GRAMMY

ประกาศ ที่ 17/2555

เรื่อง นโยบายความมั่นคงด้านเทคโนโลยีสารสนเทศ (Information Technology Security Policy)

เพื่อประสิทธิภาพสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของบริษัท จีเอ็มเอ็มแกรมมี่ จำกัด (มหาชน) และบริษัทในเครือ ("กลุ่มบริษัท") จึงเห็นสมควรให้มีการกำหนดนโยบายความมั่นคงด้านเทคโนโลยีสารสนเทศขึ้น โดยมีวัตถุประสงค์หลัก ดังนี้

1. เพื่อเป็นแนวปฏิบัติของบุคลากร ซึ่งรวมทั้งพนักงานและผู้บริหารในการใช้งาน ดูแลรักษา และควบคุมระบบคอมพิวเตอร์ของกลุ่มบริษัท
2. เพื่อเป็นแนวทางในการกำหนดมาตรฐานการทำงานที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศ[1] ของกลุ่มบริษัท ตลอดจนกำหนดขั้นตอนการทำงานที่ถูกต้องและเป็นมาตรฐานเดียวกันในการบริหารจัดการข้อมูล และกำหนดระดับชั้นความมั่นคงปลอดภัยของข้อมูล
3. เพื่อสร้างความเชื่อมั่นในระบบรักษาความปลอดภัยของข้อมูลธุรกิจต่อบุคลากรซึ่งเป็นผู้ใช้บริการ และผู้มีส่วนเกี่ยวข้องในการดำเนินธุรกิจของกลุ่มบริษัท

โดยสาระสำคัญของนโยบายความมั่นคงด้านเทคโนโลยีสารสนเทศฉบับนี้ ประกอบด้วย

1) การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
2) การควบคุมการเข้าออกห้อง Server และการป้องกันความเสียหาย (Physical Security)
3) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
4) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
5) การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Contingency Plan)
6) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation) และการใช้งานทั่วไป
7) การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

ระบบข้อมูลสารสนเทศ[1] เป็นระบบคอมพิวเตอร์ ระบบโครงข่าย และอุปกรณ์โครงข่ายสำคัญของระบบข้อมูลทางการบริหารจัดการของกลุ่มบริษัท การจัดทำ จัดเก็บ นำไปใช้ และควบคุมดูแลรักษาระบบความมั่นคงปลอดภัยของข้อมูลทางธุรกิจของกลุ่มบริษัท จะสามารถปกป้องคุ้มครองข้อมูลและความลับทางธุรกิจของกลุ่มบริษัทมิให้รั่วไหลและก่อให้เกิดความเสียหายต่อธุรกิจได้ ดังนั้น ความสำเร็จทางธุรกิจของกลุ่มบริษัทส่วนหนึ่งจึงขึ้นอยู่กับประสิทธิภาพในการใช้งานและการคุ้มกันให้เกิดความมั่นคงปลอดภัยของระบบคอมพิวเตอร์อย่างถูกต้องและเหมาะสม

รายละเอียดนโยบาย

1) **การแบ่งแยกอำนาจหน้าที่** (Segregation of Duties)

การแบ่งแยกอำนาจหน้าที่มีวัตถุประสงค์เพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายต่างๆ ที่เกี่ยวข้อง เพื่อลดความเสี่ยงด้าน Infrastructure risk

1.1 คณะทำงานระบบสารสนเทศ (ตามคำสั่งที่ 1/2555) เป็นผู้กำหนดทิศทางการใช้ระบบสารสนเทศของกลุ่มบริษัท รวมทั้งกำหนดนโยบายและระเบียบการปฏิบัติงาน และติดตามความก้าวหน้าของระบบสารสนเทศ ศึกษาความเป็นไปได้เพื่อนำมาพัฒนาระบบสารสนเทศของกลุ่มบริษัท กำกับดูแล และสนับสนุนให้มีการใช้งานระบบสารสนเทศให้เกิดประสิทธิภาพสูงสุด ตลอดจนสอบทาน และนำเสนอแนวทางเพื่อปรับปรุงนโยบายและระเบียบการปฏิบัติงาน เพื่อนำเสนอต่อประธานเจ้าหน้าที่บริหารกลุ่มบริษัทฯ เพื่อพิจารณาอนุมัติ

1.2 ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบดำเนินการและควบคุมให้เกิดการปฏิบัติตามนโยบายความมั่นคงด้านเทคโนโลยีสารสนเทศฉบับนี้ และให้มีการรายงานตามโครงสร้างการบังคับบัญชาตามปกติ ทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศมีบทบาท หน้าที่ และความรับผิดชอบ (IT Security Roles and Responsibilities) ดังนี้

1.2.1 ดูแลรักษาระบบข้อมูลสารสนเทศอันเป็นทรัพย์สินของกลุ่มบริษัทให้มีความมั่นคงปลอดภัยอยู่เสมอ

1.2.2 กำหนด Procedure หรือ Work Instruction (ถ้าจำเป็นต้องมี) เพื่อสร้างมาตรฐานการทำงานที่ถูกต้องและเข้าใจร่วมกัน

1.2.3 ให้ความรู้ สร้างความเข้าใจ เผยแพร่เนื้อหาและแนวทางปฏิบัติที่ดี และควบคุมให้เป็นไปตามนโยบายฉบับนี้อย่างถูกต้องและเคร่งครัด

1.2.4 จัดแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง

1.2.5 จัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีที่จำเป็น เช่น ผู้บริหารระบบ (System administrator) เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) เป็นต้น

1.3 ฝ่ายบริการและบริหารงานกลาง เป็นผู้รับผิดชอบในการตรวจสอบและจัดทำทะเบียนเครื่องคอมพิวเตอร์ เครื่องพิมพ์ และซอฟท์แวร์คอมพิวเตอร์ โดยแต่ละหน่วยงานจะเป็นผู้รับผิดชอบทรัพย์สินของตนเอง ทั้งนี้ ทรัพย์สินในทะเบียนจะต้องมีการตรวจทานอย่างน้อยปีละ 1 ครั้ง ซึ่งอุปกรณ์ที่ต้องมีการจัดทำทะเบียน ได้แก่

1.3.1 เครื่องคอมพิวเตอร์ (Personal Computer, Laptop/ Notebook, Tablet และอุปกรณ์อื่นๆ ที่จัดอยู่ในหมวดเครื่องคอมพิวเตอร์)

1.3.2 เครื่องพิมพ์และอุปกรณ์ต่อเชื่อมคอมพิวเตอร์

1.3.3 ซอฟท์แวร์คอมพิวเตอร์

1.3.4 Switch / Router / Access Point / Firewall / UPS

อนึ่ง รายละเอียดของผู้ใช้งานในทะเบียน จะต้องระบุรายละเอียดให้ครบถ้วน ดังนี้

1.3.5 ชั้นที่อุปกรณ์ถูกใช้งาน (จัดเก็บ/ ตั้งอยู่/ โต๊ะทำงานของผู้ใช้งาน)

1.3.6 ชื่อผู้ใช้งาน

1.3.7 ชื่อเครื่อง

1.3.8 รุ่นของเครื่อง และตราผลิตภัณฑ์ (Brand)

1.3.9 หมายเลข IP Address

1.4 ฝ่ายบริหารทรัพยากรบุคคล เป็นผู้รับผิดชอบในการดำเนินการต่อไปนี้

1.4.1 แจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบในทันที เมื่อมีการเปลี่ยนสถานภาพของผู้ใช้ เช่น การลาพักงาน การโอนย้าย การเปลี่ยนหน้าที่งาน เพื่อจะได้ดำเนินการระงับการใช้งาน เปลี่ยนแปลง หรือลบสิทธิการใช้งานภายใน 30 วัน หรือวันที่ผู้บังคับบัญชาเห็นสมควร

1.4.2 จัดทำ Job Description ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในฝ่ายเทคโนโลยีสารสนเทศอย่างชัดเจน เป็นลายลักษณ์อักษร

1.4.3 บุคลากรทุกคนจะต้องลงนามในสัญญาข้อตกลงว่าด้วยการรักษาความลับข้อมูลทางธุรกิจ (Non-Disclosure Agreement) กับกลุ่มบริษัท ก่อนเริ่มงานและหลังประกาศใช้นโยบายฉบับนี้ และให้ถือเป็นส่วนหนึ่งของสภาพหรือเงื่อนไขการจ้างงาน (Employment Conditions)

2) การควบคุมการเข้าออกห้อง Server และการป้องกันความเสียหาย (Physical Security)

การควบคุมการเข้าออกห้อง Server มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (Access risk) แก้ไขเปลี่ยนแปลง (Integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (Availability risk) ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (Availability risk)

2.1 การควบคุมการเข้าออกห้อง Server

2.1.1 ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบดูแล ควบคุมห้อง Server

2.1.2 จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในห้อง Server และต้องกำหนดสิทธิการเข้าออกเฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

2.1.3 มีระบบเก็บบันทึกการเข้าออกห้อง Server โดยบันทึกดังกล่าวต้องมีรายละเอียดตัวบุคคลและเวลาผ่านเข้า-ออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

2.1.4 มีการควบคุมอย่างเข้มงวด โดยมีการบันทึกการเข้า-ออก สำหรับผู้ที่ไม่ใช่บุคลากรที่มีหน้าที่เกี่ยวข้องประจำ และต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจาก IT Supervisor ก่อนเข้าปฏิบัติงาน

2.2 การป้องกันความเสียหาย

2.2.1 มีแผนภาพระบุ Rack และตำแหน่งของเครื่อง Server แต่ละเครื่อง

2.2.2 มีระบบดับเพลิงแบบอัตโนมัติ

2.2.3 มีระบบไฟฟ้าสำรอง (UPS และ Power Generator)

2.2.4 มีระบบควบคุมอุณหภูมิและความชื้น ที่สามารถควบคุมสภาพแวดล้อมให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์

2.2.5 มีระบบสัญญาณเตือนภัยพร้อมเครื่องตรวจสอบควัน

2.2.6 มีกล้องวงจรปิด ในการเก็บภาพผู้เข้าออกได้อย่างน้อยต่อเนื่อง 2 สัปดาห์

2.2.7 สายสัญญาณ และ Switch ในแต่ละชั้น ต้องเก็บอยู่ในห้องมิดชิดที่มีการปิดและมีกุญแจล็อก

2.2.8 เครื่องคอมพิวเตอร์ที่อยู่ในพื้นที่ของแต่ละหน่วยงาน อยู่ในความรับผิดชอบของผู้บริหารสูงสุดของแต่ละหน่วยงาน

3) **การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย** (Information and Network Security)

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์ มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้ (Access risk) หรือแก้ไขเปลี่ยนแปลง (Integrity risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious code ต่างๆ ไม่ให้เข้าถึง (Access risk) หรือสร้างความเสียหาย (Availability risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

3.1 การบริหารจัดการข้อมูล

3.1.1 กำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

3.1.2 การรับส่งข้อมูลธุรกรรมระหว่างบริษัท ผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น

3.1.3 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) นอกจากนี้ ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

3.2 การกำหนดสิทธิให้แก่ผู้ใช้งานที่มีสิทธิพิเศษ (User privilege) และการควบคุมการเข้าถึง (Access control)

3.2.1 ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application system) สิทธิการใช้งานอินเทอร์เนต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ (The principle of least privilege) และเท่าที่จำเป็นในการรับรู้ในงานที่ทำ (Need to know basis) เท่านั้น และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

3.2.2 ในกรณีมีความจำเป็นต้องกำหนด User ที่มีสิทธิพิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม โดยใช้แนวทางในการดำเนินการ ดังนี้

- ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาตามโครงสร้างสายงาน ตั้งแต่ระดับผู้อำนวยการฝ่ายขึ้นไป
- ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น เปลี่ยนทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น
- ควรตรวจทานสิทธิพิเศษการใช้ข้อมูลและระบบสารสนเทศอย่างน้อยทุกๆ 6 เดือน โดยให้ฝ่ายบริหารทรัพยากรบุคคลเป็นผู้ตรวจทาน

3.2.3 ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

3.2.4 ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3.2.5 ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3.2.6 การลงทะเบียนผู้ใช้ระบบ (User registration) จะต้องได้รับการอนุมัติตามโครงสร้างสายงานเป็นลายลักษณ์อักษร

3.2.7 มีการตรวจทานสิทธิการใช้ข้อมูลและระบบสารสนเทศของผู้ใช้ระบบอย่างน้อยทุกๆ 1 ปี หรือเมื่อได้รับการแจ้งการเปลี่ยนตำแหน่ง และ/หรือ ความรับผิดชอบ

3.2.8 มีการตรวจทานบัญชีรหัสผู้ใช้ที่ไม่มีการใช้งานในระยะเวลาที่กำหนด และต้องไม่เกิน 6 เดือน ในกรณีที่เหมาะสมให้ดำเนินการยกเลิก

3.2.9 ในขั้นตอนการเข้าระบบ ขณะที่ผู้ใช้เริ่มเข้าระบบ ระบบจะต้องเปิดเผยข้อมูลที่เกี่ยวกับระบบงาน หรือบริการให้น้อยที่สุด โดยใช้แนวทางในการดำเนินการ ดังนี้

- ไม่แสดงรหัสผ่านขณะป้อนรหัสบนหน้าจอ
- มีประกาศ "ระเบียบวินัยการใช้เครื่อง" ที่จัดทำขึ้นโดยฝ่ายกฎหมาย แสดงบนหน้าจอ Login ให้บุคลากรอ่านทุกครั้งก่อนทำการเข้าระบบ
- ไม่มีข้อความช่วยเหลือ หรือแนะนำในขั้นตอนการเข้าระบบ
- ตรวจสอบความถูกต้องของข้อมูลการเข้าระบบ Logon Information เมื่อผู้ใช้ระบบป้อนข้อมูลครบทั้งหมด หากมีข้อผิดพลาดเกิดขึ้น 3 ครั้ง ระบบจะล็อค User นั้นโดยอัตโนมัติ

3.3 การกำหนดรหัสผู้ใช้งานและรหัสผ่าน (User ID and Password)

3.3.1 มีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ

3.3.2 ผู้ทำหน้าที่ควบคุมระบบเป็นผู้กำหนดและลงทะเบียนรหัสผู้ใช้โดยกำหนดทะเบียนผู้ใช้จากชื่อของบุคลากร (ภาษาอังกฤษ) และตามด้วยตัวอักษรภาษาอังกฤษอย่างน้อย 1 ตัวแรกของนามสกุล

3.3.3 รหัสผู้ใช้ทุกชนิด ทุกระบบงาน (Application) จะต้องมีการลงทะเบียนและบันทึกการใช้งานโดยผู้ควบคุมระบบ โดยการได้มาซึ่งรหัสผู้ใช้นั้น บุคลากรจะต้องได้รับอนุมัติจากผู้บังคับบัญชาตามโครงสร้างสายงาน ตั้งแต่ระดับผู้จัดการฝ่ายหรือสูงกว่า

3.3.4 ผู้ใช้งานระบบทุกคนต้องมีรหัสผู้ใช้เป็นของตนเอง จะต้องไม่มีการใช้ร่วมกัน (หนึ่งรหัสต่อหนึ่งคน) แต่ถ้ามีความจำเป็นต้องใช้ร่วมกัน จะต้องได้รับอนุมัติจากผู้บังคับบัญชา และให้บันทึกไว้เป็นหลักฐานที่ผู้ควบคุมระบบ

3.3.5 ไม่นำรหัสผู้ใช้มาใช้ซ้ำ หากมีความจำเป็น ต้องมั่นใจว่า สิทธิการใช้งานทั้งหมดของผู้ใช้คนก่อนได้รับการยกเลิกแล้ว และข้อมูลที่เกี่ยวข้องทั้งหมดจะไม่สามารถใช้ได้โดยผู้ใช้คนใหม่

3.3.6 ไม่อนุญาตให้บุคลากรชั่วคราวใช้รหัสผู้ใช้ร่วมกับบุคลากรประจำ

3.3.7 ในกรณีที่ต้องมีการใช้รหัสผู้ใช้เพื่อวัตถุประสงค์เฉพาะ เช่น การทดสอบระบบ ควรกำหนดรหัสผู้ใช้ขึ้นเฉพาะและทำการยกเลิกทันทีที่ภารกิจนั้นเสร็จสมบูรณ์รหัสผ่านต้องยาวอย่างน้อย 8 หลัก

3.3.8 กำหนดให้ต้องเปลี่ยนรหัสผ่านทุก 3 เดือน โดยห้ามใช้รหัสผ่านเดิมซ้ำใน 8 รอบการเปลี่ยน

3.3.9 ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 3 ครั้ง

3.3.10 ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default password) หรือได้รับรหัสผ่านใหม่ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

3.3.11 ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

3.3.12 ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

3.3.13 ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของบุคลากรที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default user) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยน Password เป็นต้น

3.4 การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

3.4.1 มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

3.4.2 เปิดใช้บริการ (Service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

3.4.3 ดำเนินการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System software) เช่น ระบบปฏิบัติการ DBMS และ Web server เป็นต้น อย่างสม่ำเสมอ

3.4.4 ทดสอบ System software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

3.4.5 มีแนวทางปฏิบัติในการใช้งาน Software utility เช่น Personal firewall, Password cracker เป็นต้น และตรวจสอบการใช้งาน Software utility อย่างสม่ำเสมอ

3.4.6 กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน

3.5 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรและการตรวจสอบระบบเครือข่าย (Network / Information Security Incident Management)

3.5.1 Log Centralization Management

- ติดตั้งระบบเพื่อจัดเก็บ Log ของ Internet และ e-mail Log ของบุคลากรทุกคน เพื่อการตรวจสอบตาม "พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550"

3.5.2 Network

- ติดตั้งระบบป้องกันการบุกรุก เช่น Firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก
- มีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องต่อไปนี้อย่างสม่ำเสมอ
  - ความพยายามในการบุกรุกผ่านระบบเครือข่าย
  - การใช้งานในลักษณะที่ผิดปกติ
  - การใช้งาน การแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

- มีการตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า Parameter ต่างๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physical disconnect) และจุดเชื่อมต่อ (Disable port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่ายออกจากระบบเครือข่ายโดยสิ้นเชิง

3.5.3 Network Incident Monitor

- มีระบบส่ง e-mail เตือนในกรณีที่ระบบสำหรับตรวจสอบ Traffic ของระบบ Network มีปัญหา ทั้งนี้ ในกรณีที่มี e-mail แจ้งแต่ไม่พบสัญญาณ ฝ่ายเทคโนโลยีสารสนเทศต้องส่งเจ้าหน้าที่ไปตรวจสอบ และดำเนินการดังนี้
  - กรณีที่มีอุปกรณ์เสียหาย เจ้าหน้าที่จะนำอุปกรณ์สำรองไปทดแทนและทำการจัดซื้ออุปกรณ์ตัวใหม่
  - กรณีที่มีเหตุผิดปกติอันเกิดจากการบุกรุกจากภายนอก ให้แจ้งผู้จัดการแผนก IT Service หรือผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเพื่อแก้ไขปัญหา

3.6 การป้องกันไวรัส และ Malicious code

3.6.1 ต้องมีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟท์แวร์ป้องกันไวรัส เป็นต้น

3.6.2 ฝ่ายเทคโนโลยีสารสนเทศควรประชาสัมพันธ์และให้ความรู้เกี่ยวกับไวรัสชนิดใหม่ๆ และแนวปฏิบัติในการป้องกันไวรัสให้แก่ผู้ใช้งานอย่างสม่ำเสมอ

3.6.3 ควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (Disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้ และควรแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีไวรัส

4) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

4.1 การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

4.1.1 การร้องขอ

- การพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานจะต้องผ่านการวิเคราะห์ความต้องการร่วมกับฝ่ายเทคโนโลยีสารสนเทศ
- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (IT Request Form) และต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามโครงสร้างสายงาน ตั้งแต่ระดับผู้อำนวยการฝ่ายขึ้นไป
- ในกรณีที่ระบบงานที่ได้รับการร้องขอให้พัฒนาหรือแก้ไขเปลี่ยนแปลงมีผลกระทบกับการปฏิบัติงาน หรือมีการแสดงข้อมูลของหน่วยงานอื่น เอกสาร (IT Request Form) จะต้องได้รับการอนุมัติจากผู้บังคับบัญชาตั้งแต่ระดับผู้อำนวยการฝ่ายขึ้นไปตามโครงสร้างสายงานของหน่วยงานที่ได้รับผลกระทบด้วย

4.1.2 การปฏิบัติงานพัฒนาระบบงาน

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop environment) ออกจากส่วนที่ใช้งานจริง (Production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น
- ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ โดยร่วมกับฝ่ายเทคโนโลยีสารสนเทศในการสรุป Functional specification วิธีการ และรูปแบบการใช้งาน (หน้าจอ/ รายงาน)

4.1.3 การทดสอบ

- ผู้ที่ร้องขอและฝ่ายเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง และให้มีการร่วมลงนามยอมรับผลการทดสอบและรับมอบงานในเอกสาร (IT Request Form)

4.1.4 การโอนย้ายระบบงานเพื่อใช้งานจริง

- ต้องตรวจสอบการโอนย้ายระบบงานไปที่เครื่อง Server – Production ให้ถูกต้องครบถ้วน
- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดเก็บเอกสาร IT Request Form, Functional specification เอกสารแสดงสิทธิการใช้งาน และเอกสารที่เกี่ยวข้องอย่างน้อย 1 ปี

5) **การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน** (Backup and IT Contingency Plan)

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (Availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

5.1 การสำรองข้อมูลและระบบคอมพิวเตอร์

5.1.1 การสำรองข้อมูล (Data Backup)

- มีการสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating system) โปรแกรมระบบงานคอมพิวเตอร์ (Application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง
- มีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้
  - ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
  - ประเภทสื่อบันทึก (Media)
  - จำนวนที่ต้องสำรอง (Copy)
  - ขั้นตอนและวิธีการสำรองโดยละเอียด
  - สถานที่และวิธีการเก็บรักษาสื่อบันทึก
- ควรมีการบันทึกการปฏิบัติงาน (Log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
- ระบบและข้อมูลสำรองจะต้องมีการปรับปรุงให้เป็นปัจจุบัน
- ระบบและข้อมูลสำรองต้องได้รับการบำรุงรักษา เช่นเดียวกันและในระดับเดียวกบข้อมูลหลัก

5.1.2 การทดสอบ

- ทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้
- มีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

5.1.3 การเก็บรักษา

- ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย
- ติดตั้ง Database Backup Site (DR Site) ห่างจากอาคาร GMM Grammy Place มากกว่า 10 กิโลเมตร
- จัดส่งข้อมูลจากอาคาร GMM Grammy Place ไปยัง DR Site อย่างน้อยทุก 15 นาที
- ผู้ดูแลระบบ DR Site ต้องทำการตรวจสอบข้อมูลทุกอาทิตย์
- Backup ข้อมูลใส่ Tape และนำไปเก็บรักษาที่ตู้เซฟของธนาคาร
- ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น
- ติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด
- การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา

5.2 การเตรียมพร้อมกรณีฉุกเฉิน

5.2.1 มีการจัดทำแผนฟื้นฟู (DR – Disaster Recovery Plan) เพื่อให้สามารถกอบกู้ระบบการทำงานและข้อมูลคืนมาเมื่อมีปัญหาใดๆ เกิดขึ้น ทั้งจากปัญหาของระบบเอง และปัญหาจากภายนอก ทั้งนี้ แผนฉุกเฉินควรมีรายละเอียด ดังนี้

- จัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน
- กำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา
- มีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์
- กำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

- มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะ ของเครื่องคอมพิวเตอร์ (Specification) ขั้นต่ำ ค่า configuration และอุปกรณ์เครือข่าย เป็นต้น
- ในกรณีที่บริษัทมีศูนย์คอมพิวเตอร์สำรอง ก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น
- ปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่

5.2.2 ทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย

5.2.3 สื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น

5.2.4 ในกรณีเกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

6) **การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์** (Computer Operation) **และการใช้งานทั่วไป**

การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์และการใช้งานทั่วไปมีวัตถุประสงค์เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหาและการควบคุมการจัดทำรายงาน การปฏิบัติตามข้อกำหนด เช่น การป้องกันและควบคุมการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ การรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์พกพา และแนวปฏิบัติในการใช้เครือข่ายสังคม (Social Network) ซึ่งเป็นการลดความเสี่ยงด้าน Integrity risk และ Availability risk

6.1 การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

6.1.1 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer operator) เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงานของระบบและตารางเวลาในการปฏิบัติงาน เป็นต้น และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

6.1.2 ควรกำหนดให้เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ปฏิบัติงานโดยผ่านเมนู และควรจำกัดการปฏิบัติงานโดยใช้ Command line เท่าที่จำเป็น

6.2 การติดตามการทำงานของระบบคอมพิวเตอร์ (Monitoring)

6.2.1 ต้องติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพ (Capacity) ของระบบ

6.2.2 ควรบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่างๆ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ

6.3 การจัดการปัญหาต่างๆ

6.3.1 ต้องกำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน รวมถึงหมายเลขโทรศัพท์ของผู้ที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่มีปัญหา

6.3.2 ควรมีระบบจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้น และรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหาและตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป

6.4 การปฏิบัติตามข้อกำหนด (Compliance)

6.4.1 เครื่องคอมพิวเตอร์ของกลุ่มบริษัท บุคลากรต้องใช้ซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

6.4.2 บุคลากรจะไม่นำซอฟท์แวร์ไม่มีลิขสิทธิ์มาติดตั้ง (Install) และใช้งานในเครื่องคอมพิวเตอร์ของกลุ่มบริษัท

6.4.3 ฝ่ายเทคโนโลยีสารสนเทศจะทำการตรวจสอบโปรแกรมลิขสิทธิ์ ในเครื่องคอมพิวเตอร์ของบุคลากรอย่างน้อยปีละ 1 ครั้ง ถ้าพบการกระทำผิด ทางฝ่ายฯ จะทำหนังสือแจ้งหัวหน้าหน่วยงานเพื่อจัดซื้อหรือทำการลงโทษบุคลากรต่อไป

6.5 การป้องกันและควบคุมการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ (Protection & Control of Usage of Internet and e-mail)

6.5.1 ต้องไม่ใช้รหัสผู้ใช้(User ID) และ รหัสผ่าน (Password) ร่วมกัน หรือใช้ของผู้อื่น เว้นแต่จะต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือ หัวหน้าสายงาน

6.5.2 ต้องไม่ทำการท่องอินเตอร์เน็ตในเรื่องที่ไม่เกี่ยวกับงานในเวลางาน

6.5.3 ไม่เล่นเกมส์คอมพิวเตอร์ไม่ว่าเวลาใด

6.5.4 ไม่ร่วมในห้องสนทนา (Chat room) ที่ไม่เกี่ยวกับงาน ไม่ว่าเวลาใด

6.5.5 ไม่ดูภาพ ดู Websites หรือ Web board ที่ไม่เหมาะสม

6.5.6 ไม่เข้าร่วมในกิจกรรมที่ผิดศีลธรรม หรือผิดกฎหมาย ทุกเรื่อง

6.5.7 ไม่ดูภาพยนตร์ทุกชนิด ไม่ว่าเวลาใด

6.5.8 ไม่เล่นและร้องเพลง Karaoke ไม่ว่าเวลาใด

6.5.9 ไม่ทำการส่งอีเมล์ หรือ Upload/Download ไฟล์เพลง รูปภาพ ภาพยนตร์ และอื่นๆ ที่ไม่เกี่ยวกับงานทุกชนิด ไม่ว่าในเวลาใด เว้นแต่ได้รับการอนุมัติจากผู้บังคับบัญชาตามโครงสร้างสายงาน ตั้งแต่ระดับ MD ขึ้นไป

6.5.10 ไม่ทำการส่งเอกสารหรือจดหมายที่มีภาพและเนื้อหาที่ไม่เหมาะสมต่อศีลธรรม เช่น ภาพความรุนแรง ภาพโป๊เปลือย เป็นต้น

6.5.11 การกระทำอื่นๆ ที่ปุถุชนทั่วไปเห็นว่า เป็นสิ่งที่ไม่ถูกต้องและไม่สมควรกระทำ

6.6 การป้องกันการเชื่อมต่อโครงข่ายอื่น นอกเหนือจากที่ฝ่ายเทคโนโลยีสารสนเทศดำเนินการให้

6.6.1 การเชื่อมต่อโครงข่ายอื่นต้องได้รับความเห็นชอบจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ และผู้บริหารสูงสุดตามโครงสร้างสายงาน ตั้งแต่ระดับ MD ขึ้นไปเท่านั้น

6.7 การรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์พกพา

6.7.1 อุปกรณ์พกพา หมายรวมถึง Laptop/ Notebook, Tablet, Smart phone และอุปกรณ์อื่นๆ ที่มีคุณสมบัติหรือความสามารถในลักษณะเดียวกัน

6.7.2 อุปกรณ์พกพาต่างๆ ที่นำมาเชื่อมต่อระบบข้อมูลสารสนเทศ ต้องดำเนินการตามนโยบายความมั่นคงด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยต่อข้อมูล

6.7.3 การนำอุปกรณ์พกพาส่วนตัวมาเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารสูงสุดตามโครงสร้างสายงาน ตั้งแต่ระดับ MD ขึ้นไปเท่านั้น

6.7.4 บุคลากรผู้ใช้งานอุปกรณ์พกพาต้องตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ จากการรั่วไหลของข้อมูลหรือการเชื่อมต่อของอุปกรณ์พกพานั้น

6.8 แนวปฏิบัติในการใช้เครือข่ายสังคม (Social Network)

6.8.1 เครือข่ายสังคม หรือ Social Network หมายถึง ระบบงานที่ทำให้มีการสื่อสาร ทั้งการรับรู้ข่าวสารและการแบ่งปันข้อมูลกับคนจำนวนมากผ่านช่องทางอินเตอร์เน็ต โดยการใช้งานเทคโนโลยีประเภทสื่อสังคม (Social Media)

6.8.2 บุคลากรที่ใช้งานเทคโนโลยีประเภทสื่อสังคม ต้องป้องกัน และรักษาความลับของกลุ่มบริษัท โดยยึดแนวปฏิบัติในการใช้เครือข่ายสังคม ดังนี้

- บุคลากรต้องไม่เข้าถึง หรือละเมิดข้อมูลส่วนบุคคลของผู้อื่น โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล
- บุคลากรต้องรับผิดชอบต่อข้อความที่จัดทำขึ้นหรือนำไปเผยแพร่ทั้งหมด

- บุคลากรต้องไม่แอบอ้างหรือกระทำการใดอันอาจทำให้ผู้อื่นเข้าใจผิดว่ากำลังสื่อความในนามกลุ่มบริษัท
- บุคลากรต้องไม่ใช้เครือข่ายสังคมในลักษณะที่อาจก่อให้เกิดความเสียหายต่อกลุ่มบริษัทในทุกรูปแบบ
- บุคลากรต้องไม่ใช้เครือข่ายสังคมในลักษณะที่หยาบคาย ก้าวร้าว หรือกล่าวโทษให้ผู้อื่นเกิดความเสียหาย หรือละเมิดต่อสิทธิของผู้อื่น ขัดต่อศีลธรรมอันดี ผิดต่อกฎหมาย หรือขัดต่อรัฐธรรมนูญ
- บุคลากรต้องเคารพความคิดเห็นของผู้อื่น และใช้วิจารณญาณในการโต้ตอบอย่างเหมาะสม
- บุคลากรต้องไม่แสดงความคิดเห็นอันก่อให้เกิดความเสียหายต่อเครื่องหมายการค้าหรือสิ่งที่มีการแจ้งจดทะเบียนลิขสิทธิ์ทั้งสิ้น
- บุคลากรต้องไม่แสดงความคิดเห็นในเรื่องใดๆ ที่เกี่ยวข้องกับประเด็นทางกฎหมายหรือเกี่ยวข้องกับคู่กรณีที่กลุ่มบริษัทกำลังดำเนินการฟ้องร้องอยู่โดยเด็ดขาด
- บุคลากรควรหลีกเลี่ยงประเด็นที่ละเอียดอ่อน อันอาจนำไปสู่ข้อพิพาทได้ เช่น การเมือง หรือศาสนา เป็นจต้น
- กลุ่มบริษัทสงวนสิทธิ์ในการเฝ้าระวังการใช้งานเครือข่ายสังคมผ่านระบบเครือข่ายของกลุ่มบริษัท
- หากมีความผิดพลาดใด ที่เกิดขึ้นจากการใช้งานเครือข่ายสังคมของบุคลากร อันอาจส่งผลกระทบในทางลบต่อกลุ่มบริษัท บุคลากรต้องรับผิดชอบและรีบแก้ไขโดยเร็ว

7) **การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น** (IT Outsourcing)

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อกลุ่มบริษัทในรูปแบบที่แตกต่างไปจากการดำเนินงานปกติโดยกลุ่มบริษัทเอง เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (Access risk) ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการประมวลผลของระบบงาน (Integrity risk) ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น ดังนั้น การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นจึงมีวัตถุประสงค์เพื่อให้กลุ่มบริษัทใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

7.1 การควบคุมผู้ให้บริการ

7.1.1 ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

7.1.2 ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข

ทั้งนี้ ให้มีผลตั้งแต่วันที่ 1 มิถุนายน 2555 เป็นต้นไป

ประกาศ ณ วันที่ 1 มิถุนายน 2555

ลงชื่อ .....

(นางสาวบุษบา ดาวเรือง)

ประธานเจ้าหน้าที่บริหารกลุ่ม

บริษัท จีเอ็มเอ็ม แกรมมี่ จำกัด (มหาชน)