>14th fl. phahonyotin place
>408/55 phahonyotin rd.
>phayatai samsennai
>bangkok 10400
>Thailand >www.inteltion.com >call 662 619 0209 >fax 662 619 0208

นโยบายและแนวปฏิบัติเรื่องการบริหารจัดการข้อมูลสารสนเทศ

1 วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยให้แก่ทรัพย์สินของบริษัท อินเทลชั่น จำกัด โดยเฉพาะอย่างยิ่งทรัพย์สินที่เป็นข้อมูลสารสนเทศสำคัญที่ใช้ในการดำเนินการธุรกิจ โดยการป้องกันเพื่อให้พ้นจากภัยคุกคามและความเสี่ยงด้านเทคโนโลยีสารสนเทศต่างๆ ทั้งจากภายในและภายนอกบริษัท รวมถึงการกระทำที่ผิดกฎหมาย หรือสร้างความเสียหายให้กับบุคคลอื่น ไม่ว่าจะเกิดขึ้นโดยเจตนาหรือไม่เจตนาก็ตาม รวมถึงเพื่อลดความเสียหายต่างๆ ที่อาจเกิดขึ้นจากเหตุละเมิดความมั่นคงปลอดภัย และเพื่อรักษาไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง

2 ขอบเขต

- ข้อมูลทั้งหมด (ทั้งที่อยู่ในรูปแบบเอกสาร และ/หรือข้อมูลอิเล็กทรอนิกส์) ที่ได้รับการจัดเก็บ ใช้งาน เปิดเผย และ/หรือถูกนำไปใช้การสื่อสารเพื่อดำเนินการกิจการของบริษัท
- บุคคลากรภายในองค์กร และบุคคลภายนอกองค์กรที่ใช้ระบบสารสนเทศของบริษัท
- ทรัพย์สินทั้งหมดที่เกี่ยวข้องกับข้อมูล และที่ใช้ในการจัดเก็บ ส่งผ่าน และประมวลผลข้อมูล ซึ่งได้แก่ เครื่องเซิร์ฟเวอร์ ซอฟต์แวร์โปรแกรม ข้อมูลอิเล็กทรอนิกส์ เอกสารตีพิมพ์

3 นโยบาย

3.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

1) ปกป้องข้อมูล (ไม่ว่าจะถูกเก็บในรูปแบบใดก็ตาม) ให้พ้นจากเหตุละเมิดต่าง ๆ ซึ่งอาจส่งผลกระทบต่อความลับของข้อมูล (Confidentiality) ความถูกต้องและสมบูรณ์ครบถ้วนของข้อมูล (Integrity) และความพร้อมใช้ของข้อมูล (Availability)
2) ปฏิบัติตามมาตรฐาน ISO/IEC 27001 และมาตรฐานอื่น ๆ ตลอดจนนโยบายด้านความมั่นคงปลอดภัยที่บริษัทฯ กำหนด เพื่อความมั่นคงปลอดภัยของข้อมูล
3) ปฏิบัติตามข้อกฎหมายอื่น ๆ ที่เกี่ยวข้องทั้งหมด

โดยบริษัทฯ มีนโยบายดังต่อไปนี้

1) ข้อมูลที่สำคัญของบริษัทฯ ต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต
2) ข้อมูลที่สำคัญของบริษัทฯ ต้องได้รับการรักษาความลับอย่างเหมาะสม
3) ข้อมูลที่สำคัญของบริษัทฯ ต้องมีความถูกต้องและสมบูรณ์ครบถ้วน
4) ข้อมูลที่สำคัญของบริษัทฯ ต้องพร้อมใช้งานอยู่เสมอ
5) กฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้องต่าง ๆ ต้องได้รับการปฏิบัติตามอย่างถูกต้องครบถ้วน
6) ต้องมีการจัดทำรายการทรัพย์สินสารสนเทศที่สมบูรณ์และครบถ้วน ประกอบด้วยรายการทรัพย์สินที่เกี่ยวกับอุปกรณ์และเครื่องคอมพิวเตอร์ ระบบงานสารสนเทศ และข้อมูล
7) บุคลากรภายในองค์กร และบุคลากรภายนอกองค์กรทุกคนจะต้องปฏิบัติงานโดยคำนึงถึงความมั่นคงปลอดภัยสารสนเทศเสมอ (Awareness)

3.2 การปฏิบัติตามนโยบายและการตรวจสอบ

1) บุคลากรภายในองค์กรต้องรับทราบนโยบาย ระเบียบ และวิธีการปฏิบัติงานของบริษัทฯ เพื่อเป็นการยอมรับว่าข้อมูลต่าง ๆ ที่ได้รับทราบ และใช้ระหว่างการปฏิบัติหน้าที่ เป็นทรัพย์สินของบริษัทฯ และไม่สามารถนำไปใช้เพื่อการอื่นโดยไม่ได้รับอนุญาต ทั้งนี้ในการใช้งานข้อมูลทั้งหลายในบริษัทฯของบุคลากรภายในองค์กรจะถือเป็นการรับทราบและยินยอมปฏิบัติตามเงื่อนไขของนโยบายนี้ทุกประการ
2) บุคลากรภายนอกองค์กรต้องมีสัญญาที่ระบุถึงการรักษาความลับ การรับทราบ และปฏิบัติตามนโยบาย ระเบียบ และวิธีการปฏิบัติงานของบริษัทฯ ในการใช้ข้อมูล หรือกระใช้ระบบสารสนเทศขอบริษัทฯ
3) บริษัทฯ ขอสงวนสิทธิ์ในการตรวจสอบระบบสารสนเทศของบริษัทฯ ที่ถูกใช้โดยบุคลากรภายในองค์กร หรือบุคลากรภายนอกองค์กรตามกระบวนการตรวจสอบภายใน (Internal Audit) หรือการตรวจสอบภายนอก (External Audit) เพื่อให้เป็นไปตามนโยบายการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่ดี และปฏิบัติตามกฎหมาย หรือประกาศจากหน่วยงานกำกับดูแลที่เกี่ยวข้อง

3.3 การทบทวนและปรับปรุงนโยบาย

ในกรณีที่มีการเปลี่ยนแปลงกฎหมาย ข้อบังคับ นโยบาย หรือแนวปฏิบัติใด ๆ ซึ่งส่งผลกระทบต่อนโยบายฉบับนี้ หรือเห็นว่านโยบายฉบับนี้ไม่เหมาะสมหรือไม่เพียงพอต่อการดำเนินธุรกิจ ให้นำเสนอนโยบาย

ฉบับใหม่ที่ได้มีการทบทวนและปรับปรุงแก้ไขดังกล่าวต่อคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย

3.4 บทลงโทษ

การละเมิด ฝ่าฝืน ละเลย หรือไม่ปฏิบัติตามนโยบาย ตลอดจนวิธีการปฏิบัติงาน และเอกสารสนับสนุนต่าง ๆ ที่เกี่ยวข้องของบริษัทฯไม่ว่าโดยเจตนา รหือไม่ก็ตาม สำหรับบุคลากรภายในองค์กร บริษัทฯ จะพิจารณาลงโทษตามดุลยพินิจ หรือทางวินัยตามกฎระเบียบของบริษัทฯสำหรับบุคลากรภายนอกองค์กรถือเป็นความผิดตามสัญญาจ้าง บริษัทฯจะพิจารณาลงโทษตามสัญญาจ้าง นอกจากนี้หากการละเมิดหรือฝ่าฝืนนโยบายนั้นเข้าข่ายเป็นการกระทำที่ผิดกฎหมาย หรือก่อนให้เกิดความเสียหายแก่บริษัทฯและ/หรือบุคคลอื่นใด บริษัทฯ อาจพิจารณาดำเนินคดีตามที่กฎหมายระบุไว้ต่อไป

4 แนวปฏิบัติ

ให้ปฏิบัติตามแนวทางตามมาตรฐานสากลเกี่ยวกับการใช้เทคโนโลยีสารสนเทศ ซึ่งประกอบด้วยหลัก 4 ประการ คือ Privacy, Accuracy, Property และ Accessibility (PAPA) โดยมีรายละเอียด ดังนี้

ความเป็นส่วนตัวของข้อมูลสารสนเทศ (Information Privacy)

- รักษาความลับและปกป้องความปลอดภัยของข้อมูลส่วนตัวของบุคลากร ลูกค้า คู่ค้าธุรกิจ และพันธมิตรทางธุรกิจ
- ไม่ใช้ข้อมูลของลูกค้าจากแหล่งต่างๆ เพื่อผลประโยชน์ทางการตลาดหรือนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่แล้วนำไปขายให้กับบริษัทอื่น
- เก็บรักษาชื่อบัญชีผู้ใช้งาน (account) และรหัสผ่าน (password) ที่เกี่ยวข้องกับระบบข้อมูลสารสนเทศของบริษัทไว้เป็นส่วนตัวและสร้างให้เป็นเอกลักษณ์
- ไม่จด password ไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น ที่ไม่ได้รับอนุญาต และง่ายต่อการถอดรหัสผ่าน
- กรณีที่มีความจำเป็นต้องบอก password แก่ผู้อื่นเพื่อเข้าดาเนินการในระบบข้อมูลสารสนเทศหลังจากดำเนินการเรียบร้อยให้ทาการเปลี่ยนรหัสผ่านทันที

>14th fl. phahonyotin place
>408/55 phahonyotin rd.
>phayatai samsennai
>bangkok 10400
>Thailand >www.inteltion.com >call 662 619 0209 >fax 662 619 0208

ความถูกต้องของข้อมูล (Information Accuracy)

- การจัดทาข้อมูลสารสนเทศให้มีความถูกต้องและน่าเชื่อถือนั้น ข้อมูลควรได้รับการตรวจสอบความถูกต้องก่อนที่จะนำเข้าฐานข้อมูล รวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่เสมอ
- แหล่งที่มาของข้อมูลต้องมีความน่าเชื่อถือและตรวจสอบได้ เช่น หน่วยงานภาครัฐ องค์กรอื่นที่เชื่อถือได้ เป็นต้น

ความเป็นเจ้าของ (Information Property)

- บริษัทเป็นเจ้าของในทรัพย์สินทางปัญญาที่บุคลากรได้พัฒนาหรือสร้างขึ้นไม่ว่าจะทั้งหมดหรือบางส่วน
- ไม่ละเมิดหรือเปิดเผยโดยไม่ได้รับอนุญาตในทรัพย์สินทางปัญญาและลิขสิทธิ์ของงานที่ทำร่วมกัน
- ไม่ใช้งาน ทำซ้ำ ตีพิมพ์หรือเผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท
- ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ตซึ่งรวมถึงการอัพเดทโปรแกรมต่างๆ ซอฟต์แวร์ที่ใช้ในระบบข้อมูลสารสนเทศของบริษัทต้องไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น
- ปกป้องทรัพย์สินทางปัญญาของบริษัทโดยไม่เปิดเผยก่อนได้รับอนุญาต
- ปกป้องทรัพย์สินทางปัญญาโดยไม่ใช้ผิดวิธีหรือผิดกฎหมาย และเมื่อใช้ ต้องแน่ใจว่าได้ประทับตราหรือแสดงเครื่องหมายการค้า หรือเครื่องหมายบริการ หรือสัญลักษณ์ลิขสิทธิ์ เช่น การใช้ ®, TM, © (201x) เป็นต้น
- แจ้งให้กลุ่มธุรกิจ/ หน่วยงานทราบถึงการค้นพบ การประดิษฐ์ เช่น โปรแกรมคอมพิวเตอร์ สิ่งประดิษฐ์ทางเทคโนโลยีและผลงานนวัตกรรม รวมไปถึงข้อมูลจาเพาะ
- ให้ความช่วยเหลือบริษัทเพื่อให้ได้มาซึ่งสิทธิบัตร ลิขสิทธิ์ หรือปกป้องเครื่องหมายการค้าที่เป็นทรัพย์สินทางปัญญาของบริษัท

การเข้าถึงข้อมูล (Data Accessibility)

- การใช้งานระบบสารสนเทศ เช่น ระบบคอมพิวเตอร์ แอปพลิเคชัน อีเมล ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น ผู้บริหารต้องกาหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศก่อนเข้าใช้ระบบฯ ของผู้ใช้งานให้เหมาะสมกับงานและหน้าที่ความรับผิดชอบ
- ผู้รับมอบอำนาจจากผู้บริหารเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ การเข้าถึงข้อมูลและระบบฯ

4.1 การจัดระดับความลับข้อมูลสารสนเทศ (Classification of Information)

โดยพิจารณาจากระดับความเสี่ยงต่อความมั่นคงปลอดภัย ผลกระทบต่อมูลค่า ผลกระทบต่อความเสียหายทางทรัพย์สินและภาพพจน์บริษัทโดยแบ่งตามประเภทดังต่อไปนี้

- เอกสารลับพิเศษ (Special Control) เป็นข้อมูลสารสนเทศที่ส่งผลกระทบต่อการดาเนินยุทธศาสตร์ทางธุรกิจและก่อให้เกิดความเสียเปรียบในการแข่งขันเชิงธุรกิจอย่างร้ายแรง ถ้าเกิดการรั่วไหลของข้อมูลออกมาจะก่อให้เกิดความเสียหายต่อภาพพจน์ของบริษัทในระดับสากล เช่น ข้อมูลความลับทางการค้า (Trade Secret) แผนกลยุทธ์ทางธุรกิจ แผนการตลาด / การพัฒนาผลิตภัณฑ์ แผนควบรวมกิจการ
- เอกสารลับ (Confidential) เป็นข้อมูลสารสนเทศที่ส่งผลกระทบต่อการดาเนินธุรกิจและความก้าวหน้าของธุรกิจ องค์กรอาจถูกฟ้องร้องเรียกค่าเสียหาย ถ้าเกิดการรั่วไหลของข้อมูลและก่อให้เกิดความเสียหายต่อภาพพจน์บริษัทในระดับประเทศ เช่น เอกสารทางการตลาด (ที่ยังไม่เปิดเผยต่อสาธารณะ) ข้อมูลส่วนบุคคล ข้อมูลลูกค้า
- เอกสารใช้ภายในเท่านั้น (Internal Use Only) เป็นข้อมูลสารสนเทศที่อนุญาตให้ใช้ภายในบริษัทเท่านั้น ส่งผลกระทบต่อการปฏิบัติงานประจาวันและอาจทาให้เกิดความเสียหายต่อภาพพจน์ เช่น ประกาศภายใน/นโยบายต่างๆ ระเบียบ/คู่มือปฏิบัติงาน บันทึกการปฏิบัติงานประจำวัน
- 4.3.4 เอกสารเปิดเผย (Public) เป็นข้อมูลสารสนเทศที่พิจารณาแล้วเห็นว่าไม่มีผลกระทบต่อองค์กร สามารถเปิดเผยต่อบุคคลภายนอกได้ เช่น ข้อมูลด้านความยั่งยืน ข้อมูลประชาสัมพันธ์ โปรโมชั่นทางการค้าต่างๆ
- ทั้งนี้ เอกสารหรือสิ่งตีพิมพ์ไม่ว่าจะทั้งหมดหรือบางส่วนที่พิมพ์หรือทาซ้าขึ้นมาจากต้นฉบับซึ่งมีการกาหนดชั้นความลับไว้ ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับ

4.2 การจัดเก็บข้อมูลสารสนเทศและอุปกรณ์

- ผู้บริหารและผู้รับผิดชอบดูแลข้อมูลสารสนเทศเป็นผู้กาหนดระยะเวลาจัดเก็บข้อมูลสารสนเทศตามระดับความลับ
- รักษาความปลอดภัยของระบบสารสนเทศและอุปกรณ์ซึ่งบรรจุข้อมูลสารสนเทศของบริษัท เช่น โทรศัพท์มือถือ แล็ปท็อป แท็บเล็ต เป็นต้น และต้องระมัดระวังเป็นพิเศษในการใช้งานอุปกรณ์ดังกล่าวนอกสถานประกอบการ รวมทั้งจัดเก็บไว้ในที่ที่มีกุญแจล็อคหลังการใช้งาน
- ตั้งรหัสผ่าน (password) ล็อคหน้าจอซึ่งบรรจุข้อมูลสารสนเทศของบริษัทเมื่อต้องการออกจากระบบสารสนเทศหรือเสร็จสิ้นงาน
- รายงานผู้รับผิดชอบทันทีเมื่อข้อมูลสารสนเทศหรืออุปกรณ์ซึ่งบรรจุข้อมูลสารสนเทศของบริษัทสูญหายหรือถูกขโมย

4.3 การนำอุปกรณ์ส่วนตัวมาใช้ในบริษัท

อุปกรณ์สื่อสารไร้สายเป็นสิ่งสาคัญต่อการสื่อสารทางธุรกิจและช่วยเพิ่มประสิทธิผลการทางาน นอกจากนี้การใช้อุปกรณ์สื่อสารไร้สายของพนักงานที่เพิ่มขึ้นทาให้ต้องมีการขออนุญาตเชื่อมต่อกับเครือข่ายของบริษัท การอนุมัติการใช้อุปกรณ์ส่วนตัวและแอปพลิเคชั่นให้เป็นไปตามแต่ละบริษัทกาหนด

บุคลากรที่ใช้อุปกรณ์สื่อสารไร้สายส่วนตัวต้องปฏิบัติ ดังต่อไปนี้

- งานที่ได้พัฒนาขึ้นบนอุปกรณ์ส่วนตัวถือเป็นทรัพย์สินทางปัญญาของบริษัท
- อุปกรณ์สื่อสารไร้สายส่วนตัวให้ฝ่ายเทคโนโลยีสารสนเทศตั้งค่าระบบและติดตั้งโปรแกรมพื้นฐานก่อนการเข้าถึงเครือข่าย
- อุปกรณ์สื่อสารไร้สายจะต้องตั้งรหัสผ่านสาหรับการเข้าถึงข้อมูลของบริษัทเพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และจะต้องไม่วางทิ้งไว้ในที่สาธารณะ
- ต้องสารองข้อมูลที่เกี่ยวข้องกับบริษัทเป็นประจาเพื่อป้องกันการสูญหาย
- แจ้งให้บริษัททราบในกรณีที่อุปกรณ์ที่เก็บข้อมูลของบริษัทสูญหายหรือถูกขโมย
- รับผิดชอบต่อความเสี่ยงที่ข้อมูลส่วนตัวหรือข้อมูลของบริษัท บนอุปกรณ์ส่วนตัวจะสูญหายอันเกิดจากความล้มเหลวของระบบปฏิบัติการ ไวรัส โปรแกรมประสงค์ร้าย (malware) หรือข้อผิดพลาดใดๆ ของซอฟต์แวร์และตัวอุปกรณ์

- ส่งคืนหรือทำลายข้อมูลของบริษัทที่อยู่ในอุปกรณ์สื่อสาร ไร้สายส่วนตัวเมื่อสิ้นสุดการเป็นพนักงาน
- บริษัทสงวนสิทธิ์ในการตัดสัญญาณการเชื่อมต่อเครือข่ายหรืองดให้บริการโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

4.4 การสำรองข้อมูล

- สำรองข้อมูลในระบบข้อมูลสารสนเทศและ Hard Drives ของบริษัทมาไว้ที่สื่อบันทึกข้อมูล เช่น USB Drives, External Hard Disk และแผ่นดิสก์ ให้เป็นปัจจุบันอย่างสม่าเสมอ
- สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษระหว่างหน่วยงาน/บริษัท

4.5 การแลกเปลี่ยนข้อมูลสารสนเทศกับบุคคลภายนอก

- ในกรณีที่จาเป็นต้องให้ข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษแก่บุคคลภายนอกหรือบุคคลที่ไม่ได้รับอนุญาตต้องได้รับการตรวจสอบความถูกต้องของข้อมูลจากผู้รับผิดชอบดูแลข้อมูลสารสนเทศและต้องได้รับอนุญาตจากผู้บริหาร รวมทั้งบุคคลภายนอกจะต้องลงนามในข้อตกลงห้ามเปิดเผยข้อมูล (Non Disclosure Agreement หรือ NDA)
- สร้างรหัสลับ (Encryption) เมื่อส่งข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษให้กับบุคคลภายนอก

4.6 การใช้อินเทอร์เน็ต

- ไม่ใช้อินเทอร์เน็ตในทางที่ละเมิดกฎหมายลิขสิทธิ์ เช่น การดาวน์โหลดโปรแกรม ไฟล์เพลง ไฟล์ภาพยนตร์ รูปภาพหรือข้อความของบุคคลอื่นบนเว็บไซต์โดยไม่ได้รับอนุญาตและนาไปใช้เพื่อแสวงหาผลประโยชน์โดยไม่ได้รับอนุญาตจากเจ้าของ
- ไม่ใช้อินเทอร์เน็ตเพื่อกระทาการใดๆ ซึ่งขัดต่อจรรยาบรรณธุรกิจของบริษัท
- ไม่ใช้อินเทอร์เน็ตของบริษัทซึ่งทำให้การใช้งานอินเทอร์เน็ตของบุคคลอื่นช้าลง เช่น ดาวน์โหลดไฟล์จานวนมากเกินไป

4.7 การใช้อีเมล

- ห้ามส่งอีเมลแก่บุคคลอื่นโดยปลอมแปลงแหล่งที่มาของการส่งอีเมล อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

- ห้ามส่งอีเมลที่มีข้อความหรือรูปภาพซึ่งก่อให้เกิดความเดือดร้อนราคาญแก่ผู้รับ มีเนื้อหาผิดกฎหมาย สร้างความอับอาย คุกคาม ก้าวร้าว สร้างความเกลียดชังหรือสนับสนุนให้มีการกระทาผิดกฎหมาย
- ระมัดระวังเมื่อจาเป็นต้องเปิดอีเมลจากผู้ส่งที่ไม่รู้จักซึ่งอาจพบโปรแกรมประสงค์ร้าย (malware) การหลอกเก็บข้อมูลที่มาจากอีเมลหลอกลวง (phishing) รวมถึงระมัดระวังอีเมลจากผู้ที่ไม่รู้จักและแจ้งฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อพบอีเมลที่ต้องสงสัย
- ระมัดระวังในการเปิดลิงค์ซึ่งอาจพบโปรแกรมประสงค์ร้าย (malware) เช่น ไวรัส spyware trojan เป็นต้น
- ไม่ส่งอีเมลทางธุรกิจโดยใช้สาเนาลับ (Blind Carbon Copy: Bcc)

4.8 การทำลายข้อมูลสารสนเทศ

- ข้อมูลสารสนเทศที่จัดพิมพ์เป็นเอกสารในรูปแบบกระดาษหรือวัตถุใดๆ ซึ่งอยู่ในระดับเอกสารใช้ภายในเท่านั้น เอกสารลับและเอกสารลับพิเศษ เมื่อไม่ต้องการแล้วให้ทาลายโดยเครื่องทาลายเอกสารเท่านั้น ส่วนเอกสารเปิดเผยให้ทิ้งลงถังขยะหรือเครื่องทำลายเอกสาร
- ย้ายข้อมูลสารสนเทศที่สาคัญแล้วจึงลบข้อมูลสารสนเทศเป็นการถาวรก่อนทาลายสื่อบันทึก

4.9 การตรวจสอบการรั่วไหลของข้อมูลสารสนเทศ

ในกรณีที่เกิดการรั่วไหลของข้อมูลสารสนเทศที่อยู่ในระดับลับและลับพิเศษ ผู้บริหารที่รับผิดชอบต้องแต่งตั้งคณะกรรมการสอบสวนเพื่อสอบสวนและตรวจสอบหาสาเหตุความผิดพลาด พร้อมทั้งปรับปรุงวิธีจัดเก็บข้อมูลสารสนเทศไม่ให้รั่วไหลและระบบการป้องกันการรั่วไหลของข้อมูลสารสนเทศ ตลอดจนรายงานให้ผู้บริหารรับทราบ

5 หน้าที่และความรับผิดชอบ

5.1 คณะกรรมการ

- กำหนดให้มีนโยบายและแนวปฏิบัติเรื่องการบริหารจัดการข้อมูลสารสนเทศ
- กำกับดูแลให้มีการนานโยบายและแนวปฏิบัติไปปฏิบัติอย่างเป็นรูปธรรม
- ดูแลรักษาเทคโนโลยีสาหรับระบบข้อมูลสารสนเทศ
- ควบคุมการเข้าถึงระบบข้อมูลสารสนเทศและเครือข่าย
- รักษาความปลอดภัยของข้อมูลสารสนเทศ
- จัดให้มีการเก็บสารองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง

- ตรวจสอบให้มีการบริหารจัดการข้อมูลสารสนเทศตามนโยบายฯ
- ให้คำแนะนาและให้ความรู้แก่บุคลากรเพื่อให้เกิดการปฏิบัติตามนโยบายฯ

5.2 ผู้บริหาร

- จัดให้มีระเบียบปฏิบัติให้เหมาะสมกับบริบทของบริษัท
- จัดให้มีโครงสร้างผู้รับผิดชอบ เช่น หน่วยงาน หรือบุคคลผู้รับผิดชอบเพื่อดูแลข้อมูลและระบบสารสนเทศ
- กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ
- มั่นใจว่ามีการบริหารความเสี่ยงจากการใช้ข้อมูลสารสนเทศ
- มั่นใจว่ามีการรายงานผลการปฏิบัติงานตามนโยบายฯ รวมถึงรายงานปัญหาจากการใช้ข้อมูลสารสนเทศ

5.3 พนักงาน

- รักษาความลับและปกป้องความปลอดภัยของข้อมูลส่วนตัว รวมทั้งข้อมูลสารสนเทศของบริษัท ลูกค้าและคู่ค้าธุรกิจและพันธมิตรทางธุรกิจ
- จัดทาข้อมูลสารสนเทศ บันทึกและรายงานให้มีความถูกต้อง น่าเชื่อถือ
- ปกป้องทรัพย์สินทางปัญญาของบริษัท และไม่ละเมิดสิทธิในทรัพย์สินทางปัญญาของผู้อื่น
- ปฏิบัติตามนโยบายฯ กฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลสารสนเทศ