรือการนำ MAC Address (Media Access Control Address) ของอุปกรณ์เชื่อมต่อ มาแจ้งขออนุมัติและทำการลงทะเบียนกับฝ่ายไอทีก่อนนำไปใช้งาน

ข้อ 1.8 การควบคุมการเข้าถึงระบบงาน ระบบปฏิบัติการ โปรแกรมประยุกต์ และโปรแกรมอรรถประโยชน์ต่างๆ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต กำหนดให้ผู้ที่จะเข้าใช้งานต้องได้รับการอนุมัติจากฝ่ายไอทีก่อน ต้องมีขั้นตอนในการพิสูจน์ยืนยันตัวตน (Authentication) โดยมีการใส่บัญชีชื่อ (Username) เพื่อแสดงตัวตนด้วยชื่อผู้ใช้งาน และใส่รหัสผ่านก่อนเข้าใช้งาน โดยการเข้าถึงระบบงานที่สำคัญ ต้องให้สิทธิเฉพาะการปฏิบัติงานในขอบเขตหน้าที่ โดยได้รับอนุมัติจากผู้บังคับบัญชา หรือผู้มีสิทธิในการอนุมัติเป็นลายลักษณ์อักษร หรือร้องขอสิทธิจากระบบแจ้งร้องขอสิทธิของกลุ่มบริษัท เพื่อบันทึกไว้เป็นหลักฐานในการตรวจสอบ และให้มีการทบทวนสิทธิที่ได้รับอย่างสม่ำเสมอ และสำหรับคอมพิวเตอร์ของกลุ่มบริษัทที่มีการเชื่อมต่อกับระบบอินเทอร์เน็ต ให้มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ หรือมีการบังคับเส้นทางเชื่อมต่อกับระบบอินเทอร์เน็ตให้ผ่านระบบควบคุม ระบบตรวจสอบ และระบบรักษาความปลอดภัยตามที่กลุ่มบริษัทกำหนด

ข้อ 1.9 กำหนดให้มีการรักษาความมั่นคงปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ (อีเมล) ของกลุ่มบริษัท มีการกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งานในการใช้ระบบอีเมลของกลุ่มบริษัท โดยพนักงานต้องใช้ระบบอีเมลของกลุ่มบริษัทเท่านั้นในการติดต่องานที่เกี่ยวข้องกับภารกิจของกลุ่มบริษัท และกำหนดให้มีการกำหนดข้อห้าม ข้อควรระวังตลอดจนสิทธิในการใช้งานโดยฝ่ายไอที โดยคำนึงถึงความมั่นคงปลอดภัยของระบบไอทีของกลุ่มบริษัท

ข้อ 1.10 เพื่อการป้องกันการเข้าถึงระบบไอทีของกลุ่มบริษัทโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยข้อมูล กำหนดให้พนักงานของกลุ่มบริษัทมีหน้าที่รับผิดชอบในการตั้งและเปลี่ยนค่ารหัสผ่านสำหรับการเข้าสู่ระบบไอทีของกลุ่มบริษัทให้ถูกต้องตามนโยบายควบคุมของฝ่ายไอที ไม่เปิดหน้าจอเครื่องคอมพิวเตอร์ค้างไว้ โดยไม่มีการป้องกันผู้อื่นเข้ามาใช้งานแทน ตลอดจนการเก็บรักษาดูแลสินทรัพย์ในระบบไอทีของกลุ่มบริษัทไว้ในที่ปลอดภัย เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีนำสินทรัพย์ดังกล่าวไปใช้ในทางที่ทำให้เกิดความเสียหายต่อกลุ่มบริษัทได้

<u>หมวด 2 การสำรองข้อมูลและการเตรียมความพร้อมรับมือกับสถานการณ์ฉุกเฉินและภัยคุกคามทางไซเบอร์</u>

ข้อ 2.1 กำหนดให้มีการจัดทำระบบสำรองข้อมูลที่สำคัญในระบบไอทีของกลุ่มบริษัท เพื่อสามารถให้บริการได้อย่างต่อเนื่อง มีเสถียรภาพ มีความปลอดภัย มีการตรวจสอบและดูแลระบบสำรองให้อยู่ในสภาพที่พร้อมนำมาใช้งานได้อยู่เสมอ โดยเรียงลำดับความสำคัญในการสำรองข้อมูลในระบบไอทีของกลุ่มบริษัทตามความจำเป็น จากมากไปน้อย มีการกำหนดหน้าที่ความรับผิดชอบให้กับเจ้าหน้าที่ผู้ตรวจสอบและดูแลระบบการสำรองข้อมูล

ข้อ 2.2 การสำรองข้อมูลในระบบงานที่สำคัญในระบบไอทีของกลุ่มบริษัท กำหนดให้มีการสำรองข้อมูลเป็นประจำ โดยพิจารณาจำนวนรอบในการสำรองข้อมูล วิธีการ และเทคโนโลยีที่นำมาใช้ในการสำรองข้อมูลให้เหมาะสมกับความสำคัญของข้อมูลในระบบงานของกลุ่มบริษัท ตลอดจนพิจารณาจัดเก็บระบบงานและข้อมูลที่สำคัญของกลุ่มบริษัทไว้ให้พร้อมใช้งาน ณ สถานที่ปลอดภัยอีกแห่งหนึ่งแทน และให้จัดทำแผนเตรียมความพร้อมในสถานการณ์ฉุกเฉิน (IT Contingency Plan) และจัดเตรียมระบบประมวลผลสำรองรองรับ เพื่อให้ธุรกรรมหลักของกลุ่มบริษัทสามารถดำเนินต่อไปได้อย่างต่อเนื่อง

ข้อ 2.3 ให้ฝ่ายไอทีหรือให้ตกลงกับหน่วยงานเจ้าของข้อมูลในการกำหนดรอบระยะเวลาการสำรองข้อมูล ระยะเวลาในการจัดเก็บรักษาข้อมูล ซึ่งต้องมั่นใจได้ว่าข้อมูลและฐานข้อมูลของกลุ่มบริษัทได้มีการสำรองข้อมูลอย่างสม่ำเสมอ ครบถ้วน และต่อเนื่อง พร้อมที่จะนำกลับมาใช้งานภายในเวลาที่กำหนดไว้ เมื่อเกิดเหตุการณ์ฉุกเฉินขึ้น

ข้อ 2.4 มีการกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ฝ่ายไอทีในการสำรองข้อมูล ตรวจสอบข้อมูลที่สำรอง และการกู้คืนข้อมูล รวมถึงหน้าที่ในการประเมินและทบทวนแผนเตรียมความพร้อมกรณีเกิดสถานการณ์ฉุกเฉิน ตลอดจนมีการกำหนดหน้าที่ความรับผิดชอบและวิธีปฏิบัติในการจัดการกับสถานการณ์ฉุกเฉินที่เกิดขึ้น โดยการเข้าถึงข้อมูลสำรองของกลุ่มบริษัทและการเรียกข้อมูลกลับมาใช้งาน ให้กระทำโดยผู้ได้รับอนุญาตจากกลุ่มบริษัทและผู้ดูแลระบบงานเท่านั้น

ข้อ 2.5 สื่อและระบบที่ใช้ในการเก็บสำรองข้อมูลและฐานข้อมูลที่สำคัญของกลุ่มบริษัท ต้องมีการทดสอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง และรายงานผลทดสอบให้กับทางผู้บริหารระดับสูงของฝ่ายไอทีรับทราบ เพื่อให้มั่นใจว่าจะสามารถนำระบบงานและข้อมูลกลับมาใช้งานได้ตลอดเวลาหรือเมื่อเกิดสถานการณ์ฉุกเฉินขึ้น

ข้อ 2.6 พนักงานของกลุ่มบริษัทมีหน้าที่รับผิดชอบในการไม่สำรองข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการปฏิบัติงานของกลุ่มบริษัทลงในระบบข้อมูลของกลุ่มบริษัท ตลอดจนการเก็บรักษาข้อมูลของกลุ่มบริษัทไว้ในที่ที่กำหนดไว้อย่างปลอดภัย เพื่อให้ระบบสำรองข้อมูลสามารถกู้คืนข้อมูลของกลุ่มบริษัทกลับมาได้ และป้องกันไม่ให้ผู้ไม่ประสงค์ดีนำข้อมูลดังกล่าวไปใช้ในทางที่ทำให้เกิดความเสียหายต่อกลุ่มบริษัท

ข้อ 2.7 กำหนดให้จัดทำแผนบริหารความต่อเนื่องและการกู้คืนระบบเทคโนโลยีสารสนเทศจากเหตุภัยพิบัติ (Business Continuity Plan and Disaster Recovery Plan for Information Technology Systems) เพื่อเป็นแนวทางปฏิบัติ รวมถึงการจัดเตรียมระบบประมวลผลสำรองและทรัพยากรที่จำเป็นต้องใช้ในการเชื่อมต่อเข้าสู่เครือข่ายหลักและเครือข่ายสำรอง เพื่อให้ธุรกรรมหลักของกลุ่มบริษัทสามารถดำเนินงานต่อไปได้อย่างต่อเนื่อง

ข้อ 2.8 เพื่อตอบสนองต่อสถานการณ์ฉุกเฉินของระบบไอทีที่มีผลกระทบต่อการดำเนินธุรกิจของกลุ่มบริษัท กำหนดให้มีการจัดตั้งคณะทำงานและบุคลากรเพื่อทำหน้าที่บริหารจัดการเมื่อเกิดสถานการณ์ฉุกเฉินขึ้น โดยมีการกำหนดบทบาท ความรับผิดชอบ ขั้นตอนดำเนินการที่จำเป็น และวิธีการสื่อสารที่ชัดเจน เพื่อปฏิบัติตามแผนที่จัดเตรียมไว้

ข้อ 2.9 กำหนดให้จัดทำแผนรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) และพัฒนาแผนให้ครอบคลุมทั้งข้อมูลสารสนเทศ รวมถึงองค์ประกอบโครงสร้างพื้นฐานของระบบงานและระบบเครือข่ายที่สำคัญและพึงต้องมีตามกิจกรรมทางธุรกิจหลักของกลุ่มบริษัท และต้องมีการซ้อมและทบทวนเป็นประจำทุกปี เพื่อให้มั่นใจว่าจะสามารถนำไปใช้ในสถานการณ์จริงได้อย่างมีประสิทธิภาพ โดยฝ่ายบริหารและพนักงานที่เกี่ยวข้องต้องรับทราบและเข้าใจวิธีดำเนินการตามที่กำหนด

ข้อ 2.10 เพื่อตอบสนองต่อเหตุการณ์ที่เป็นภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ กำหนดให้มีการจัดตั้งคณะทำงานและบุคลากรเพื่อทำหน้าที่รับมือและตอบสนองต่อเหตุโจมตีทางไซเบอร์ โดยมีการกำหนดบทบาท ความรับผิดชอบ ขั้นตอนดำเนินการที่จำเป็น และวิธีการสื่อสารที่ชัดเจน เพื่อให้พนักงานที่มีส่วนเกี่ยวข้องเข้าใจในบทบาทหน้าที่ของตนเอง เพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างถูกต้องและรวดเร็วเมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้น

<u>หมวด 3 การตรวจสอบ การประเมินความเสี่ยง และการควบคุมข้อมูลภายใน</u>

"ข้อมูลภายใน" หมายถึง ข้อมูลความลับทางธุรกิจของกลุ่มบริษัท หรือข้อมูลสำคัญของกลุ่มบริษัทที่ยังไม่เปิดเผยต่อสาธารณะหรือตลาดหลักทรัพย์แห่งประเทศไทย และมีผลต่อราคาหุ้นของบริษัทหรือมีผลต่อการตัดสินใจซื้อขายหุ้นของบริษัท ซึ่งบุคลากรของกลุ่มบริษัทและผู้ที่เกี่ยวข้องได้ล่วงรู้ข้อมูลดังกล่าวจากตำแหน่ง หรือจากฐานะที่สามารถล่วงรู้ข้อเท็จจริง หรือจากการเป็นพนักงานของกลุ่มบริษัท

ข้อ 3.1 บริษัทกำหนดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท โดยจัดให้มีผู้ตรวจสอบภายในของกลุ่มบริษัท หรือผู้ตรวจสอบอิสระจากภายนอก (External Auditor) อย่างน้อยปีละ 1 ครั้ง เพื่อให้บริษัทและหน่วยงานได้รับทราบถึงระดับความเสี่ยงและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท

ข้อ 3.2 บริษัทกำหนดให้ทุกหน่วยงานจัดระบบงาน สถานที่ปฏิบัติงาน เพื่อเก็บรักษาข้อมูลภายในของกลุ่มบริษัท ไม่ให้ข้อมูลเหล่านั้นถูกเปิดเผยไปยังบุคคลที่ไม่เกี่ยวข้อง หรือไม่จำเป็นต้องล่วงรู้ และการใช้ข้อมูลภายในหรือการส่งข้อมูลภายในให้กระทำโดยผู้มีหน้าที่รับผิดชอบหรือได้รับอนุญาตจากผู้มีอำนาจอนุมัติเท่านั้น

ข้อ 3.3 ห้ามพนักงานที่ปฏิบัติงานเกี่ยวข้องกับข้อมูลภายในของกลุ่มบริษัท เปิดเผยข้อมูลภายในไม่ว่าทางตรงหรือทางอ้อมแก่บุคคลใดๆ เว้นแต่จะได้รับมอบหมายเป็นหน้าที่รับผิดชอบและได้รับอนุญาตจากผู้มีอำนาจอนุมัติเท่านั้น

<u>หมวด 4 การสร้างความตระหนักและระเบียบการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ</u>

ข้อ 4.1 จัดอบรมแนวปฏิบัติตามนโยบาย IT Security ของกลุ่มบริษัทแก่พนักงานอย่างสม่ำเสมอ และให้ความรู้ด้านกฎหมายและกฎระเบียบที่เกี่ยวข้องกับการใช้งาน

ข้อ 4.2 เผยแพร่นโยบาย IT Security ของกลุ่มบริษัททางอินทราเน็ตของกลุ่มบริษัท เพื่อให้พนักงานกลุ่มบริษัททุกคนสามารถเข้าถึงได้โดยสะดวก

ข้อ 4.3 จัดให้มีมาตรการเชิงป้องกัน โดยการให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะวิธีใช้ ข้อควรระวังในการใช้งานระบบไอทีของกลุ่มบริษัท รวมถึงกำหนดบทลงโทษแก่พนักงาน เมื่อพบว่ามีการกระทำผิด หรือมีการใช้งานระบบไอทีที่ไม่ถูกต้อง เช่น การระงับการเข้าถึงหรือการระงับสิทธิในการใช้งาน

ข้อ 4.4 พนักงานมีหน้าที่ต้องรับผิดชอบดำเนินการให้เป็นไปตามนโยบายที่กำหนดขึ้นนี้อย่างเคร่งครัด ผู้ที่ฝ่าฝืนไม่ปฏิบัติตามนโยบายฉบับนี้ไม่ว่าข้อหนึ่งข้อใด หรือละเมิดลิขสิทธิ์ในการใช้โปรแกรมคอมพิวเตอร์ของกลุ่มบริษัท เพื่อผลประโยชน์ของตนเอง หรือบุคคลอื่นนอกเหนือจากภาระหน้าที่รับผิดชอบของตนหรือเพื่อผลประโยชน์ของกลุ่มบริษัท ถือเป็นการผิดวินัยพนักงาน

ข้อ 4.5 กรณีที่เครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ใดๆ เกิดความเสียหาย หรือสูญหาย ให้พนักงานผู้ใช้งาน ผู้รับผิดชอบครอบครองหรือผู้ได้รับมอบหมาย แจ้งให้ผู้บริหารหรือบุคคลที่ได้รับมอบหมายให้ทำหน้าที่แทนทราบโดยทันที เพื่อดำเนินการแก้ไขหรือบรรเทาความเสียหายต่อไป

<u>หมวด 5 การปฏิบัติเกี่ยวกับโปรแกรมคอมพิวเตอร์ที่กลุ่มบริษัทหรือพนักงานจัดหา สร้างสรรค์ พัฒนา</u>

ข้อ 5.1 การสร้างสรรค์หรือพัฒนาโปรแกรมเพื่อนำมาใช้งานของกลุ่มบริษัท จะต้องได้รับการพิจารณาเห็นชอบเป็นลายลักษณ์อักษรจากผู้บริหารหรือผู้มีอำนาจที่ได้รับมอบหมายจากกลุ่มบริษัท

ข้อ 5.2 โปรแกรมคอมพิวเตอร์ที่พนักงานได้สร้างสรรค์หรือพัฒนาขึ้นในฐานะพนักงานของกลุ่มบริษัท ให้ลิขสิทธิ์โปรแกรมคอมพิวเตอร์นั้นเป็นของกลุ่มบริษัท

<u>หมายเหตุ</u> กำหนดให้แนวปฏิบัติหรือระเบียบต่าง ๆ ที่เกี่ยวข้องหรือเกี่ยวเนื่องกับนโยบาย IT Security ฉบับนี้ถือเป็นส่วนหนึ่งของนโยบายฉบับนี้

****