(ฉบับปรับปรุงครั้งที่ 2)

ALLA | ONVALLA

เอกสาร บจ. หมวด ข
ลำดับที่ 015
เรื่อง นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

กลุ่มบริษัทตระหนักถึงความสำคัญในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงการกำหนดแนวทางปฏิบัติที่ชัดเจน เพื่อให้การดำเนินงานเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ กลุ่มบริษัทจึงได้มีการกำหนดนโยบายและแนวปฏิบัติการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยมีเนื้อหาครบถ้วนสอดคล้องตามกฎหมายที่แก้ไขเพิ่มเติมและมีการควบคุมภายในที่ดี ดังรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศฉบับนี้

ทั้งนี้ ให้มีผลตั้งแต่วันที่ 3 กุมภาพันธ์ 2569 เป็นต้นไป

(นายองอาจ ปัณฑุยากร)
ประธานเจ้าหน้าที่บริหาร

หมายเหตุ: 1. เพิ่มแนวทางปฏิบัติ การควบคุมการเข้าออกและการป้องกันความเสียหาย สำหรับระบบ Cloud
2. ปรับปรุงการตั้งค่าความปลอดภัยในระบบสารสนเทศตามแนวปฏิบัติที่ดีที่สุด (Leading Practice)

(ฉบับปรับปรุงครั้งที่ 2)

นโยบายการรักษาความปลอดภัย
ด้านเทคโนโลยีสารสนเทศ



บริษัท ออลล่า จำกัด (มหาชน)



และบริษัทในเครือ (บริษัท ออนวัลล่า จำกัด)

ผู้จัดทำและหน่วยงานที่รับผิดชอบ : ฝ่ายเทคโนโลยีและสารสนเทศ

สารบัญ

หน้า

บทนำ : นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ 3

1. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) 8

2. การควบคุมการเข้าออกและการป้องกันความเสียหาย ต่อห้องเก็บคอมพิวเตอร์ (Access Control & Physical Security) 10

3. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security) 14

4. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management) 20

5. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) 22

6. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation) 24

7. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) 25

8. การใช้งานระบบคอมพิวเตอร์และเครือข่ายสำหรับผู้ใช้งาน 26

9. การใช้อินเทอร์เน็ต (Internet) 28

10. การใช้งานจดหมายอิเล็กทรอนิกส์ (Email) 30

11. การใช้เครือข่ายสื่อสังคมออนไลน์ (Social Media) 31

บทนำ : นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย ของ บริษัท ออลล่า จำกัด (มหาชน) และบริษัทในเครือ ซึ่งต่อไปนี้จะเรียกว่า “บริษัท” ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ และเป็นมาตรฐานสากล
- เพื่อให้ระบบสารสนเทศขององค์กรมีความมั่นคงปลอดภัย ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
- เพื่อให้มีแนวทางปฏิบัติอย่างชัดเจน
- เพื่อให้ผู้มีส่วนได้ส่วนเสีย มีความพึงพอใจและมั่นใจในข้อมูลและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ขอบเขต

- ใช้กับทุกฝ่ายที่ประจำแต่ละสาขาขององค์กร ได้แก่ สำนักงานใหญ่มิตรภาพ สาขาโรงงานเทพราช สาขาบริการชลบุรี และสำนักงานใหญ่ออนวัลล่า นิมิตรใหม่
- ใช้สำหรับควบคุมและบังคับใช้สำหรับทุกฝ่ายภายในกลุ่มบริษัทและผู้เกี่ยวข้องภายนอก ในกิจกรรมต่าง ๆ ด้านเทคโนโลยีสารสนเทศ เช่น การเข้าถึงข้อมูลที่มีการจัดเก็บไว้ การบันทึกข้อมูล การทำรายงาน การใช้งานด้านการสื่อสารทั้งภายในและภายนอกองค์กร เป็นต้น
- ให้มีการควบคุมการใช้งาน ให้สอดคล้องและเป็นไปตามกฎหมายที่เกี่ยวข้อง เช่น กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์)
- ให้มีผลบังคับใช้กับทุกอุปกรณ์ ทั้งที่ติดตั้งภายในองค์กรและอุปกรณ์ที่ต้องนำไปใช้นอกสถานที่

แนวทางปฏิบัติ

- ดำเนินการจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร โดยผู้บริหารระดับสูง เจ้าหน้าที่ฝ่ายสารสนเทศ และผู้ใช้งานของแต่ละฝ่ายงาน มีส่วนร่วมในการจัดทำนโยบาย และได้รับการอนุมัติจากประธานเจ้าหน้าที่บริหารหรือคณะกรรมการบริษัท
- กำหนดให้มีการทบทวนและปรับปรุงนโยบาย ปีละหนึ่งครั้ง

- กำหนดให้มีการประเมินความเสี่ยง และระบุความเสี่ยงที่เกี่ยวข้อง จัดลำดับความสำคัญของข้อมูลและระบบคอมพิวเตอร์ กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง
- จัดเก็บนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้อง สามารถเข้าถึงได้โดยง่าย ในรูปแบบเอกสารหรือแบบไฟล์อิเล็กทรอนิกส์

รายละเอียดของนโยบาย

ประกอบด้วยหัวข้อ ดังนี้

1. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
2. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
3. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
4. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
5. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
6. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
7. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)
8. การใช้งานระบบคอมพิวเตอร์และเครือข่าย สำหรับผู้ใช้งาน
9. การใช้อินเทอร์เน็ต (Internet)
10. การใช้งานจดหมายอิเล็กทรอนิกส์ (Email)
11. การใช้เครือข่ายสื่อสังคมออนไลน์ (Social Media)

การปฏิบัติตามนโยบาย

- ขออนุมัติประกาศใช้และสื่อสารนโยบายให้แก่บุคคลที่เกี่ยวข้องอย่างทั่วถึง เพื่อให้สามารถปฏิบัติตามได้ รวมทั้งจัดการฝึกอบรมให้กับผู้ใช้งานระบบเทคโนโลยีสารสนเทศ
- ต้องแจ้งต่อผู้บริหารของบริษัทโดยเร็ว เมื่อมีกรณีที่ส่งผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ
- มีการจัดทำขั้นตอนหรือวิธีปฏิบัติเพื่อรองรับให้มีการปฏิบัติตามนโยบายที่ได้กำหนดไว้
- กำหนดหน้าที่และความรับผิดชอบของผู้ใช้งานและบุคคลที่เกี่ยวข้องอย่างชัดเจน

การฝ่าฝืนนโยบาย

- ผู้ที่มีหน้าที่รับผิดชอบและผู้ใช้งานในระบบสารสนเทศ ต้องปฏิบัติตามนโยบายฉบับนี้ หากมีการละเมิดนโยบาย ฝ่าฝืน จงใจกระทำความผิด อาจหรือมีผลให้เกิดความเสียหายต่อบริษัท จะถูกตักเตือนในครั้งแรกและให้ผู้จัดการฝ่ายผู้ใช้งานรับทราบ หากยังมีการละเมิดซ้ำ ผู้จัดการฝ่ายเทคโนโลยีและสารสนเทศรายงานต่อผู้บริหารระดับสูง และขออนุมัติ เพื่อส่งเรื่องให้ฝ่ายทรัพยากรบุคคลลงโทษตามระเบียบของบริษัท โดยอาจมีการพิจารณาโทษทางวินัยและเรียกค่าเสียหาย
- พนักงานและลูกจ้างที่ฝ่าฝืนข้อกำหนดนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยจงใจหรือประมาทเลินเล่อ และก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัท หรือบุคคลหนึ่งบุคคลใด บริษัทจะพิจารณาดำเนินการทางวินัยและความรับผิดทางแพ่งและอาญาแก่พนักงานและลูกจ้างนั้น ตามกฎหมาย ข้อบังคับ ระเบียบ หรือประกาศที่เกี่ยวข้อง
- ผู้บังคับบัญชาผู้ใด งดเว้น หรือละเว้นการปฏิบัติตามหน้าที่ และเป็นเหตุให้พนักงานหรือลูกจ้างที่อยู่ภายใต้การบังคับบัญชาของตน ฝ่าฝืนข้อกำหนดของนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ ให้นำบทบัญญัติในวรรคก่อนมาใช้บังคับโดยอนุโลม
- การฝ่าฝืนข้อกำหนดใด ๆ ตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ แม้จะไม่ก่อให้เกิดความเสียหายแก่บริษัท หรือบุคคลหนึ่งบุคคลใดก็ตาม ถ้าผู้บังคับบัญชาเห็นว่ามีเหตุอันสมควร อาจจะบันทึกในประวัติการปฏิบัติงานและจะใช้เป็นข้อมูลประกอบการพิจารณาต่ออายุสัญญาจ้าง การขึ้นเงินเดือน หรือ เลื่อนตำแหน่งด้วยก็ได้

คำจำกัดความ

นโยบาย คือกรอบและแนวทางในการปฏิบัติหรือตัดสินใจเพื่อให้การดำเนินการต่าง ๆ บรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้อย่างมีประสิทธิภาพ นโยบายถือเป็นคำสั่ง หากผู้ใดต้องการทำสิ่งใดก็ตามที่ถือเป็นการไม่ยินยอมปฏิบัติตามนโยบาย ต้องได้รับการอนุมัติเป็นกรณีพิเศษ

บริษัท หมายถึง บริษัท ออลล่า จำกัด (มหาชน) ทั้ง 3 สาขา คือ สำนักงานใหญ่มิตรภาพ สาขาโรงงานเทพราช และสาขาบริการชลบุรี รวมทั้งบริษัทในเครือ ได้แก่ บริษัท ออนวัลล่า จำกัด

ผู้บริหารระดับสูง หมายถึง ผู้บริหารระดับผู้จัดการทั่วไปขึ้นไป ในแต่ละฝ่ายงานของบริษัท รวมทั้งผู้มีอำนาจสูงสุดของบริษัท

ผู้มีอำนาจอนุมัติ หมายถึง ผู้บังคับบัญชาแต่ละฝ่าย รวมทั้งผู้บริหารระดับสูง ประธานเจ้าหน้าที่บริหาร และคณะกรรมการบริษัท

ผู้บริหารฝ่ายเทคโนโลยีและสารสนเทศ หมายถึง ผู้ที่มีอำนาจบริหารจัดการและตัดสินใจในการดำเนินงานเกี่ยวกับระบบสารสนเทศ ตามนโยบายของบริษัท

ผู้ดูแลระบบสารสนเทศ หมายถึง ผู้ที่มีหน้าที่รับผิดชอบในการดูแลรักษาระบบงานระบบเครือข่ายคอมพิวเตอร์ที่สามารถเข้าถึงระบบเครือข่ายคอมพิวเตอร์ และระบบงานได้ทุกระบบ และอาจมีการกำหนดระดับการเข้าถึงตามที่ได้รับมอบหมายจากผู้บริหารฝ่ายเทคโนโลยีและสารสนเทศ

ผู้ใช้งาน หมายถึง พนักงาน ผู้บริหารทุกระดับ ของบริษัท และบุคคลภายนอกที่ได้รับสิทธิให้สามารถเข้าใช้งานระบบสารสนเทศของบริษัทได้ โดยสิทธิและหน้าที่ที่ขึ้นอยู่กับบทบาทที่บริษัทกำหนด

สิทธิของผู้ใช้งาน หมายถึง สิทธิที่เกี่ยวข้องกับระบบสารสนเทศของบริษัท

เทคโนโลยีสารสนเทศ (Information Technology – I.T.) หมายถึง เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งครอบคลุมถึงการรับ-ส่ง การแปลง การจัดเก็บ การประมวลผล และการค้นคืนสารสนเทศ โดยมีองค์ประกอบ 3 ส่วน คือ คอมพิวเตอร์ การสื่อสาร และสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบ ให้ผู้ใช้เข้าใจง่ายซึ่งอาจจะอยู่ในรูปแบบของ ตัวเลข ข้อความ หรือกราฟ สามารถนำไปใช้ในขบวนการบริหารจัดการ การวางแผน การตัดสินใจได้

ระบบสารสนเทศ (Information System) หมายถึง โครงสร้างของอุปกรณ์และโปรแกรม ที่เกี่ยวข้องกับสารสนเทศ

ศูนย์คอมพิวเตอร์ (Computer Center) หมายถึงสถานที่ติดตั้งอุปกรณ์คอมพิวเตอร์ที่สำคัญ ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่าย (Networking Devices) และอุปกรณ์อื่น ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ โดยมีการควบคุมด้านความปลอดภัยทุก ๆ ด้าน เพื่อให้การทำงานของระบบคอมพิวเตอร์ มีความมั่นคงและง่ายต่อการปฏิบัติงาน

การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ หมายถึง การดูแลปกป้องระบบสารสนเทศให้มั่นคงปลอดภัย เพื่อป้องกันการละเมิดหรือการบุกรุก โดยมีองค์ประกอบ 3 ประการคือ ความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) ความพร้อมใช้งาน (Availability)

ความลับ (Confidentiality) หมายถึง การรักษาความลับของสารสนเทศ เพื่อทำให้มั่นใจว่ามีเฉพาะผู้ที่มีสิทธิ์หรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงได้

การรักษาความถูกต้อง/สมบูรณ์ (Integrity) หมายถึง การปกป้องสารสนเทศให้มีความถูกต้องสมบูรณ์ สามารถแก้ไขได้เฉพาะผู้ที่มีสิทธิ์หรือได้รับอนุญาตเท่านั้น

ความพร้อมใช้งาน (Availability) หมายถึง การทำให้ระบบสารสนเทศมีประสิทธิภาพเพียงพอ สามารถใช้งานจากผู้ที่มีสิทธิได้เมื่อต้องการ

กฎหมายที่เกี่ยวข้อง

การใช้งานระบบสารสนเทศ ด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ สอดคล้องกับกฎหมายดังต่อไปนี้

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ 1 พ.ศ. 2550
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ 2 พ.ศ. 2560
- พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2558 (ฉบับที่ 2 และฉบับที่ 3)

1. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

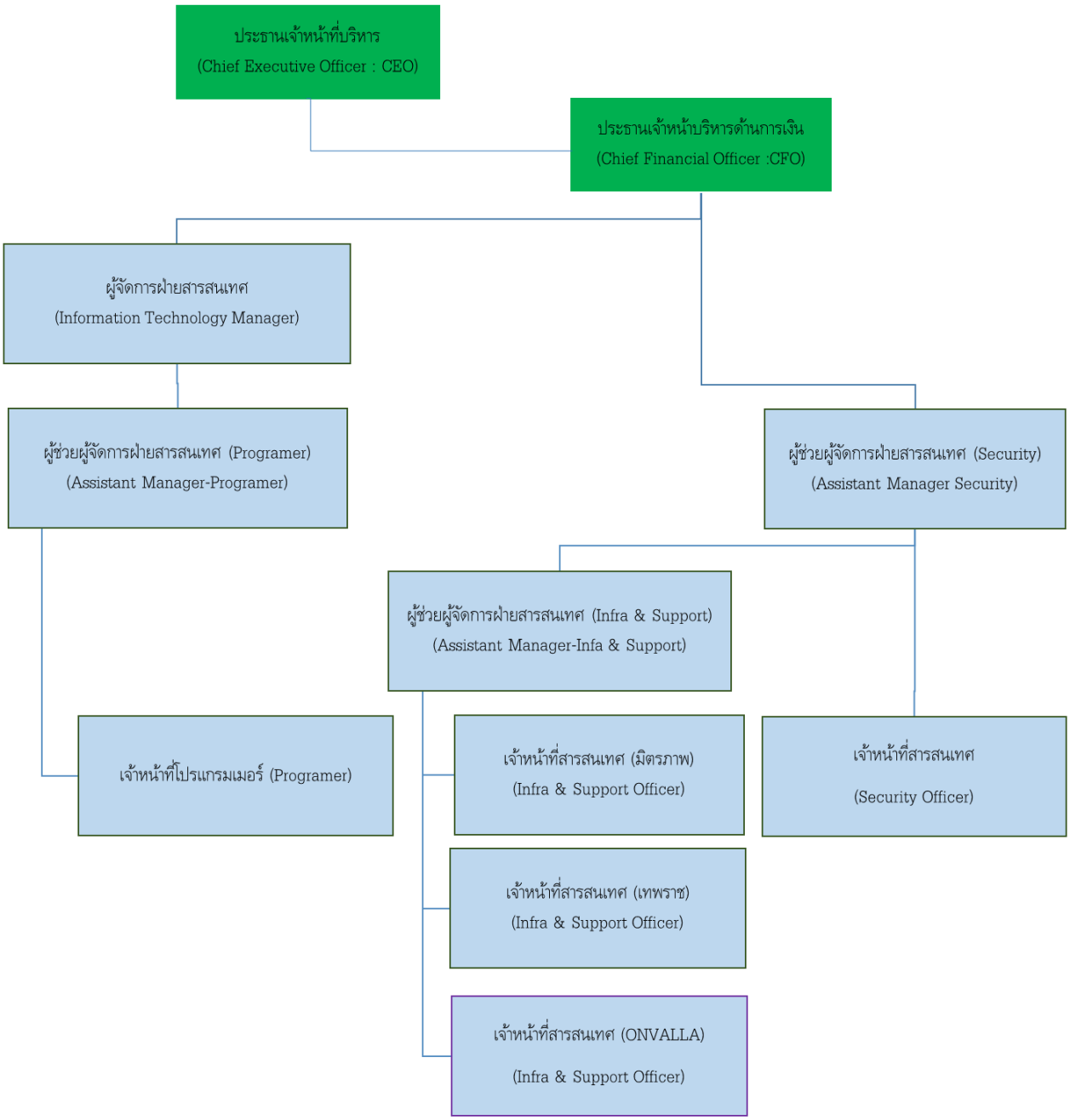
วัตถุประสงค์

- เพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายเทคโนโลยีและสารสนเทศ ซึ่งเป็นการลดความเสี่ยงด้าน Infrastructure risk

แนวทางปฏิบัติ

- บริษัทกำหนดให้มีการแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment)
- กำหนดให้ระบุขอบเขตหน้าที่และความรับผิดชอบเป็นลายลักษณ์อักษรลงใน Job Description ซึ่งระบุรายละเอียดหน้าที่หลัก หน้าที่รอง และความรับผิดชอบการทำงาน
- กำหนดแนวทางการทำงานในงานที่มีความสำคัญทดแทนกันได้ในกรณีจำเป็น

ผังโครงสร้าง


ประธานเจ้าหน้าที่บริหาร
(Chief Executive Officer : CEO)
ประธานเจ้าหน้าบริหารด้านการเงิน
(Chief Financial Officer :CFO)
ผู้จัดการฝ่ายสารสนเทศ
(Information Technology Manager)
ผู้ช่วยผู้จัดการฝ่ายสารสนเทศ (Programer)
(Assistant Manager-Programer)
ผู้ช่วยผู้จัดการฝ่ายสารสนเทศ (Security)
(Assistant Manager Security)
ผู้ช่วยผู้จัดการฝ่ายสารสนเทศ (Infra & Support)
(Assistant Manager-Infa & Support)
เจ้าหน้าที่โปรแกรมเมอร์ (Programer)
เจ้าหน้าที่สารสนเทศ (มิตรภาพ)
(Infra & Support Officer)
เจ้าหน้าที่สารสนเทศ
(Security Officer)
เจ้าหน้าที่สารสนเทศ (เทพราช)
(Infra & Support Officer)
เจ้าหน้าที่สารสนเทศ (ONVALLA)
(Infra & Support Officer)

2. การควบคุมการเข้าออกและการป้องกันความเสียหาย ต่อศูนย์คอมพิวเตอร์ (Access Control & Physical Security)

วัตถุประสงค์

- เพื่อควบคุมการเข้าออกศูนย์คอมพิวเตอร์ ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าถึง ล่วงรู้ (Access risk) แก้ไขเปลี่ยนแปลง (Integrity risk) หรือก่อให้เกิดความเสียหายต่ออุปกรณ์ระบบคอมพิวเตอร์ (Availability Risk) โดยมีการบันทึกทั้งทางอิเล็กทรอนิกส์หรือเป็นเอกสาร
- เพื่อการป้องกันความเสียหาย ต่ออุปกรณ์ระบบคอมพิวเตอร์ ได้แก่ คอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายต่าง ๆ รวมทั้งอุปกรณ์ทั้งหมด ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ (Availability Risk) เช่น ไฟไหม้ น้ำท่วม เป็นต้น
- เพื่อควบคุมและจำกัดการเข้าถึงระบบคอมพิวเตอร์ทั้งแบบ On-premise และระบบ Cloud โดยต้องมั่นใจว่าผู้มีสิทธิ์เข้าถึงเท่านั้นที่สามารถใช้งานได้ตามขอบเขตหน้าที่ที่ได้รับมอบหมาย
- เพื่อป้องกันการบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาตไม่ว่าจะเป็นทางกายภาพหรือผ่านระบบเครือข่ายในกรณีของระบบ Cloud

แนวทางปฏิบัติ

สำหรับระบบ On-premise

1. การควบคุมศูนย์คอมพิวเตอร์
    - กำหนดให้จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ ได้แก่ เครื่องแม่ข่ายรวมทั้งอุปกรณ์เครือข่าย ไว้ในห้องหรือพื้นที่ที่กำหนด โดยมีขนาดที่เหมาะสม
    - กำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเป็นประจำ ได้แก่ เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ดูแลระบบ (System Administrator) เป็นต้น โดยให้ติดตั้งระบบ Access Control มีการใช้ Finger Scan และรหัสผ่านในการควบคุมการเข้าพื้นที่
    - กำหนดให้มีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ (Log) โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และมีการตรวจสอบบันทึกดังกล่าวเป็นประจำทุกเดือน โดยทำเป็นรายงานเสนอให้ผู้จัดการฝ่ายรับทราบ กำหนดให้เก็บ Log ไว้ 1 ปี
    - ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ และมีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ในบางครั้ง ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีเจ้าหน้าที่ฝ่ายเทคโนโลยีและสารสนเทศควบคุมดูแลการทำงานตลอดเวลา เป็นต้น รวมทั้งให้มีการบันทึกรายละเอียดการเข้าออกและวัตถุประสงค์ไว้ในเอกสาร

ทุกครั้ง และมีการตรวจสอบบันทึกดังกล่าวเป็นประจำ โดยให้ผู้จัดการฝ่ายเป็นผู้รับทราบ กำหนดให้เก็บเอกสารไว้ 1 ปี

- จัดวางอุปกรณ์คอมพิวเตอร์ให้เป็นสัดส่วน เพื่อสะดวกในการปฏิบัติงาน เพื่อให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น
- ห้ามมิให้นำอุปกรณ์หรือชิ้นส่วนใดออกจากศูนย์คอมพิวเตอร์ เว้นแต่ จะได้รับอนุญาตจากผู้บริหารระดับสูง หรือผู้จัดการฝ่าย เท่านั้น
- กรณีที่เกิดเหตุฉุกเฉินนอกเวลางาน จำเป็นต้องให้เจ้าหน้าที่รักษาความปลอดภัยเข้าตรวจสอบ ให้เจ้าหน้าที่รักษาความปลอดภัยในเวลานั้น โทรศัพท์แจ้งให้กับผู้จัดการฝ่ายเทคโนโลยีและสารสนเทศ
- เพื่อรับรหัสผ่าน โดยให้เปลี่ยนรหัสทุกครั้งหลังจากเสร็จสิ้นงานดังกล่าวแล้ว

2. การป้องกันความเสียหาย

2.1 ระบบป้องกันไฟไหม้

- ติดตั้งอุปกรณ์ตรวจจับและเตือนไฟไหม้ เช่น เครื่องตรวจจับควันไฟ (Smoke Detector) อุปกรณ์ส่งเสียงเตือน ได้แก่ ออดหรือไซเรน เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา
- ให้มีถังดับเพลิงติดตั้งไว้ทั้งภายในและหน้าศูนย์คอมพิวเตอร์ เพื่อใช้สำหรับการดับเพลิงในเบื้องต้น โดยให้ฝ่ายที่รับผิดชอบด้านความปลอดภัยภายในบริษัทเป็นผู้ดูแลอุปกรณ์ ให้มีสภาพพร้อมใช้งาน

2.2 ระบบป้องกันไฟฟ้าขัดข้อง

- กำหนดให้มีอุปกรณ์ป้องกันมิให้ระบบคอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ ได้แก่เครื่องสำรองไฟ (UPS) ที่มีคุณภาพตามมาตรฐานสากล และออกแบบขนาดที่เหมาะสม เพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่องอย่างน้อย 45 นาที หรือมากกว่านั้น ขึ้นอยู่กับลักษณะการใช้งานของแต่ละสถานที่ โดยอุปกรณ์ต้องมีระบบเก็บบันทึกเหตุการณ์ต่างๆ (Event Logs) สามารถตรวจสอบย้อนหลังได้ เพื่อนำมาวิเคราะห์ความผิดปกติ หรืออายุของอุปกรณ์ได้

2.3 ระบบควบคุมอุณหภูมิและความชื้น

- ติดตั้งเครื่องปรับอากาศอย่างน้อย 2 เครื่อง และมีระบบควบคุมการทำงานสลับกันในเวลาทุก ๆ 4 ชั่วโมง เพื่อให้มีอุณหภูมิและความชื้นที่เหมาะสม ตามมาตรฐานที่กำหนด โดยเครื่องปรับอากาศต้องมีขนาดที่เหมาะสมและมีอย่างน้อย 2 เครื่อง และมีระบบควบคุมการทำงานสลับกันในเวลาทุก ๆ 4 ชั่วโมง มีการเก็บบันทึกเหตุการณ์ตลอดเวลาโดยอุปกรณ์อิเล็กทรอนิกส์ และบันทึกลงเอกสารรายวันโดยเจ้าหน้าที่ และทำรายงานเสนอให้ผู้จัดการฝ่ายรับทราบ ทุกๆเดือน

สำหรับระบบ Cloud

สำหรับระบบสารสนเทศที่ใช้งานบน Cloud ให้กำหนดและบังคับใช้มาตรการควบคุมเพิ่มเติมจากระบบ On-premise โดยคำนึงถึงลักษณะความเสี่ยงที่แตกต่างกันของ Cloud Computing ทั้งด้านการเข้าถึง การประมวลผลข้อมูล และการพึ่งพาผู้ให้บริการภายนอก โดยมีแนวทางปฏิบัติดังต่อไปนี้

1. การควบคุมการเข้าถึงระบบ Cloud

- ต้องบังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับผู้ใช้งานทุกระดับ โดยเฉพาะบัญชีที่มีสิทธิ์สูง
- ต้องกำหนดสิทธิ์การใช้งานตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) หรือระบบการบริหารจัดการตัวตนและสิทธิ์ (IAM) เพื่อให้ผู้ใช้งานเข้าถึงทรัพยากรได้เฉพาะที่จำเป็นต่อหน้าที่
- ต้องมีการจัดเก็บ ตรวจสอบ และทบทวนบันทึกการใช้งานและกิจกรรมต่าง ๆ (Audit Logs) อย่างสม่ำเสมอ เพื่อรองรับการตรวจสอบด้านความปลอดภัยและการ Audit
- ห้ามใช้บัญชีผู้ดูแลระบบ (Administrator) ร่วมกันโดยเด็ดขาด และต้องสามารถระบุตัวตนของผู้ปฏิบัติงานได้อย่างชัดเจน (Accountability)

2. การแยกพื้นที่การประมวลผลใน Cloud

- ต้องแบ่งสภาพแวดล้อมการทำงาน (Environment) เช่น Development, Test และ Production ออกจากกันอย่างชัดเจน เพื่อลดความเสี่ยงจากการเปลี่ยนแปลงหรือความผิดพลาดที่อาจกระทบระบบจริง
- การเข้าถึงหรือดำเนินการใด ๆ บนระบบ Production ต้องได้รับการอนุมัติจากผู้มีอำนาจตามสายงาน และต้องมีการบันทึกหลักฐานการอนุมัติไว้ตรวจสอบได้

3. ความมั่นคงปลอดภัยของระบบ Cloud

- ต้องมีการเข้ารหัสข้อมูลทั้งขณะจัดเก็บ (Data at-rest) และขณะรับ-ส่งข้อมูล (Data in-transit) ตามมาตรฐานสากล เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ผู้ให้บริการ Cloud ต้องผ่านการรับรองมาตรฐานด้านความมั่นคงปลอดภัยที่เหมาะสม เช่น ISO/IEC 27001 หรือมาตรฐานที่เทียบเท่า
- ต้องจัดทำแผนสำรองและกู้คืนระบบ (Disaster Recovery Plan: DRP) รวมถึงแผน Exit Strategy เพื่อรองรับกรณีเปลี่ยนผู้ให้บริการหรือยกเลิกการใช้งาน Cloud ในอนาคต โดยไม่กระทบต่อความต่อเนื่องทางธุรกิจ

4. การควบคุมการเข้าถึงจากภายนอกและบุคคลภายนอก

- การเข้าถึงระบบ Cloud จากเครือข่ายภายนอกองค์กรต้องผ่านช่องทางที่มีการควบคุมความปลอดภัย เช่น VPN หรือวิธีการที่เทียบเท่า
- การให้สิทธิ์แก่บุคคลภายนอก เช่น ผู้ให้บริการหรือที่ปรึกษา ต้องมีข้อตกลงและเงื่อนไขที่ชัดเจน ทั้งด้านขอบเขตงาน ความลับของข้อมูล และระยะเวลาการเข้าถึง พร้อมมีการยกเลิกสิทธิ์ทันทีเมื่อสิ้นสุดความจำเป็น

หมายเหตุ

การควบคุมความปลอดภัยของระบบ Cloud ให้เป็นไปตามแนวทางที่กำหนดไว้ใน “นโยบายการพิจารณาและนำระบบ Cloud มาใช้ในองค์กร” ในหมวดข้อกำหนดด้านความปลอดภัยและการบริหารจัดการความเสี่ยง โดยให้ถือเป็นกรอบอ้างอิงหลักในการกำหนดมาตรการควบคุมเพิ่มเติมทุกกรณี

3. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

- เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง
- เพื่อป้องกันการบุกรุกผ่านระบบเครือข่าย ได้แก่ Hacker ไวรัส รวมทั้ง Malicious Code ต่าง ๆ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ใด ๆ ในระบบ
- มีแนวปฏิบัติครอบคลุมเกี่ยวกับการรักษาความปลอดภัยข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย ระบบเครือข่าย และอุปกรณ์ทั้งหมด ทั้งภายในและภายนอกบริษัท

แนวทางปฏิบัติ

1. การบริหารจัดการข้อมูล
   - กำหนดชุดของข้อมูลที่ใช้ในการดำเนินธุรกิจในโปรแกรม ERP ของแต่ละฝ่ายหรือแต่ละผู้ใช้งานที่มีหน้าที่ต่าง ๆ เพื่อควบคุมการเข้าถึงข้อมูลผ่านระบบงานของแต่ละฝ่าย โดยให้ผู้บริหารระดับสูงเป็นผู้อนุมัติ
   - ควบคุมการเข้าถึงระบบฐานข้อมูลโดยตรงของโปรแกรมต่าง ๆ โดยการกำหนดสิทธิและขั้นตอนที่เหมาะสม ให้แก่ผู้ดูแลระบบ
   - การเข้าถึงข้อมูลสำคัญทางธุรกิจจากระยะไกลผ่านเครือข่ายสาธารณะ กำหนดให้มีการใช้ VPN (Virtual Private Network) และมีเข้าการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล
   - กำหนดให้มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) อย่างถูกต้อง สามารถตรวจสอบเหตุการณ์ได้ (Log)
   - กำหนดให้มีมาตรการรักษาความปลอดภัยข้อมูลในกรณีมีการส่งซ่อมเครื่องคอมพิวเตอร์ให้กับผู้ซ่อมภายนอก โดยถอดสื่อบันทึกออก เป็นต้น ยกเว้นเป็นการซ่อมตัวอุปกรณ์บันทึก ให้มีการเลือกผู้ซ่อมที่มีการเก็บรักษาข้อมูลเป็นความลับ
2. การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)
   - มีการกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application System) สิทธิการใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าว ทุกเดือน หรือทันทีที่มีการเปลี่ยนแปลง
   - กำหนดผู้ดูแลเฉพาะ สำหรับระบบงาน ERP ซึ่งแบ่งเป็นแต่ละส่วนที่สำคัญ ได้แก่

- Database Administration
- User Administration
- User/application support
- Change the report program/ update data on production
- Move the program developed and change to production

- หากจำเป็นต้องให้สิทธิพิเศษหรือระดับสูงสุด (Administrator) แก่ผู้ใช้งาน ต้องมีการควบคุมอย่างรัดกุม โดยกำหนดดังต่อไปนี้
  - ได้รับความเห็นชอบจากผู้บริหารฝ่ายเทคโนโลยีและสารสนเทศ
  - จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
  - กำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
  - กำหนดให้ระบบมีการเปลี่ยนรหัสผ่านอัตโนมัติ หรือให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามความจำเป็น โดยรหัสผ่านจะต้องถูกเปลี่ยนทุก 3 เดือนหลังจากการเปลี่ยนรหัสครั้งล่าสุด
  - ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ กำหนดให้มีตั้งค่าการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง โดยกำหนดให้ผู้ใช้งานออกจากระบบงานโดยอัตโนมัติ (log out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ หากมีเวลานานเกินกว่า 15 นาที
  - ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญ มีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ share files เป็นต้น จะต้องให้ผู้จัดการฝ่ายดังกล่าวเป็นผู้อนุมัติและให้ผู้ดูแลระบบเป็นผู้ดำเนินการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว
  - ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว กำหนดให้มีการขออนุมัติจากผู้มีอำนาจหน้าที่ที่เกี่ยวข้องทุกครั้ง โดยบันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
  - กำหนดให้มีการตรวจสอบสิทธิการใช้งานของผู้ใช้งานในระบบสารสนเทศ 1 ครั้งต่อปี โดยจะต้องมีการลงนามตรวจสอบของผู้ใช้งาน หัวหน้า หรือผู้ตรวจสอบการทำงาน

3. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password)
   - กำหนดให้มีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ ได้แก่ กำหนดแนวทางการตั้งรหัสผ่านให้ยากแก่การคาดเดา และกำหนดให้ผู้ใช้งานแต่ละรายมี User account เป็นของตนเอง

- กำหนดวิธีการตั้งรหัสผ่านที่มีความยากแก่การคาดเดา (Complexity) ดังต่อไปนี้
  - กำหนดให้รหัสผ่านมีความยาวขั้นต่ำ 10 ตัวอักษร ซึ่งเป็นมาตรฐานสากลโดยส่วนใหญ่
  - ต้องใช้อักขระพิเศษประกอบ เช่น : ; < > เป็นต้น
  - ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำ 5 ครั้งล่าสุด
  - ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”, “aaaaaa”, “123456”, “admin”, “password” เป็นต้น
  - ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
  - ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
- สำหรับผู้ใช้งานทั่วไป กำหนดให้เปลี่ยนรหัสผ่านโดยอัตโนมัติทุก ๆ 3 เดือน หรือตามความจำเป็น ในกรณีที่เป็นข้อจำกัดของ Application กำหนดให้ฝ่ายสารสนเทศ ส่ง e-mail แจ้งเตือนผู้ใช้งานให้เปลี่ยนรหัสผ่านทุก 3 เดือนแทนระบบอัตโนมัติ
- สำหรับผู้ใช้งานบนระบบ MA SQL Server กรณี User “sa” มีการกำหนดการเปลี่ยนรหัสผ่าน ก็ต่อเมื่อมีการเบิกใช้งานรหัสผ่าน อ้างอิงตาม Document Procedure (DP-IT-01) โดยได้รับการตรวจสอบจากผู้จัดการฝ่าย
- สำหรับผู้ใช้งานที่มีสิทธิพิเศษหรือระดับสูงสุด เช่น ผู้บริหารระบบ (System Administrator) กำหนดให้เปลี่ยนรหัสผ่าน ทุก ๆ 3 เดือน หรือตามความจำเป็น
- สำหรับผู้ใช้งานด้านโปรแกรมระบบ ERP กำหนดให้ผู้ใช้เปลี่ยนรหัสผ่านทุก ๆ 3 เดือน หรือตามความจำเป็น
- กรณีที่เป็น Username ที่มีอยู่ในระบบ และไม่ควรเปลี่ยนรหัสโดยไม่จำเป็น เนื่องจากมีผลกระทบต่อระบบ ให้ขออนุมัติต่อผู้บริหารระดับสูง โดยแจ้งเหตุผลประกอบ
- ระบบจะจำกัดจำนวนครั้งในการป้อนรหัสผ่านผิดไม่เกิน 5 ครั้งภายในระยะเวลา 60 นาที (Reset Account Lockout Counter After) หากผู้ใช้งานป้อนรหัสผิดไม่เกิน 5 ครั้งในช่วงเวลาดังกล่าว ระบบจะรีเซ็ตจำนวนครั้งที่ป้อนรหัสผิดให้เป็น 0 และเริ่มนับจำนวนครั้งใหม่หากเวลาผ่านไปเกิน 60 นาที
- กรณีที่ผู้ใช้งานใส่รหัสผ่านผิดเกิน 5 ครั้ง ระบบจะล็อคทำให้ไม่สามารถใช้งานได้ ผู้ใช้งานต้องทำเอกสารขออนุมัติเพื่อปลดล็อค เนื่องจากระบบจะไม่ปลดเอง ต้องให้ผู้ดูแลระบบเป็นผู้ปลดล็อค (Account Lockout Duration)
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่านนั้นโดยทันที
- ผู้ใช้งานต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที

- ตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของพนักงานที่ลาออกแล้ว เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น disable หรือ ลบออกจากระบบ หรือ เปลี่ยน password เป็นต้น

4. การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)
   - กำหนดให้มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย โดยในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการทำบันทึก
   - กำหนดให้เปิดใช้บริการ (service) เท่าที่จำเป็น
   - ดำเนินการติดตั้ง patch ที่จำเป็นของระบบงานสำคัญ (Operating System) อย่างสม่ำเสมอ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software)
   - กำหนดให้ผู้ดูแลระบบรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของโปรแกรมระบบ
   - การสร้างข้อมูลบนฐานข้อมูลจริงบนเครื่องคอมพิวเตอร์แม่ข่ายใช้งาน (Production) ตามที่ได้รับการอนุมัติการเปลี่ยนแปลงมาแล้ว ต้องให้ผู้จัดการฝ่ายเป็นผู้อนุมัติ
   - ปรับตั้งค่าการเก็บบันทึกข้อมูลตรวจสอบการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย Domain Controller ดังนี้
     - Audit account Logon Events = Success and Failure
     - Audit account management = Success and Failure
     - Audit directory service access = Failure
     - Audit Logon Events = Success and Failure
     - Audit Object Access = Failure
     - Audit policy change = Success and Failure
     - Audit privilege use = Failure
     - Audit system events = Failure
   - กำหนดให้เจ้าหน้าที่ที่ไม่ใช่ผู้ดูแลระบบเป็นผู้สอบทานการเข้าใช้งานในระบบ จากข้อมูลตาม Log ที่ทำการจัดเก็บไว้เดือนละ 1 ครั้ง และจัดทำเป็นรายงานเสนอต่อผู้จัดการฝ่ายเทคโนโลยีและสารสนเทศ

5. การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)
   - กำหนดให้มีการแบ่งแยกระบบเครือข่าย เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก

- กำหนดให้ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายภายในกับเครือข่ายสาธารณะภายนอก โดยสามารถตรวจสอบการบุกรุก และการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย ดังต่อไปนี้
  - ความพยายามในการบุกรุกผ่านระบบเครือข่าย
  - การใช้งานในลักษณะที่ผิดปกติ
  - การใช้งานและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
- จัดทำแผนผังระบบเครือข่าย (Network diagram) โดยมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- กำหนดให้ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่าพารามิเตอร์ (parameter) ต่าง ๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (physical disconnect) และจุดเชื่อมต่อ (disable port) ที่ไม่มีความจำเป็นในการเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง
- ในกรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ Remote access หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้ระบบอินเทอร์เน็ต ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และมีการควบคุมอย่างเข้มงวด ได้แก่ การตรวจสอบตัวตนจริงและสิทธิของผู้ใช้งาน และตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว
- กำหนดให้ผู้ดูแลระบบรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าพารามิเตอร์ (parameter) ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่าย และมีการทบทวนการกำหนดค่าพารามิเตอร์ (parameter) ต่าง ๆ ปี 1 ละครั้ง
- การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจเช็คระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6. การเปลี่ยนแปลงระบบคอมพิวเตอร์ (Configuration Management)
   - ก่อนการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์ ต้องมีการประเมินผลกระทบที่เกี่ยวข้อง และบันทึกการเปลี่ยนแปลงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ
   - การติดตั้งซอฟต์แวร์ต้องติดตั้งเท่าที่จำเป็นแก่การใช้งาน และถูกต้องตามลิขสิทธิ์เท่านั้น
7. การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (Capacity Planning)
   - กำหนดแผนประเมินการใช้งานระบบคอมพิวเตอร์สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคตอย่างน้อย 1 ครั้งต่อปี
8. การป้องกันไวรัส และ malicious code

- มีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ โดยติดตั้งซอฟต์แวร์ป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง
- ควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้
- ผู้ใช้งานต้องแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีไวรัสอยู่ในเครื่อง

9. บันทึกเพื่อการตรวจสอบ (Audit logs)
    - กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการใช้งานระบบอินเทอร์เน็ต
    - มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งาน (Log monitoring) ทุกเดือน
    - กำหนดให้มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกต่าง ๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

4. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

วัตถุประสงค์

เพื่อให้ระบบสารสนเทศที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลง มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity risk โดยกำหนดให้แนวทางครอบคลุมกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้น ซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง โดยการแก้ไขเปลี่ยนแปลงอาจมีผลทำให้การทำงานมีประสิทธิภาพมากขึ้น

แนวทางปฏิบัติ

1. การกำหนดขั้นตอนการปฏิบัติงาน
   - กำหนดให้มีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ การพัฒนา หรือแก้ไขเปลี่ยนแปลง และการทดสอบ
   - มีการสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม
2. การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงาน

   2.1 การร้องขอ
   - การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศ ได้แก่ ระบบ ERP โครงสร้างระบบสารสนเทศ (Infrastructure) และโปรแกรมใช้งานต่าง ๆ (Applications Software) ต้องจัดทำรายละเอียดประกอบ เช่น จุดประสงค์ ขอบเขต วิธีการดำเนินการ ประโยชน์ที่จะได้รับ รวมทั้งงบประมาณที่ต้องใช้ ให้เป็นลายลักษณ์อักษร และได้รับอนุมัติจากผู้บริหารระดับสูงที่รับผิดชอบในสายงานธุรกิจ
   - ให้มีการสอบทานและประเมินความเสี่ยงก่อนทุกครั้ง เนื่องจากการเปลี่ยนแปลงอาจส่งผลกระทบต่อการปฏิบัติงานของหน่วยงานหรือทั้งบริษัท และอาจมีผลกระทบต่อการปฏิบัติภายใต้กฎหมาย

   2.2 การปฏิบัติงานพัฒนาระบบงาน
   - กำหนดให้มีการแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) ออกจากส่วนที่ใช้งานจริง (production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น โดยการแบ่งแยกส่วนตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

- กำหนดให้พิจารณาเกี่ยวกับระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง ควบคู่กันไป

2.3 การทดสอบ

- ผู้ที่ร้องขอและฝ่ายเทคโนโลยีและสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้อง ต้องมีส่วนร่วมในการทดสอบเพื่อให้มั่นใจว่าระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลง มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง โดยมีการจัดทำเอกสารประกอบการทดสอบระบบและลงนามยืนยันโดยผู้ร้องขอ ผู้ทดสอบทั้งหมด ผู้เกี่ยวข้อง และผู้พัฒนาระบบ โดยเอกสารดังกล่าวต้องระบุรายละเอียดต่าง ๆ รวมทั้งแผนงานดำเนินการ

2.4 การโอนย้ายระบบงานเพื่อใช้งานจริง

- ต้องได้รับการอนุมัติจากผู้บริหารระดับสูง โดยทำเป็นเอกสารพร้อมแนบผลการทดสอบระบบ
- กำหนดให้มีแผนงานโอนย้ายระบบ
- ตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วน

2.5 การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ version ของระบบงานที่ได้รับการพัฒนา

- กำหนดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
- ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน
- ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งาน ในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

2.6 การทดสอบหลังการใช้งาน (post- implementation test)

- กำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งอาจมีการสอบถามโดยตรงกับผู้ใช้งาน เพื่อเก็บข้อมูล

2.4 การสื่อสารการเปลี่ยนแปลง

- ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง โดยอาจใช้วิธีการอบรมเพิ่มเติมเกี่ยวกับระบบงานที่เปลี่ยนแปลงและระบบงานที่เกี่ยวข้อง

5. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

วัตถุประสงค์

เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (availability risk) หากเกิดปัญหากับอุปกรณ์หลัก (Production) หรือเกิดภัยพิบัติ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

แนวทางปฏิบัติ

1. การสำรองข้อมูลและระบบคอมพิวเตอร์

1.1. การสำรอง

- กำหนดให้มีการสำรองข้อมูลระบบงาน ERP ได้แก่ โปรแกรมระบบปฏิบัติการ (Operating system) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และข้อมูล (Database) ให้มีความพร้อมสามารถกลับนำมาใช้งานได้อย่างต่อเนื่อง ถูกต้อง
- การสำรองข้อมูล มีการกำหนดดังนี้
    - สำรองข้อมูลที่สำคัญทางธุรกิจ ได้แก่ ข้อมูลระบบงาน ERP ระบบงาน HR
    - ความถี่ในการสำรอง มากที่สุดเท่าที่ระบบสามารถทำได้
    - ประเภทสื่อบันทึก (media) ได้แก่ ระบบ Hard disk บนเครื่องแม่ข่ายสำรอง External Drive
    - จำนวนที่ต้องสำรองอย่างน้อย 1 ชุด ต้องเก็บนอกสถานที่ที่ติดตั้งระบบคอมพิวเตอร์
    - ขั้นตอนและวิธีการสำรองเป็นไปตามที่ระบุในคู่มือของโปรแกรม
    - มีการบันทึกการปฏิบัติงาน (Log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน โดยให้ผู้จัดการฝ่ายรับทราบทุกเดือน

1.2. การทดสอบ

- มีการทำขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน
- กำหนดให้มีการทดสอบข้อมูลที่ได้สำรองไว้ ปีละ 1 ครั้ง ในช่วงเวลาที่เหมาะสม เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้จริง

1.3. การเก็บรักษา

- จัดเก็บข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆไว้ทั้งในและนอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย
- ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน กำหนดให้ทบทวนวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย โดยกำหนดให้ทบทวนปีละ 1 ครั้ง
- การขอใช้งานข้อมูลสำรองที่บันทึกไว้ ต้องได้รับอนุมัติจากผู้บริหารระดับสูง และจัดเก็บประวัติการส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ รวมทั้งวันเวลา

2. การเตรียมพร้อมกรณีฉุกเฉิน
   - กำหนดให้มีแผนฉุกเฉิน เพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินมีรายละเอียด ดังนี้
   - จัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน
   - กำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา
   - จัดทำขั้นตอนการแก้ไขปัญหาในแต่ละสถานการณ์
   - กำหนดเจ้าหน้าที่รับผิดชอบและผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด
   - จัดทำรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (specification) ขั้นต่ำ ค่าจ้างทำระบบ (Configuration) และอุปกรณ์เครือข่าย เป็นต้น
   - ปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่
   - ทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย
   - มีการสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น
   - ในกรณีเกิดเหตุการณ์ฉุกเฉิน มีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

6. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

วัตถุประสงค์

เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่าง ๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity risk และ Availability risk

แนวทางปฏิบัติ

1. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์
   - จัดทำขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญ เป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer operator)
2. การติดตามการทำงานของระบบคอมพิวเตอร์ (Monitoring)
   - จัดทำบันทึกติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เช่น การใช้งานฮาร์ดดิสก์ การใช้งานหน่วยประมวลผล (CPU) เป็นต้น เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพ (Capacity) ของระบบ กำหนดให้บันทึกทุกวัน และให้ผู้จัดการฝ่ายทราบทุกเดือน
   - มีการบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ
3 การจัดการปัญหาต่าง ๆ
   - ต้องกำหนดรายชื่อ หน้าที่ และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน
   - ควรมีระบบจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้น และรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหาและตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป
4 การควบคุมการจัดทำรายงาน
   - การขอให้จัดพิมพ์รายงานของระบบงาน ERP ที่สำคัญ ต้องได้รับการอนุมัติจากผู้บริหารระดับสูง
   - มีทะเบียนคุมการพิมพ์และการจัดส่งรายงาน จัดเก็บรายงานต่าง ๆ ที่ได้จัดพิมพ์แล้วอย่างรัดกุม และกำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

7. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อ บริษัท ในรูปแบบที่แตกต่างไปจากการดำเนินงานปกติของบริษัท เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (Access risk) ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการประมวลผลของระบบงาน (Integrity risk) ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น ดังนั้น การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นจึงมีวัตถุประสงค์ เพื่อให้บริษัทใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

แนวทางปฏิบัติ

1. การคัดเลือกผู้ให้บริการ
   - การกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ
   - จัดทำสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service level agreement) อย่างชัดเจน
2. การควบคุมผู้ให้บริการ
   - ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น
   - การเข้าถึงส่วนที่ใช้งานจริง (Production environment) กำหนดให้มีการควบคุมและตรวจสอบขณะทำงานของผู้ให้บริการตลอดเวลา เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้
   - กรณีที่เป็นการให้บริการในลักษณะ Remote access ให้เจ้าหน้าที่ควบคุมและตรวจสอบการทำงานของผู้ให้บริการตลอดเวลา และปิดทันทีที่การให้บริการเสร็จสิ้น
   - กำหนดให้ผู้ให้บริการเก็บบันทึกรายงานการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไข เพื่อให้สามารถตรวจสอบย้อนหลังได้
   - กำหนดให้มีขั้นตอนในการตรวจรับงานของผู้ให้บริการ

8. การใช้งานระบบคอมพิวเตอร์และเครือข่าย สำหรับผู้ใช้งาน

วัตถุประสงค์

เพื่อกำหนดวิธีปฏิบัติให้กับผู้ใช้งานระบบสารสนเทศในบริษัท รวมทั้งผู้เกี่ยวข้องใด ๆ

แนวทางปฏิบัติ

1. ปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศโดยเคร่งครัด
2. ปฏิบัติตามกิจกรรมหรือกระบวนการด้านความปลอดภัยที่กำหนดไว้
3. ผู้ใช้งานต้องใช้งานระบบสารสนเทศตามสิทธิและขอบเขตที่ได้รับอนุญาตให้ใช้งานเท่านั้น
4. ผู้ใช้งานต้องรับผิดชอบในการเก็บรักษาข้อมูลของตนเองไว้ในที่ที่บริษัทกำหนด หากเป็นความลับ ต้องแจ้งให้ผู้ดูแลระบบทราบเพื่อกำหนดสิทธิเฉพาะ
5. ผู้ใช้งานต้องเก็บสื่อบันทึกข้อมูลไว้ในที่ปลอดภัย เช่น ใส่ตู้ หรือ โต๊ะ ที่สามารถใส่กุญแจได้ เป็นต้น
6. ผู้ใช้งานต้องช่วยกันดูแลอุปกรณ์คอมพิวเตอร์ส่วนตัวและส่วนกลางที่ใช้งานร่วมกัน ถ้าพบเหตุการณ์ผิดปกติร้ายแรง ให้แจ้งผู้ดูแลระบบทราบทันทีเพื่อเข้าตรวจสอบ
7. การนำเครื่องคอมพิวเตอร์ประจำสำนักงาน ได้แก่ Notebook Tablet รวมทั้งอุปกรณ์คอมพิวเตอร์ใด ๆ ไปใช้นอกสถานที่ต้องระมัดระวังข้อมูลสำคัญ ไม่ให้บุคคลภายนอกเข้าถึง หรือทำสำเนา และต้องบันทึกการครอบครองอุปกรณ์ดังกล่าว และต้องเก็บรักษาอุปกรณ์ดังกล่าวไม่ให้เกิดความเสียหาย
8. การร้องขอใด ๆ เพื่อให้มีการใช้งานระบบสารสนเทศเพิ่มเติมจากระบบเดิม ต้องผ่านการอนุมัติจากผู้บังคับบัญชา ตามสายงานที่ร้องขอ และผู้บังคับบัญชาสายงานสารสนเทศเท่านั้น โดยสามารถแจ้งให้ผู้ดูแลระบบดำเนินการโดยใช้แบบฟอร์มที่กำหนดไว้ในระบบ ISO ทั้งนี้ ผู้ดูแลระบบอาจจะขอข้อมูลเพิ่มเติม เพื่อให้ดำเนินการได้อย่างเหมาะสม
9. ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข ทำลาย หรือทำให้เสียหายต่อทรัพย์สินสารสนเทศของบริษัท โดยไม่ได้รับอนุญาต
10. ผู้ใช้งานต้องไม่ใช้งานระบบสารสนเทศ โดยมีวัตถุประสงค์ดังนี้
    a. เพื่อเปิดเผยข้อมูลลับของบริษัท
    b. เพื่อละเมิดทรัพย์สินทางปัญญาขององค์กร
    c. เพื่อการรับหรือส่งข้อมูลที่ก่อให้เกิดความเสียหายต่อองค์กร
    d. เพื่อกระทำผิดกฎหมาย หรือก่อความเสียหายให้แก่บุคคลอื่น
    e. เพื่อประโยชน์ส่วนตัว
    f. เพื่อขัดต่อความสงบเรียบร้อย หรือศีลธรรม
    g. เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร

11. ก่อนนำข้อมูลสำคัญใด ๆ ออกเผยแพร่สู่สาธารณชน ผู้ใช้งานหรือผู้มีหน้าที่รับผิดชอบ ต้องขออนุญาตต่อผู้มีอำนาจอนุมัติในงานดังกล่าว
12. ห้ามผู้ใช้งานนำเครื่องคอมพิวเตอร์ส่วนบุคคลมาใช้งาน หากมีความจำเป็นต้องได้รับอนุมัติจากผู้บริหารระดับสูงก่อน
13. ผู้ใช้งานต้องไม่เล่นเกมส์บนเครื่องคอมพิวเตอร์ใด ๆ
14. กรณีที่ผู้ใช้งานได้รับสิทธิในการจัดการเครื่องคอมพิวเตอร์ระดับ Administrator ต้องไม่ติดตั้งโปรแกรมใช้งานเอง ไม่ว่าจะเป็นโปรแกรม Freeware โปรแกรมถูกต้องตามลิขสิทธิ์ รวมทั้งโปรแกรมที่ไม่มีลิขสิทธิ์ ถ้าต้องการใช้งานโปรแกรมนอกเหนือจากที่มีการติดตั้งไว้ให้ ให้แจ้งความประสงค์ไปยังผู้ดูแลระบบเพื่อดำเนินการตามขั้นตอนระบบ ISO
15. ผู้ใช้งานที่ลักลอบติดตั้งและใช้งานโปรแกรมหรือ Software ที่ไม่ถูกต้องตามลิขสิทธิ์ หากมีผลทำให้บริษัทมีความผิดด้านกฎหมาย รวมทั้งอาจมีการฟ้องร้องเรียกค่าเสียหาย บริษัทจะเรียกเก็บจากผู้ใช้งานตามมูลค่าดังกล่าว รวมทั้งได้รับโทษตามที่กำหนดไว้ในระเบียบของบริษัท

9. การใช้อินเทอร์เน็ต (Internet)

วัตถุประสงค์

เพื่อควบคุมดูแลการใช้งานอินเทอร์เน็ตของบริษัทให้มีความมั่นคงปลอดภัย และไม่ละเมิดกฎหมายใด ๆ เกี่ยวกับการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ทั้ง 2 ฉบับ ที่ออกมาในปี 2550 และ ปี 2560 โดยบริษัทได้มีการสื่อสารให้ทุกคนได้รับทราบกฎหมายที่เกี่ยวข้องอย่างทั่วถึง

แนวทางปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดให้เฉพาะผู้ที่มีสิทธิ์เท่านั้นที่จะสามารถเชื่อมต่อระบบเพื่อใช้งานอินเทอร์เน็ตได้ โดยสิทธิดังกล่าวต้องได้รับการอนุมัติจากระดับผู้จัดการฝ่ายหรือผู้บริหารระดับสูง
2. ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อเพื่อการใช้งานอินเทอร์เน็ต ผ่านระบบรักษาความปลอดภัย (Firewall) และให้มีการเก็บข้อมูลการใช้งาน
3. ผู้ดูแลระบบต้องกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลที่เหมาะสม เพื่อประสิทธิภาพของเครือข่าย ได้แก่ การกำหนดกลุ่มเว็บไซต์ที่สามารถใช้งานได้ในงานเท่านั้น หรือการกำหนด Application ที่จำเป็นต้องใช้ในการปฏิบัติงาน โดยสิทธิดังกล่าวจะกำหนดเป็นกลุ่มและกำหนดเป็นรายบุคคลตามความเหมาะสม
4. ผู้ดูแลระบบต้องจัดทำบัญชีรายชื่อผู้ใช้งาน รวมทั้งสิทธิการใช้งาน และปรับปรุงให้ทันสมัยอย่างสม่ำเสมอ หรือทันทีที่ได้รับแจ้งจากฝ่ายทรัพยากรบุคคลกรณีที่พนักงานลาออก
5. ผู้ใช้งานต้องทำการตรวจสอบความถูกต้องน่าเชื่อถือของข้อมูลที่นำมาจากเครือข่ายอินเทอร์เน็ตก่อนไปใช้งาน
6. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตอย่างสร้างสรรค์ ทั้งในและนอกเวลางาน
7. ผู้ใช้งานต้องไม่ใช้อินเทอร์เน็ตเพื่อวัตถุประสงค์ในทางที่ไม่เหมาะสม ดังนี้
    a. เปิดเผยข้อมูลลับขององค์กร
    b. หาประโยชน์เชิงธุรกิจส่วนตัว
    c. เผยแพร่ข้อมูลที่เป็นเท็จ ภาพดัดแปลง ตัดต่อข้อความ
    d. ยั่วยุ ให้ร้าย ทำลายความสัมพันธ์ของพนักงานในบริษัท หรือทำให้บริษัทเสื่อมเสียภาพลักษณ์
    e. ละเมิดทรัพย์สินทางปัญญา
    f. กระทำผิดกฎหมาย
    g. ก่อความเสียหาย หรือก่อความรำคาญ ให้แก่บุคคลอื่น
    h. ขัดต่อความสงบเรียบร้อยหรือศีลธรรม
    i. เล่นเกมส์ออนไลน์ หรือเกมส์ใด ๆ ในระหว่างการทำงาน

j. เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร

8. ห้ามผู้ใช้งานทำการ Download ประเภทสื่อลามก อนาจาร มาเก็บไว้ภายในเครื่องหรือระบบคอมพิวเตอร์ รวมทั้งห้ามส่งไฟล์ดังกล่าว ภายในหรือภายนอกบริษัท
9. ห้ามใช้อินเทอร์เน็ตเพื่อดูวิดีโอ ภาพยนต์ หรือฟังเพลง ผ่านทางอินเทอร์เน็ตในเวลาทำงาน
10. ห้ามเข้าเว็บไซต์อยู่ในประเภทต่อไปนี้
    - การพนัน
    - การวิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติ ศาสนา และพระมหากษัตริย์
    - ลามก อนาจาร
    - อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย และศีลธรรมอันดี
11. ห้ามใช้อินเทอร์เน็ตเพื่อส่ง “สื่อหรือข้อมูล” ที่เป็นการละเมิดลิขสิทธิ์ทางปัญญาหรือข้อมูลส่วนตัวของผู้อื่น
12. ห้ามใช้อินเทอร์เน็ตเพื่อส่งหรือ Upload ข้อมูลใด ๆ ที่เป็นความลับของบริษัท ไปเก็บที่ระบบ Cloud ยกเว้นได้รับการอนุมัติจากผู้บริหารระดับสูง
13. ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อภาพลักษณ์ของบริษัท

10. การใช้งานจดหมายอิเล็กทรอนิกส์ (Email)

วัตถุประสงค์

เพื่อให้มีการใช้งานจดหมายอิเล็กทรอนิกส์ ผ่านระบบเครือข่ายที่บริษัทจัดไว้ให้อย่างเหมาะสม และไม่ใช้ในกิจกรรมอื่น ๆ ที่อาจก่อให้เกิดความเสียหายต่อตนเอง ผู้อื่น หรือต่อบริษัท

แนวทางปฏิบัติ

1. ผู้ที่ประสงค์จะใช้งานจดหมายอิเล็กทรอนิกส์ ต้องกรอกใบคำร้องตามที่ฝ่ายเทคโนโลยีและสารสนเทศกำหนดไว้ในระบบ ISO โดยได้รับการอนุมัติจากผู้จัดการฝ่าย
2. ผู้ดูแลระบบต้องจัดทำบัญชีรายชื่อผู้ใช้งานให้ทันสมัยตลอดเวลา และมีการสื่อสารให้ผู้ใช้งานทราบโดยทั่วถึงทุกเดือน
3. ให้ใช้ที่อยู่ของจดหมายอิเล็กทรอนิกส์ หรือ ที่อยู่อีเมล (email address) ของบริษัท ในการติดต่องานทั้งภายในและภายนอกตามหน้าที่ความรับผิดชอบของตนเองเท่านั้น
4. ให้ระบุชื่อผู้ส่ง สังกัด และตำแหน่งหน้าที่ ในอีเมล (email) ทุกฉบับ
5. ควรใช้คำที่สุภาพในการสื่อสาร ทั้งภายในและภายนอก ไม่ควรใช้ชื่อเล่นในการระบุตัวตน
6. ให้ใช้ความระมัดระวังในการระบุชื่อผู้รับ รวมทั้งที่อยู่ที่ถูกต้อง เพื่อป้องกันการส่งข้อมูลที่ผิดพลาด หากมีการส่งสำเนาควรจำกัดกลุ่มผู้รับเท่าที่จำเป็น
7. ฝ่ายเทคโนโลยีและสารสนเทศต้องมีการตั้งค่าการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ
8. กรณีที่ไม่แน่ใจในด้านความปลอดภัยของข้อมูลที่รับ-ส่ง ผู้ใช้งานควรแจ้งให้เปลี่ยนรหัส โดยใช้แบบฟอร์มที่กำหนด
9. ผู้ใช้ควรปิดโปรแกรมรับส่งจดหมายอิเล็กทรอนิกส์ทันทีที่เลิกใช้งาน
10. ผู้ใช้งานต้องปรับปรุงรายชื่อผู้ที่ติดต่อในเครื่องของตนเองตามที่มีในรายการบัญชีผู้ใช้งานล่าสุด เพื่อป้องกันความผิดพลาดในการส่ง
11. ไม่ใช้จดหมายอิเล็กทรอนิกส์ในเรื่องส่วนตัว
12. ห้ามเข้าถึงข้อมูลอีเมล (email) ของบุคคลอื่น โดยไม่ได้รับอนุญาต
13. ห้ามนำที่อยู่อีเมล (email address) ไปลงทะเบียนบนเว็บไซต์ที่ไม่เกี่ยวข้องกับงานของบริษัท
14. ต้องไม่ส่งจดหมายอิเล็กทรอนิกส์ที่มีข้อความเป็นความเห็นส่วนตัว โดยอ้างว่าเป็นความเห็นของบริษัท
15. บริษัทสงวนสิทธิ์ในการป้องกันการส่งอีเมล (email) พร้อมข้อมูลที่มีขนาดใหญ่เกินกว่า 25 เมกกะไบต์(MB) เพื่อป้องกันการรั่วไหลของข้อมูล และเพื่อความเสถียรของระบบ
16. ข้อมูลขนาดใหญ่ ควรใช้วิธีการฝากไฟล์ไว้บนสถานที่เก็บแบบ Cloud และต้องใส่รหัสเพื่อป้องกัน รวมทั้งกำหนดวันหมดอายุ โดยส่งให้ผู้รับเป็น Link address ในการเข้าถึง

11. การใช้เครือข่ายสื่อสังคมออนไลน์ (Social Media)

วัตถุประสงค์

1. เพื่อกำหนดขอบเขตของการใช้เครือข่ายสื่อสังคมออนไลน์ของบริษัทฯ
2. เพื่อเป็นแนวทางปฏิบัติให้พนักงานของบริษัทได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล ในการใช้ประโยชน์จากเครือข่ายสื่อสังคมออนไลน์ ซึ่งเป็นหน้าที่ทุกคนที่ต้องปฏิบัติตามอย่างเคร่งครัด
3. เพื่อป้องกันการเปิดเผยข้อมูลความลับในทุกระดับชั้น
4. เพื่อลดความเสี่ยงหรือหลีกเลี่ยงปัญหาอันอาจจะเกิดขึ้นจากการใช้เครือข่ายสื่อสังคมออนไลน์
5. เพื่อสร้างและรักษาภาพลักษณ์ของบุคลากรและการดำเนินงานของบริษัท
6. เพื่อปฏิบัติตามกฎหมาย ระเบียบ ประกาศ นโยบาย ข้อบังคับ ตลอดจนแนวทางปฏิบัติและข้อสั่งการที่เกี่ยวข้องทั้งหมด

แนวทางปฏิบัติ

1. ฝ่ายเทคโนโลยีและสารสนเทศมีหน้าที่ในการปิดกั้นการใช้เครือข่ายสื่อสังคมออนไลน์ใด ๆ ผ่านระบบอินเทอร์เน็ตของบริษัท
2. บริษัทไม่อนุญาตให้บุคลากรใช้เครือข่ายสื่อสังคมออนไลน์ใด ๆ ผ่านระบบอินเทอร์เน็ตของบริษัท ยกเว้นผู้มีหน้าที่เกี่ยวข้องในการเผยแพร่ข้อมูลข่าวสารของบริษัท หรือใช้เพื่อเป็นสื่อติดต่อเกี่ยวกับงานที่รับผิดชอบเท่านั้น โดยได้รับการอนุมัติโดยตรงจากผู้บริหารระดับสูง
3. หน่วยงานภายในบริษัท บุคลากร สามารถแสดงชื่อผู้ใช้งานบนเครือข่ายสื่อสังคมออนไลน์ เพื่อประโยชน์ในการเผยแพร่ประชาสัมพันธ์ข้อมูลข่าวสารที่เกี่ยวข้องกับบริษัท ติดต่อสื่อสารระหว่างกัน แต่ต้องแยกแยะให้ชัดเจนว่า ข้อความใดเป็น “ข่าวประชาสัมพันธ์” ข้อความใดเป็น “ความคิดเห็น”, “ความคิดเห็นส่วนบุคคล”, “การแลกเปลี่ยนข่าวสารส่วนตัว”, “การเผยแพร่ข่าวสารเรื่องงาน” หรือข้อความอื่นใด และความคิดเห็นดังกล่าวควรคำนึงว่าเป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ทั้งนี้ ผู้เผยแพร่ต้องรับผิดชอบทั้งทางด้านสังคม และด้านกฎหมาย นอกจากนี้ ยังอาจมีผลกระทบต่อชื่อเสียงของบริษัทได้และควรคำนึงถึงประโยชน์สาธารณะด้วย
4. การใช้เครือข่ายสื่อสังคมออนไลน์ต้องไม่รบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย
5. พึงระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่นหรือประมาทบุคคลอื่น และควรใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์
6. งดเว้นการใช้เพื่อวิพากษ์วิจารณ์ ตลอดจนแสดงความคิดเห็นในเรื่องที่เป็นข้อมูลภายในบริษัท หรืออาจส่งผลกระทบต่อบริษัทได้
7. ไม่นำข้อมูลที่เป็นความลับทุกระดับชั้นของบริษัทมาเผยแพร่

8. การพูดคุยแลกเปลี่ยนกับชุมชนออนไลน์ รวมถึงการโพสต์ข้อความที่เกี่ยวข้องกับงานประจำ เป็นสิ่งที่บุคคลสามารถกระทำได้ ถ้าไม่ขัดต่อหลักจรรยาบรรณบริษัท เว้นแต่ข้อมูลนั้น เป็นข้อมูลที่มีความสำคัญหรือเป็นความลับของบริษัท
9. บุคลากรของบริษัทไม่ควรโพสต์ข้อมูลใดที่ขัดแย้งกับข้อกำหนดของบริษัท รวมถึงละเว้นการแสดงออกถึงความเห็นที่ก้าวร้าว หมิ่นประมาท ดูถูกเป็นการส่วนตัว ลามกอนาจาร และอื่น ๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือขัดต่อจริยธรรม เช่น การเมือง ศาสนา ชนชาติ เป็นต้น
10. คำนึงถึงผลกระทบของการโพสต์ข้อความในเว็บบล็อกส่วนตัว โดยเฉพาะข้อความที่อาจก่อให้เกิดความขัดแย้งกับบริษัท ดังนั้น จึงควรระมัดระวังในการถูกนำข้อความในเว็บบล็อกส่วนตัวมาเป็นข้อมูลอ้างอิง
11. การเผยแพร่ข้อมูลข่าวสารที่ประชาสัมพันธ์ในนามของบริษัท ผู้เผยแพร่ต้องแสดงชื่อ-สกุล ตำแหน่ง สังกัด เลขหมายโทรศัพท์ติดต่อให้ชัดเจน เพื่อความน่าเชื่อถือของข้อมูล และเพื่อให้ผู้ที่เข้ามาอ่านข้อมูลข่าวสารสามารถใช้ดุลพินิจในการติดตามข้อมูลที่เผยแพร่ออกไปได้
12. บริษัทไม่รับผิดชอบต่อผลของการกระทำที่เกิดจากผู้ใช้งานและ/หรือบัญชีผู้ใช้งานที่ฝ่าฝืนต่อนโยบายนี้

.....