10. การควบคุมภายใน

บริษัทฯ ตระหนักถึงความสำคัญของระบบการควบคุมภายในที่ดี และเป็นไปตามหลักกำกับดูแลกิจการที่ดี กล่าวคือดูแลการปฏิบัติงานในหน้าที่ต่างๆ ให้มีความโปร่งใส ยุติธรรม และเชื่อถือได้ อันนำไปสู่ประโยชน์สูงสุดต่อผู้ถือหุ้น พนักงาน และผู้ที่เกี่ยวข้องทุกฝ่าย นอกจากนี้ในที่ประชุมวิสามัญผู้ถือหุ้นของบริษัทฯ ครั้งที่ 1/2556 เมื่อวันที่ 1 กุมภาพันธ์ 2556 ได้มีมติแต่งตั้งคณะกรรมการตรวจสอบจำนวน 3 ท่าน เพื่อสอบทานความเพียงพอและประสิทธิผลของระบบการควบคุมภายในของบริษัทฯ รวมทั้งสอบทานให้การดำเนินธุรกิจของบริษัทฯ เป็นไปตามกฎหมายหลักทรัพย์ที่เกี่ยวข้อง กฎเกณฑ์ของตลาดหลักทรัพย์ และกฎหมายอื่นใดที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัทฯ

บริษัทฯ ได้แต่งตั้งบริษัท เคพีเอ็มจี ภูมิไชย ที่ปรึกษาธุรกิจ จำกัด ("ผู้ตรวจสอบภายใน") เพื่อทำการประเมินความเพียงพอของระบบการควบคุมภายในของกลุ่มบริษัทฯ ซึ่งผู้ตรวจสอบภายใน ได้จัดทำรายงานผลการประเมินความเพียงพอ และประสิทธิผลของระบบควบคุมภายในของบริษัทฯ ฉบับลงวันที่ 23 พฤษภาคม 2555 และจัดทำรายงานแผนปฏิบัติการที่สำคัญจากข้อสังเกตในรายงานการประเมินการควบคุมภายในลงวันที่ 9 พฤศจิกายน 2555 ซึ่งที่ประชุมคณะกรรมการตรวจสอบของบริษัทฯ ครั้งที่ 1/2556 เมื่อวันที่ 18 กุมภาพันธ์ 2556 ได้มีมติพิจารณาและอนุมัติ รายงานดังกล่าว (รายละเอียดปรากฏในตารางด้านล่าง)

รายงานผลการประเมินความเพียงพอ และประสิทธิผลของระบบควบคุมภายในฉบับลงวันที่ 23 พฤษภาคม 2555 ซึ่งประเมินตามแนวทางการควบคุมของ COSO (The Committee of Sponsoring Organization of the Treadway Commission) โดยการประเมินแบ่งออกเป็น 5 ส่วน ดังนี้ (1) องค์กรและสภาพแวดล้อม (2) การบริหารความเสี่ยง (3) การควบคุมการปฏิบัติงานของฝ่ายบริหาร (4) ระบบสารสนเทศและการสื่อสารข้อมูล และ (5) ระบบการติดตาม

ประเด็น	ข้อสังเกต และข้อเสนอแนะ	ผลการตรวจ ติดตามการปรับปรุงโดยบริษัทฯ
1. องค์กรและสภาพแวดล้อม		
1.1. ควรมีการสอบทานโครงสร้างองค์กรและจัดให้มีการเผยแพร่โครงสร้างดังกล่าวให้แก่บุคคลที่เกี่ยวข้องทราบ	▪ บริษัทฯ ควรจัดให้มีการทบทวนโครงสร้างองค์กรเป็นประจำทุกปี เพื่อให้แน่ใจว่าโครงสร้างองค์กรแสดงให้เห็นถึงรูปแบบการประกอบธุรกิจในปัจจุบันอย่างแท้จริง นอกจากนี้ ควรจัดให้มีขั้นตอนการเผยแพร่ และการสื่อสารเกี่ยวกับการเปลี่ยนแปลงของโครงสร้างองค์กรดังกล่าวเพื่อให้บุคคลที่เกี่ยวข้องรับทราบอย่างเหมาะสม	▪ จากการประเมินของผู้ตรวจสอบภายในพบว่า บริษัทฯ ได้มีการทบทวน และจัดทำโครงสร้างองค์กร เพื่อเสนอ และได้รับอนุมัติจากที่ประชุมคณะกรรมการบริษัทฯ ครั้งที่ 3/2556 เมื่อวันที่ 22 พฤษภาคม 2556 และจะดำเนินการให้มีการเผยแพร่โครงสร้างองค์กรดังกล่าวผ่านเว็บไซต์ของบริษัทฯ ฝ่ายทรัพยากรบุคคล และผ่านที่ประชุมต่างๆ ภายในองค์กรอีกด้วย
1.2. ควรจัดให้มีการสื่อสารและเผยแพร่ประมวลจริยธรรมและจรรยาบรรณทางธุรกิจ (Code of Ethics and	▪ บริษัทฯ ควรจัดให้มีการทำประมวลจริยธรรมและจรรยาบรรณทางธุรกิจ และกำหนดให้พนักงานทุกคนลงนาม รับทราบ / ยืนยัน	▪ จากการประเมินของผู้ตรวจสอบภายในพบว่า บริษัทฯ ได้มีการจัดทำร่างนโยบายจริยธรรมทางธุรกิจ และประมวล

ประเด็น	ข้อสังเกต และข้อเสนอแนะ	ผลการตรวจ ติดตามการปรับปรุงโดยบริษัทฯ
Conduct) และความขัดแย้งทางผลประโยชน์ (Conflict of Interest) โดยให้พนักงานที่เกี่ยวข้องทุกคนลงนามรับทราบ	ประมวลดังกล่าว ▪ บริษัทฯ ควรจัดทำแบบรายงานความขัดแย้งทางผลประโยชน์ และกำหนดให้พนักงานทุกคนลงนามยืนยันรับทราบ ▪ ควรมีการรายงานความขัดแย้งทางผลประโยชน์ และรับทราบประมวลจริยธรรมและจรรยาบรรณทางธุรกิจอย่างสม่ำเสมอ ควรกำหนดให้การไม่ปฏิบัติตามนโยบายดังกล่าวเป็นเหตุในการเลิกจ้างได้ ▪ บริษัทฯ ควรจัดให้มีการอบรมเกี่ยวกับระเบียบและกฎเกณฑ์ต่างๆ และประมวลจริยธรรมทางธุรกิจ และความขัดแย้งทางผลประโยชน์ ในวันปฐมนิเทศพนักงานใหม่ หรือการเตรียมความพร้อมในการปฏิบัติงาน	จรรยาบรรณทางธุรกิจ ซึ่งเป็นส่วนหนึ่งของ "Business Ethics & Code of Conduct" หมายเลขนโยบาย: BOD/CCB/01 ▪ บริษัทฯ ได้จัดทำ "Conflict of Interest Declaration Form" หรือแบบแสดงความแย้งทางผลประโยชน์ ซึ่งมีหมายเลขนโยบาย BOD/COI/01 ▪ ทั้งนี้ในเดือน กรกฎาคม 2556 บริษัทฯ ได้ส่งนโยบายจรรยาบรรณทางธุรกิจให้แก่ผู้บริหารและพนักงานอาวุโสทุกราย และดำเนินการให้ผู้บริหารและพนักงานอาวุโสรับทราบนโยบายดังกล่าวเป็นลายลักษณ์อักษร นอกจากนี้ บริษัทฯ ยังมีแผนจะเผยแพร่เอกสารดังกล่าวให้แก่พนักงานอื่นๆ ผ่านผู้บริหารและพนักงานอาวุโส นอกจากนี้บริษัทฯ จะเผยแพร่นโยบายจริยธรรมทางธุรกิจอย่างเป็นทางการที่เว็บไซต์ของบริษัทฯ ซึ่งประชาชนทั่วไปและพนักงานสามารถเข้าดูได้ สำหรับแบบแสดงความขัดแย้งทางผลประโยชน์ บริษัทฯ ได้ดำเนินการส่งแบบฟอร์มดังกล่าวให้แก่ผู้บริหารและพนักงานอาวุโส โดยผู้บริหารและพนักงานอาวุโสดังกล่าวได้กรอกข้อมูลและส่งแบบฟอร์มดังกล่าวกลับมายังแผนกกำกับและดูแลเป็นที่เรียบร้อยแล้ว
2. การบริหารความเสี่ยง		
2.1. ควรอนุมัติและเผยแพร่คู่มือการบริหารจัดการความเสี่ยงแก่พนักงานทุกคน และควรจัดให้มีการบันทึกการประชุม หรือหารือเกี่ยวกับประเด็นความเสี่ยงที่เกี่ยวข้องเป็นเอกสารที่เหมาะสม	▪ บริษัทฯ ควรบันทึกข้อมูลการปรึกษาหารือเกี่ยวกับการประเมินความเสี่ยงไว้เป็นเอกสาร หรือเป็นลายลักษณ์อักษร และแจกจ่ายให้แก่ฝ่ายจัดการ และพนักงานที่เกี่ยวข้องเพื่อให้เกิดความตระหนัก และให้ความรู้แก่พนักงาน ▪ คู่มือการบริหารจัดการความเสี่ยงควรได้รับการอนุมัติจากคณะกรรมการบริษัทฯ และดำเนินการเผยแพร่ให้แก่พนักงานทุกคนทราบ นอกจากนี้ ขั้นตอนการบริหารจัดการความเสี่ยงควรครอบคลุมถึงระดับความรับผิดชอบของพนักงานและกำหนดถึงการมีส่วนร่วมของ	▪ บริษัทฯ มีนโยบายบริหารความเสี่ยง และมีการบริหารความเสี่ยงอย่างเป็นระบบ และชัดเจน และบริษัทฯ จะดำเนินการเสนอต่อที่ประชุมคณะกรรมการตรวจสอบของบริษัทฯ ครั้งที่ 6/2556 ในเดือนสิงหาคม 2556 เพื่อพิจารณาและอนุมัตินโยบาย และแนวทางปฏิบัติการบริหารความเสี่ยงดังกล่าว นอกจากนี้บริษัทฯ จะจัดให้มีการฝึกอบรมพนักงานเกี่ยวกับแนวทางการบริหารความเสี่ยงขององค์กร

ประเด็น	ข้อสังเกต และข้อเสนอแนะ	ผลการตรวจ ติดตามการปรับปรุงโดยบริษัทฯ
	พนักงาน	และรายงานเรื่องการบริหารจัดการความเสี่ยงต่อคณะกรรมการตรวจสอบอย่างสม่ำเสมอ

ในที่ประชุมคณะกรรมการบริษัทฯ ครั้งที่ 3/2556 เมื่อวันที่ 22 พฤษภาคม 2556 ซึ่งมีกรรมการตรวจสอบเข้าร่วมประชุมจำนวน 3 ท่าน ได้มีมติอนุมัติแบบประเมินการควบคุมภายใน โดยอ้างอิงจากข้อมูลที่ได้รับจากการสัมภาษณ์ผู้บริหาร และรายงานแผนปฏิบัติการที่สำคัญจากข้อสังเกตในรายงานการประเมินการควบคุมภายในลงวันที่ 9 พฤศจิกายน 2555 ที่จัดทำโดย บริษัท เคพีเอ็มจี ภูมิไชย ที่ปรึกษาธุรกิจ จำกัด ที่ประชุมมีความเห็นว่าบริษัทฯ มีระบบการควบคุมภายในที่มีประสิทธิภาพและเพียงพอสำหรับขนาด และการดำเนินธุรกิจ และเพียงพอในการป้องกันทรัพย์สินอันเกิดจากที่ผู้บริหารนำไปใช้โดยมิชอบหรือโดยไม่มีอำนาจ (โปรดพิจารณารายละเอียดส่วนที่ 3 แบบประเมินความพอเพียงของระบบการควบคุมภายใน)

นอกจากนี้ บริษัทฯ ได้แต่งตั้ง บริษัท มาซาร์ส จำกัด เพื่อทำหน้าที่ตรวจสอบภายในให้กับบริษัทฯ สำหรับปีบัญชีสิ้นสุดวันที่ 31 ธันวาคม 2556 โดยบริษัท มาซาร์ส จำกัด จะทำการตรวจสอบ ติดตาม และประเมินระบบควบคุมภายในของบริษัทฯ ตามแผนการตรวจสอบรายปีที่ตกลงร่วมกันกับบริษัทฯ และจัดทำรายงานและข้อเสนอแนะ เพื่อปรับปรุงให้เป็นไปตามแผนและนโยบายการควบคุมภายในของบริษัทฯ เพื่อให้เป็นไปตามหลักเกณฑ์ 5 ข้อของ COSO ตามที่ได้กล่าวมาแล้วข้างต้น

นอกจากนี้ ผู้สอบบัญชีจากบริษัท เคพีเอ็มจี ภูมิไชย สอบบัญชี จำกัด ("ผู้สอบบัญชี") ได้ศึกษาและประเมินประสิทธิภาพระบบการควบคุมภายในของบริษัทฯ แล้วไม่พบข้อบกพร่องที่เป็นสาระสำคัญต่อการแสดงความเห็นต่องบการเงินสำหรับปีบัญชีสิ้นสุดวันที่ 31 ธันวาคม 2556 โดยมีรายละเอียดดังนี้

ข้อสังเกต/ข้อเสนอแนะของผู้สอบบัญชี	ความเห็นของผู้บริหาร/การดำเนินการปรับปรุงของบริษัทฯ
1. การใช้งาน และการเข้าถึงโปรแกรม และฐานข้อมูล	
1.1. <u>นโยบายความปลอดภัยของการใช้ข้อมูล และการสื่อสารภายในองค์กร</u> บริษัทฯ ควรเพิ่มเติมนโยบายเกี่ยวกับข้อกำหนดในการตั้งรหัสผ่านสำหรับแอพพลิเคชั่นและระบบโครงสร้างพื้นฐานของระบบสารสนเทศทั้งหมดดังนี้ - รหัสผ่านต้องมี 6 ถึง 8 ตัวอักษร - รหัสผ่านถูกบังคับเปลี่ยนภายใน 60 ถึง 90 วัน - รหัสผ่านต้องประกอบไปด้วย ตัวอักษรอย่างน้อย 1 ตัว ตัวเลข 1 ตำแหน่ง และตัวอักษรหรือสัญลักษณ์พิเศษ 1 ตัว - จำนวนครั้งที่ใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง นอกจากนี้ผู้สอบบัญชีแนะนำว่าควรจัดให้ผู้ใช้งานทุกคนสามารถสื่อสาร ค้นหาและศึกษาเกี่ยวกับนโยบายความปลอดภัยของข้อมูล โดยการเข้าร่วมอบรมปฐมนิเทศระบบข้อมูลสารสนเทศ และบริษัทฯ ควรจัดให้มีระบบ intranet หรือระบบภายในของบริษัทฯ และจดหมายอิเลกทรอนิกส์ เป็นต้น	▪ บริษัทฯ ได้ดำเนินการให้มีการปรับปรุงการกำหนดรหัสผ่านของบริษัทฯ และปัจจัยอื่นๆเกี่ยวข้องกับความปลอดภัยของข้อมูล และดำเนินการเผยแพร่นโยบายดังกล่าวแก่พนักงานทั้งหมดของบริษัทฯ ผ่านจดหมายอิเลกทรอนิกส์ ระบบสื่อสารหรือเวบไซต์ภายในของบริษัทฯ และการอบรมปฐมนิเทศของพนักงานใหม่ ในเดือนกรกฎาคม 2556

ข้อสังเกต/ข้อเสนอแนะของผู้สอบบัญชี	ความเห็นของผู้บริหาร/การดำเนินการปรับปรุงของบริษัทฯ
1.2. <u>การกำหนดรหัสผ่าน</u> บริษัทฯ ควรจัดให้มีการกำหนดรหัสผ่านผู้ใช้งานระบบวางแผนทรัพยากรขององค์กร (Enterprise Resource Planning หรือ ERP) ORION ที่เข้มงวดกว่าข้อกำหนดในปัจจุบัน เพื่อป้องกันความเสี่ยงจากการเข้าระบบจากผู้ใช้ที่ไม่ได้รับอนุญาต โดยมีรายละเอียดดังนี้ - รหัสผ่านต้องมีตัวอักษรอย่างน้อย 6 ถึง 8 ตัวอักษร - จำนวนครั้งที่ใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง - บังคับเปลี่ยนรหัสผ่านเมื่อใช้งานหรือเข้าระบบเป็นครั้งแรก	■ บริษัทฯ อยู่ในระหว่างดำเนินการให้มีการปรับปรุงระบบการกำหนดรหัสผ่านของผู้ใช้งานระบบวางแผนทรัพยากรขององค์กร เนื่องจากระบบวางแผนทรัพยากรขององค์กรในปัจจุบัน ไม่สามารถรองรับการกำหนดรหัสผ่านของผู้ใช้งานได้ ทั้งนี้บริษัทฯ ได้ติดต่อผู้ให้บริการระบบดังกล่าว ดำเนินการปรับปรุงพัฒนาระบบเพื่อให้รองรับการเปลี่ยนแปลงดังกล่าวแล้ว โดยปัจจุบันอยู่ในระหว่างการทดสอบระบบ ซึ่งคาดว่าจะสามารถใช้งานได้ในเดือนกรกฎาคม 2556
1.3. <u>การกำหนดรหัสผ่าน ของระบบปฏิบัติการ Window OS</u> บริษัทฯ ควรจัดทบทวนระบบการกำหนดรหัสผ่านการใช้งานระบบปฏิบัติการ Window OS เพื่อระบบควบคุมที่ดีขึ้น และป้องกันความเสี่ยงจากการเข้าระบบจากผู้ใช้ที่ไม่ได้รับอนุญาต เช่น - กำหนดระยะเวลาการปิดการใช้งานผู้ใช้ชั่วคราวหลังไม่มีการใช้งาน ตลอดไป หรือ 0 นาที - กำหนดจำนวนครั้งที่ผู้ใช้ทำการใส่รหัสไม่ถูกต้อง ไม่เกิน 3 ถึง 5 ครั้ง - กำหนดระยะเวลาที่ทำการยกเลิกการปิดใช้งานผู้ใช้ชั่วคราว 99999 นาที	■ บริษัทฯ ได้ดำเนินการให้พนักงานแผนกเทคโนโลยีสารสนเทศ ทำการตั้งค่าระบบปฏิบัติการ Window OS เพื่อปรับปรุงระบบการกำหนดรหัสผ่านของผู้ใช้งานระบบปฏิบัติการ Window OS เรียบร้อยแล้ว
1.4. <u>การกำหนดรหัสผ่าน ในระดับฐานข้อมูล (database level)</u> ในการตั้งค่าฐานข้อมูล Database Oracle 10G สำหรับระบบวางแผนทรัพยากรขององค์กร นั้น บริษัทฯ ควรมีการกำหนดสิทธิผู้ใช้งานระบบที่สามารถเข้าถึงฐานข้อมูลได้ ต้องได้รับการอนุมัติจากผู้บริหารระดับสูงเป็นรายกรณี เพื่อป้องกันความเสี่ยงจากการเข้าระบบโดยผู้ใช้ที่ไม่ได้รับอนุญาต อย่างไรก็ดี การใช้งานในระบบที่มีอยู่นั้น ผู้ใช้งานที่สามารถเข้าถึงระดับฐานข้อมูลได้นั้น มีจำนวนจำกัด	■ บริษัทฯ ได้ดำเนินการให้พนักงานแผนกเทคโนโลยีสารสนเทศ ทุกคนที่สามารถเข้าถึงระดับฐานข้อมูล ของระบบบริหารทรัพย์กรขององค์กร ซึ่งได้รับการอนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ โดยได้นำระบบและขั้นตอนดังกล่าวมาปฏิบัติใช้แล้ว ในเดือน พฤษภาคม 2556
1.5. <u>การกำหนดการเข้าถึงข้อมูล และการแก้ไขเปลี่ยนแปลงแอพพลิเคชั่นต่างๆ</u> ในการใช้งานระบบบริหารทรัพยากรขององค์กร ORION แอพพลิเคชั่น บริษัทฯ ควรกำหนดให้มีการจัดทำแบบฟอร์มเมื่อมีการเพิ่ม หรือเปลี่ยนแปลงการกำหนดค่าของผู้ใช้งาน (user profile) และมีการนำฟอร์มดังกล่าวไปใช้อย่างเคร่งครัด ทั้งนี้ แบบฟอร์มการเปลี่ยนแปลงการกำหนดค่าของผู้ใช้งาน ควรต้องได้รับการอนุมัติจากหัวหน้าสายงาน และมีการจัดเก็บเอกสาร ให้สามารถอ้างอิงได้ในอนาคต เพื่อจัดให้มีระบบควบคุมที่ดี และป้องกันความเสี่ยงจากการเข้าระบบโดยผู้ใช้ที่ไม่ได้รับอนุญาต	■ บริษัทฯ ได้จัดทำแบบฟอร์มดังกล่าว และได้รับอนุญาตจากหัวหน้าสายงาน ตามข้อสังเกตและข้อเสนอแนะของผู้สอบบัญชี แล้วในเดือน มิถุนายน 2556
1.6. <u>การยกเลิก การเข้าถึงข้อมูลของพนักงานของบริษัทฯ ที่พ้นสภาพการเป็นพนักงานแล้ว</u> บริษัทฯ ควรจัดขั้นตอนการปฏิบัติงานในการดูแลระบบการกำหนดค่าของผู้ใช้งาน และมีการจัดทำเอกสารอย่างเป็นระบบ โดยมีรายละเอียดเกี่ยวกับ การยื่นขอกำหนดค่าของผู้ใช้งานใหม่ การกำหนดและเปลี่ยนสิทธิของผู้ใช้งาน และการยกเลิกค่าของผู้ใช้งานเนื่องจากลาออกจากการเป็นพนักงานของบริษัทฯ ทั้งนี้ ขั้นตอนเกี่ยวกับการยกเลิกการตั้งค่าของผู้ใช้งาน ควรมีรายละเอียดเกี่ยวกับการยื่นข้อมูลรายชื่อของผู้ใช้งานที่ต้องการยกเลิก ผู้รับผิดชอบ ระยะเวลาในการรวบรวมและจัดเตรียมรายชื่อ และหลักฐานเมื่อมีการลบหรือยกเลิกการตั้งค่าผู้ใช้งาน	■ บริษัทฯ ได้ดำเนินการจัดทำแบบฟอร์มดังกล่าว และจัดเก็บข้อมูลการยกเลิกการกำหนดค่าของผู้ใช้งาน เมื่อพนักงานลาออกจากการเป็นพนักงานของบริษัทฯ แล้วในเดือน มิถุนายน 2556

ข้อสังเกต/ข้อเสนอแนะของผู้สอบบัญชี	ความเห็นของผู้บริหาร/การดำเนินการปรับปรุงของบริษัทฯ
ดังกล่าว โดยต้องมีการแจ้งรายชื่อดังกล่าวไปยังผู้ที่เกี่ยวข้อง จากแผนกทรัพยากรบุคคล ไปยังแผนกเทคโนโลยีสารสนเทศ อย่างรวดเร็วภายในวันที่ลาออกดังกล่าวมีผล	
1.7. <u>การใช้งานและการเข้าถึงระบบปฏิบัติการ Window OS โดย Super Users</u> การใช้งานและการเข้าถึงระบบโดยผู้ใช้งานประเภท Super Users นั้นบริษัทฯ ควรจำกัดจำนวนผู้ใช้งานดังกล่าว และให้มีการจัดเก็บรหัสผ่านในซองปิดผนึกและลงนามโดยบุคคลที่ได้รับอนุญาตเพื่อใช้ในกรณีฉุกเฉิน นอกจากนี้บริษัทฯ ควรกำหนดให้มีการเปลี่ยนรหัสผ่านภายหลังการใช้งานโดยผู้ใช้งานที่ได้รับอนุญาตและนำกลับไปเก็บในซองปิดผนึกเช่นเดิม และบริษัทฯ ควรจัดให้มีการบันทึกการใช้งานของผู้ใช้งานนั้นๆ ทั้งนี้ขั้นตอน และระบบการปฏิบัติงานดังกล่าว ควรมีการปฏิบัติตามอย่างเคร่งครัด	▪ บริษัทฯ ได้ดำเนินการจัดเก็บรหัสผ่านดังกล่าวในซองปิดผนึก และลงนามโดยประธานเจ้าหน้าที่ฝ่ายสารสนเทศเป็นที่เรียบร้อย และการใช้รหัสผ่านสำหรับผู้ใช้งานประเภท Super Users นั้นได้รับการอนุมัติโดยประธานเจ้าหน้าที่ฝ่ายสารสนเทศเป็นรายกรณี และจะสามารถบังคับใช้เป็นครั้งๆ ไปโดยจะมีการเปลี่ยนรหัสผ่านดังกล่าวทุกครั้งหลังการใช้งาน และนำกลับไปจัดเก็บในซองปิดผนึกตามขั้นตอนที่กำหนด ▪ บริษัทฯ ได้ดำเนินการจัดทำขั้นตอนการขออนุมัติการใช้งานรหัสผ่านสำหรับผู้ใช้งานประเภท Super Users แล้วใน เดือน มิถุนายน 2556
1.8. <u>การใช้งานระบบโดยผู้ใช้งานประเภท Super Users</u> เนื่องจากบริษัทฯ มีการอนุญาตการใช้งานโดยผู้ใช้งานประเภท Super Users ในการใช้งาน ระบบบริหารทรัพยากรขององค์กร จำนวน 5 ผู้ใช้งาน ทั้งนี้บริษัทฯ ยังไม่มีเอกสารขั้นตอนการอนุมัติการใช้งานของผู้ใช้งานประเภท Super Users และการกำหนดสิทธิในการใช้งาน อย่างเป็นทางการ ซึ่งอาจส่งผลให้ ในกรณีฉุกเฉินอาจไม่มีผู้ใช้งานรับทราบรหัสผ่านดังกล่าว ดังนั้นบริษัทฯ ควรจัดให้มีผู้รับผิดชอบผู้ดูแลระบบ และเป็นผู้รับทราบรหัสผ่านดังกล่าว ซึ่งต้องได้รับการอนุมัติจากผู้บริหารระดับสูง	▪ บริษัทฯ จะดำเนินการให้ผู้ใช้งานประเภท Super Users ของระบบบริหารทรัพยากรขององค์กร ได้รับการอนุมัติโดยผู้บริหารระดับสูงของบริษัทฯ และคาดว่าจะแล้วเสร็จภายใน เดือน พฤษภาคม 2556
1.9. <u>การทบทวนรายชื่อผู้ใช้งาน หรือ User</u> บริษัทฯ ควรกำหนดให้แผนกเทคโนโลยีสารสนเทศ จัดทำรายชื่อของผู้ใช้งาน และกำหนดสิทธิของผู้ใช้ สิทธิในการเข้าถึงระบบ และจัดให้มีการยืนยันและอนุมัติการเปลี่ยนแปลงการกำหนดค่าผู้ใช้งาน โดยผู้จัดการแผนกเทคโนโลยีสารสนเทศ นอกจากนี้บริษัทฯ ควรมีการทบทวนรายชื่อ สิทธิผู้ใช้ สิทธิในการเข้าถึงระบบ ทั้งระบบวางแผนทรัพยากรขององค์กร และระบบปฏิบัติการ Window Domain	▪ บริษัทฯ จัดให้มีการทบทวนรายชื่อผู้ใช้ตามที่ผู้สอบบัญชีแนะนำ เป็นประจำรายครึ่งปี ซึ่งสอดคล้องกับจำนวนพนักงาน และผู้ใช้งานในระบบของบริษัทฯ ซึ่งผ่านการตรวจสอบและอนุมัติ โดยประธานเจ้าหน้าที่สารสนเทศและหัวหน้าสายงานที่เกี่ยวข้องเป็นลำดับ ทั้งนี้รายชื่อพนักงานที่ผู้บริหารระดับสูงได้พิจารณาแล้ว เดือน มิถุนายน 2556
2. **การปฏิบัติงานของระบบคอมพิวเตอร์**	
2.1. <u>แผนฟื้นฟูภัยพิบัติ (Disaster Recovery Plan) หรือแผนสำรองภาวะฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศ</u> บริษัทฯ ควรมีการจัดเตรียมแผนสำรองภาวะฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษร โดยมีรายละเอียดแนวทาง และแผนปฏิบัติงานให้สามารถปรับเปลี่ยนอุปกรณ์คอมพิวเตอร์ อุปกรณ์เกี่ยวข้องอื่นๆ และระบบเทคโนโลยีสารสนเทศ ให้สามารถประกอบธุรกิจในกรณีที่เกิดเหตุการณ์ฉุกเฉิน และมีการจัดทำคู่มือการปฏิบัติงาน การทบทวนแผนสำรองดังกล่าวเป็นระยะ นอกจากนี้ควรกำหนดให้จัดเก็บคู่มือดังกล่าวในศูนย์ปฏิบัติงานสำรอง นอกจากนี้ บริษัทฯ ควรจัดให้มีการทดสอบระบบอย่างเคร่งครัดเป็นประจำ และผู้ใช้หลักควรมีส่วนร่วมในขั้นตอนการทดสอบระบบ เพื่อให้ผู้ใช้เหล่านั้นเข้าใจ ถึง	▪ บริษัทฯ อยู่ระหว่างการวิเคราะห์ เปรียบเทียบข้อแตกต่างระหว่างแผนฟื้นฟูภัยพิบัติในปัจจุบันของบริษัทฯ และข้อสังเกตและเสนอแนะจากผู้สอบบัญชี เพื่อระบุความเสี่ยงและข้อบกพร่องของระบบเดิม หลังการประเมินบริษัทฯ จะดำเนินการปรับปรุงแก้ไข และจัดทำแผนสำรองภาวะฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันและหลีกเลี่ยงความเสี่ยงของระบบในปัจจุบัน ให้สำเร็จ ภายในเดือน ธันวาคม 2556

ข้อสังเกต/ข้อเสนอแนะของผู้สอบบัญชี	ความเห็นของผู้บริหาร/การดำเนินการปรับปรุงของบริษัทฯ
บทบาท หน้าที่ความรับผิดชอบและความสำคัญของแผนสำรองดังกล่าว ทั้งนี้ควรมีการบันทึกผลการทดสอบระบบเพื่อให้มั่นใจว่าได้ทดสอบแผนสำรองและระบบอย่างครบถ้วน และเหมาะสม	
2.2. <u>การบริหารการแก้ไขเหตุการณ์ผิดปกติที่ทำให้การบริการต้องหยุดชะงัก</u> เนื่องจากบริษัทฯ มิได้ทำการจัดเก็บ และบันทึกข้อมูลเหตุการณ์ผิดปกติ และปัญหาที่เกิดขึ้นระหว่างการปฏิบัติงานอย่างเป็นระบบ ซึ่งอาจส่งผลต่อการบริหารจัดการระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ ได้อย่างมีประสิทธิภาพ และรวดเร็ว ดังนั้น บริษัทฯ ควรจัดให้มีแผนการบริหารการแก้ไขเหตุการณ์ผิดปกติที่ทำให้การ บริการต้องหยุดชะงัก โดยมีการบันทึกเหตุการณ์ที่เคยเกิดขึ้น เพื่อให้บริษัทฯ สามารถบริหาร และป้องกันความเสี่ยงของเหตุการณ์ที่อาจเกิดขึ้นในอนาคต และสามารถแก้ไขปัญหาได้อย่างรวดเร็ว ทั้งนี้ระบบบันทึกและติดตามเหตุการณ์ผิดปกติควรครอบคลุมถึงข้อกำหนดต่อไปนี้ - หมายเลขเหตุการณ์ รายละเอียดเหตุการณ์ วันที่ แผนที่คาดว่าจะแล้วเสร็จ ระดับความรุนแรงของเหตุการณ์นั้นๆ - ผู้รับผิดชอบ - การติดตามผลการแก้ไข	▪ บริษัทฯ อยู่ระหว่างการประเมินทางเลือกระบบสนับสนุนเพื่อให้บริการแก้ไขเหตุการณ์ผิดปกติ ในการใช้งานระบบเทคโนโลยีสารสนเทศ และได้คัดเลือกรายชื่อผู้ให้บริการระบบเพื่อบันทึกข้อมูลเหตุการณ์ผิดปกติ จำนวน 3 ราย ซึ่งคาดว่าจะสามารถสรุปและใช้งานได้ภายในเดือนสิงหาคม 2556