นิยาม

บริษัทฯ / องค์กร	หมายถึง	บริษัท แอสเซท ไฟว์ กรุ๊ป จำกัด (มหาชน)
บริษัทย่อย	หมายถึง	บริษัทหรือนิติบุคคลที่ บริษัท แอสเซท ไฟว์ กรุ๊ป จำกัด (มหาชน) ถือหุ้นที่มีสิทธิออกเสียงเกินกว่าร้อยละ 50 ไม่ว่าจะถือหุ้นโดยตรงหรือถือหุ้นโดยอ้อม
กลุ่มแอสเซท ไฟว์ / กลุ่มบริษัท	หมายถึง	1. บริษัท แอสเซท ไฟว์ กรุ๊ป จำกัด (มหาชน) และ 2. บริษัทย่อยของบริษัท แอสเซท ไฟว์ กรุ๊ป จำกัด (มหาชน)
กรรมการบริษัท	หมายถึง	กรรมการบริษัท แอสเซท ไฟว์ กรุ๊ป จำกัด (มหาชน)
ผู้บริหาร	หมายถึง	ประธานเจ้าหน้าที่บริหาร หรือผู้ดำรงตำแหน่งระดับบริหารสี่รายแรกนับต่อจากประธานเจ้าหน้าที่บริหารลงมา ผู้ซึ่งดำรงตำแหน่งเทียบเท่ากับผู้ดำรงตำแหน่งระดับบริหารรายที่สี่ทุกรายและหมายความรวมถึงผู้ดำรงตำแหน่งระดับบริหารในสายงานบัญชีหรือการเงินที่เป็นระดับผู้จัดการฝ่ายขึ้นไปหรือเทียบเท่า
ข้อมูล (Data)	หมายถึง	ข้อมูลทุกประเภทที่จัดเก็บหรือประมวลผลโดยระบบสารสนเทศของบริษัท
ผู้ใช้งาน (User)	หมายถึง	บุคลากรที่ได้รับอนุญาตให้เข้าถึงระบบหรือข้อมูลของบริษัท
เจ้าของระบบงาน (Data Owner)	หมายถึง	ผู้ที่ได้รับมอบหมายให้รับผิดชอบข้อมูลหรือระบบใดระบบหนึ่ง
BYOD (Bring Your Own Device)	หมายถึง	การอนุญาตให้พนักงานใช้อุปกรณ์ส่วนตัว เช่น Notebook, Smartphone เชื่อมต่อกับเครือข่ายหรือระบบของบริษัทฯ

วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อกำหนดกรอบและมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ เพื่อปกป้องข้อมูล ทรัพยากร และระบบงานจากการเข้าถึง การใช้ หรือการเปิดเผยโดยไม่ได้รับอนุญาต กำหนดการควบคุมสิทธิ์ผู้ใช้งานให้เหมาะสมกับหน้าที่ พร้อมแต่งตั้งเจ้าของชุดข้อมูล (Data Owner) เพื่อดูแลสิทธิ์และความถูกต้องของข้อมูล ส่งเสริมการใช้งานอุปกรณ์ส่วนตัวอย่างปลอดภัย (BYOD) และบริหารจัดการข้อมูลให้มีการจำแนก สำรอง และทำลายอย่างถูกวิธี

รวมไปถึงควบคุมการใช้บัญชีสิทธิ์ระดับสูง (Privilege User) การรายงานเหตุการณ์ด้านความปลอดภัย (Incident Management) และการสร้างความตระหนักรู้ผ่านการอบรมพนักงานอย่างต่อเนื่อง

ขอบเขต

นโยบายนี้ครอบคลุมพนักงานทุกระดับ รวมถึงพนักงานชั่วคราว ที่มีสิทธิ์การเข้าถึงระบบสารสนเทศของบริษัท ซึ่งรวมถึงระบบงานหลัก เช่น ERP ระบบ Workflow (E-Memo) และระบบพื้นฐาน (Shared Drive กลางบริษัท) อุปกรณ์เทคโนโลยีสารสนเทศทั้งหมดที่เชื่อมต่อกับเครือข่ายบริษัท ไม่ว่าจะเป็นของบริษัทหรือของพนักงาน (BYOD)

1. การควบคุมการเข้าถึงข้อมูล (Access Control)

หลักการ

กำหนดให้มีการควบคุมสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศตามหลัก "Least Privilege" และ "Need to Know" เพื่อให้พนักงานแต่ละคนเข้าถึงข้อมูลเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น

แนวทางปฏิบัติ

1.1 ผู้ใช้งานทุกคนต้องมีบัญชีผู้ใช้เฉพาะบุคคล (Unique User ID) และห้ามใช้บัญชีร่วมกัน โดยแบ่งแยกไปตามระบบงาน เช่น E-mail , ระบบ ERP , ระบบ Work Flow รวมไปถึงระบบการเข้าถึงการใช้งานอินเตอร์เน็ต VPN

1.2 การสร้าง หรือแก้ไขบัญชีผู้ใช้งาน ส่วนใดส่วน ต้องได้รับการอนุมัติจาก CFO และหัวหน้าตามสายผู้บังคับบัญชา

1.3 ต้องมีการกำหนดสิทธิ์ (Role-based Access Control) ในระบบงานต่างๆ แยกตามหน้าที่ที่ได้รับมอบหมาย

1.4 ฝ่ายเทคโนโลยีสารสนเทศ ทำการสอบทานสิทธิ์ (User Profile Review) อย่างน้อยปีละ 1 ครั้ง โดยร่วมกับหัวหน้าแผนก

1.5 การเข้าถึงข้อมูลสำคัญหรือข้อมูลระดับแผนก จะต้องผ่านระบบยืนยันตัวตนที่ปลอดภัย เช่น Username & Password, หรือผ่านระบบ VPN (กรณีเข้าถึงข้อมูลจากภายนอกบริษัท) เพื่อเป็นการยืนยันตัวตนว่าเป็นพนักงานหรือบุคคลที่ได้รับมอบหมายให้เข้าถึงข้อมูลนั้นจริง

1.6 เมื่อพนักงานลาออกหรือโอนย้าย ฝ่ายเทคโนโลยีสารสนเทศจะต้องยกเลิกสิทธิ์ การเข้าถึงระบบงานต่างๆ หลังจากวันที่สิ้นสุดการเป็นพนักงาน โดยอ้างอิงข้อมูลจาก E-mail แจ้งพนักงานลาออกจากฝ่ายทรัพยากรบุคคลภายใน 3 วัน ทำการ และแจ้งผลทางอีเมลให้ฝ่ายทรัพยากรบุคลรับทราบเมื่อดำเนินการเสร็จสิ้น กรณีเป็นการโอนย้ายจะทำการขออนุมัติเปลี่ยนแปลงสิทธิ์พนักงานผ่านระบบ Work Flow (E-memo) โดยจะต้องได้รับการอนุมัติจาก CFO และผู้บังคับบัญชาตามสายงาน

2. การกำหนดเจ้าของชุดข้อมูล (Data Owner)

หลักการ

เพื่อให้การจัดเก็บ การเข้าถึง และการปกป้องข้อมูลใน Shared Drive ของบริษัทมีความปลอดภัยและมีผู้รับผิดชอบอย่างชัดเจน บริษัทกำหนดให้ทุกชุดข้อมูลภายใน Shared Drive ต้องมีผู้รับผิดชอบในบทบาท “เจ้าของชุดข้อมูล (Data Owner)” ตามโครงสร้างของแต่ละแผนก

แนวทางปฏิบัติ

2.1 Shared Drive ของบริษัทฯ แบ่งออกเป็นโฟลเดอร์ตามแผนก เช่น บัญชี การเงิน ก่อสร้าง จัดซื้อ การตลาด การขาย เทคโนโลยีสารสนเทศ รวมไปถึง Shared Drive ที่มีพนักงานแต่ละแผนกร่วมกันใช้งานมากกว่าหนึ่งแผนกขึ้นไป

2.2 หัวหน้าแผนกหรือผู้ที่ได้รับมอบหมายทำหน้าที่เป็น Data Owner ของโฟลเดอร์แผนกตนเอง โดยมีหน้าที่ดังนี้

2.2.1 กำหนดและอนุมัติสิทธิ์การเข้าถึงไฟล์หรือโฟลเดอร์ภายในแผนก

2.2.2 ตรวจสอบสิทธิ์ผู้ใช้งานใน Shared Drive ของแผนก

2.2.3 ประสานงานกับฝ่ายเทคโนโลยีสารสนเทศ เมื่อจำเป็นต้องเพิ่ม ลด ปรับเปลี่ยนสิทธิ์ หรือยกเลิกสิทธิ์ผู้ใช้งาน

2.2.4 ควบคุมให้ข้อมูลใน Shared Drive ของแผนกมีความถูกต้อง ครบถ้วน และไม่ซ้ำซ้อน

2.2.5 รับผิดชอบต่อความปลอดภัยของข้อมูล รวมถึงการปฏิบัติตามนโยบายมาตรการในการป้องกันการรั่วไหลของข้อมูล และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ

2.3 ฝ่ายเทคโนโลยีสารสนเทศจัดทำและเก็บรักษา ทะเบียนรายชื่อ Data Owner ของแต่ละแผนก พร้อมระดับสิทธิ์ที่ได้รับ และสอบทานสิทธิ์ (User Profile Review) ข้อมูลอย่างน้อยปีละ 1 ครั้ง

2.4 หากแผนกใดไม่มีการแต่งตั้ง Data Owner อย่างเป็นทางการ ให้หัวหน้าแผนกถือเป็น Data Owner

2.5 ในกรณีที่พนักงานลาออก หรือโอนย้าย Data Owner จะต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศ เพื่อปรับสิทธิ์การเข้าถึงข้อมูล หรือยุติการให้สิทธิ์การเข้าถึงข้อมูล

3. การใช้และขออนุมัติอุปกรณ์ส่วนตัว (BYOD)

หลักการ

เพื่อเพิ่มความยืดหยุ่นในการทำงานและสนับสนุนการทำงานแบบดิจิทัล บริษัทอนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนตัว เช่น MacBook, Smartphone, Tablet เพื่อเชื่อมต่อกับระบบสารสนเทศของบริษัทได้ ภายใต้เงื่อนไขการรักษาความมั่นคงปลอดภัยของข้อมูลที่ชัดเจน

แนวทางปฏิบัติ

3.1 การขออนุมัติใช้งาน

3.1.1 พนักงานที่ต้องการใช้อุปกรณ์ส่วนตัวเพื่อเข้าถึงระบบของบริษัท หรือเชื่อมต่ออุปกรณ์ภายในบริษัท เช่น E-mail , Printer ต้องยื่นคำขออนุมัติผ่านฝ่ายเทคโนโลยีสารสนเทศ โดยระบุประเภทอุปกรณ์และวัตถุประสงค์การใช้งาน ผ่านแบบฟอร์มคำขอและจะต้องให้เจ้าหน้าหน้าฝ่ายเทคโนโลยีสารสนเทศตรวจสอบอุปกรณ์เบื้องต้น

3.1.2 ฝ่ายเทคโนโลยีสารสนเทศ จะพิจารณาความเหมาะสมของอุปกรณ์ เช่น ระบบปฏิบัติการ ความปลอดภัยและช่องทางเชื่อมต่อ ก่อนอนุมัติ

3.1.3 เมื่อได้รับอนุมัติ ฝ่ายเทคโนโลยีสารสนเทศจะขึ้นทะเบียนอุปกรณ์นั้นไว้ใน BYOD Register เพื่อใช้ในการติดตามและจัดการอุปกรณ์ตามความเหมาะสม

3.2 ข้อกำหนดด้านความปลอดภัยของอุปกรณ์

3.2.1 อุปกรณ์ส่วนตัวที่ได้รับอนุมัติต้องมีการตั้งรหัสผ่านหรือระบบยืนยันตัวตน เช่น PIN, Password หรือ Biometric

3.2.2 ต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส (Antivirus / Mobile Security) และอัปเดตระบบปฏิบัติการเป็นปัจจุบันอยู่เสมอ

3.2.3 ต้องเชื่อมต่อผ่านช่องทางที่ปลอดภัย เช่น เครือข่าย Wi-Fi ของบริษัทเท่านั้น

3.2.4 ไม่อนุญาต หากตรวจสอบเบื้องต้นพบว่าอุปกรณ์เคยผ่านการ Root หรือ Jailbreak อุปกรณ์ เพราะอาจทำให้ระบบความปลอดภัยถูกปิดกั้น และต้องไม่ติดตั้ง Application จากภายนอกจาก App store (iOS) หรือ Play Store (Android)

3.2.5 ห้ามเก็บข้อมูลที่เป็นความลับของบริษัทไว้ในเครื่องโดยตรง เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษร อีเมลหรือระบบ Work Flow (E-memo) จาก Data Owner

3.2.6 อุปกรณ์ส่วนตัวจะไม่อนุญาตให้เข้าถึง Shared Drive ของบริษัท

3.2.7 อุปกรณ์ส่วนตัวจะต้องไม่ติดตั้ง Software ที่ละเมิดลิขสิทธิ์ หรือมีข้อมูลละเมิดลิขสิทธิ์ใดๆอยู่บนตัวอุกรณ์

3.3 ความรับผิดชอบของผู้ใช้งาน

3.3.1 ผู้ใช้งานต้องรับผิดชอบต่อการรักษาความปลอดภัยของอุปกรณ์ส่วนตัวตลอดระยะเวลาที่ใช้เชื่อมต่อกับระบบบริษัท

3.3.2 หากอุปกรณ์สูญหาย ถูกขโมย หรือสงสัยว่าข้อมูลรั่วไหล ต้องแจ้งฝ่าย IT ภายใน **24 ชั่วโมง** เพื่อให้ดำเนินการจำกัดสิทธิ์หรือระงับการเข้าถึงระบบ

3.3.3 ผู้ใช้งานต้องยินยอมให้ฝ่ายเทคโนโลยีสารสนเทศ ดำเนินการตรวจสอบหรือกำหนดค่าความปลอดภัยในอุปกรณ์หากจำเป็น เพื่อป้องกันความเสี่ยง

3.4 การเพิกถอนสิทธิ์และการออกจากระบบ

3.4.1 ฝ่ายเทคโนโลยีสารสนเทศ มีสิทธิ์ระงับการเชื่อมต่อของอุปกรณ์ BYOD ได้ทันที หากตรวจพบการละเมิดนโยบายหรือภัยคุกคามด้านความปลอดภัย

3.4.2 เมื่อพนักงานลาออก หรือไม่ต้องใช้ระบบบริษัทบนอุปกรณ์ส่วนตัวอีกต่อไป ต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศ ดำเนินการลบสิทธิ์การเข้าถึงทั้งหมด รวมถึงข้อมูลที่เกี่ยวข้องกับบริษัทในอุปกรณ์นั้น

3.4.3 หากฝ่ายเทคโนโลยีสารสนเทศ ได้รับข้อมูลการละเมิดลิขสิทธิ์ อันเนื่องมาจากอุปกรณ์ส่วนตัวของพนักงาน ภายหลังการตรวจสอบอุปกรณ์และขึ้นทะเบียนอุปกรณ์ BYOD แล้วนั้น พนักงานเจ้าของอุปกรณ์จะต้องเป็นผู้รับผิดชอบความเสียหายที่เกิดขึ้นทุกกรณี

3.5 การบังคับใช้

3.5.1 พนักงานที่ไม่ปฏิบัติตามหรือฝ่าฝืนข้อกำหนดด้านความปลอดภัยของอุปกรณ์ BYOD หรือเป็นเหตุทำให้ข้อมูลของบริษัทรั่วไหล จะถูกระงับสิทธิ์การใช้งานระบบทันที และต้องรับบทลงโทษเป็นไปตามข้อบังคับเกี่ยวกับการทำงานของบริษัท และบริษัทย่อย

3.5.2 บริษัทสงวนสิทธิ์ในการดำเนินคดีทางกฎหมายหากความเสียหายเกิดจากการจงใจหรือประมาทร้ายแรง

4. การบริหารจัดการข้อมูล (Information Handling)

หลักการ

ข้อมูลของบริษัทถือเป็นทรัพย์สินที่มีคุณค่าทางธุรกิจ และเป็นส่วนสำคัญในการดำเนินงานของทุกฝ่าย บริษัทจึงกำหนดให้มีแนวทางในการจัดเก็บ ใช้งาน เผยแพร่ และทำลายข้อมูลอย่างเป็นระบบ เพื่อให้มั่นใจว่าข้อมูลทั้งหมดได้รับการปกป้อง

แนวทางปฏิบัติ

4.1 การจำแนกประเภทของข้อมูล (Data Classification) บริษัทกำหนดให้ข้อมูลทุกชุดที่จัดเก็บในระบบ เช่น Shared Drive, ERP, E-Memo หรืออีเมล ต้องถูกจำแนกตามระดับความสำคัญและความอ่อนไหว เพื่อกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสม ดังนี้

ระดับข้อมูล	คำอธิบาย	ตัวอย่าง	การควบคุม
Public	ข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้โดยไม่กระทบต่อบริษัท	ข้อมูลประชาสัมพันธ์, เว็บไซต์	สามารถเผยแพร่ได้โดยไม่ต้องอนุมัติ
Internal Use	ข้อมูลที่ใช้ภายในบริษัทเท่านั้น ห้ามเผยแพร่ภายนอก	เอกสารการทำงานทั่วไป, E-Memo ภายใน	จำกัดสิทธิ์เฉพาะพนักงานในระบบ
Confidential	ข้อมูลที่มีความอ่อนไหว ต้องได้รับการปกป้องเป็นพิเศษ	งบการเงิน, Payroll, สัญญา, ข้อมูลลูกค้า	เข้าถึงได้เฉพาะผู้ได้รับอนุมัติจาก Data Owner
Restricted	ข้อมูลสำคัญระดับสูงมากที่มีผลกระทบต่อธุรกิจโดยตรง	ข้อมูลเจรจาธุรกิจ, ข้อตกลงเชิงกลยุทธ์	จำกัดการเข้าถึงเฉพาะผู้บริหารหรือบุคลากรเฉพาะกิจเท่านั้น

4.2 การเข้าถึงและใช้งานข้อมูล (Access and Usage)

4.2.1 ผู้ใช้งานต้องเข้าถึงข้อมูลตามสิทธิ์ที่ได้รับจาก Data Owner หรือตาม Role-based Access Control ที่ได้รับ เท่านั้น

4.2.2 ห้ามใช้ข้อมูลภายในบริษัทเพื่อประโยชน์ส่วนตัวหรือส่งต่อให้บุคคลภายนอกโดยไม่ได้รับอนุญาต

4.2.3 หากจำเป็นต้องส่งข้อมูลให้หน่วยงานภายนอก ต้องใช้ช่องทางที่ได้รับอนุมัติจาก Data Owner เช่น Secure Email หรือ Drive ที่มีการป้องกันด้วยสิทธิ์เข้าถึง (Permission-based Sharing)

4.2.4 ห้ามนำข้อมูลภายในบริษัทไปจัดเก็บใน Cloud ส่วนตัว เช่น Google Drive ส่วนตัว, Dropbox, iCloud เป็นต้น

4.3 การจัดเก็บและสำรองข้อมูล (Storage and Backup)

4.3.1 ข้อมูลทั้งหมดของบริษัทต้องถูกจัดเก็บไว้ในพื้นที่ที่ได้รับอนุมัติ เช่น Shared Drive ของบริษัท หรือระบบ ERP และระบบ Work Flow (E-memo) ที่อยู่ในโครงสร้าง Network ของผู้ให้บริการระบบ ERP เท่านั้น

4.3.2 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีระบบสำรองข้อมูล (Backup System) ที่ครอบคลุมทั้งข้อมูลใน Shared Drive ตามคู่มือการปฏิบัติงานการ Backup Data ของบริษัท และตรวจสอบความสมบูรณ์การ Backup ฐานข้อมูลของระบบ ERP ตามข้อตกลงการให้บริการของผู้ให้บริการระบบ ERP

4.4 การแก้ไขและปรับปรุงข้อมูล (Data Update and Change Control)

4.4.1 ผู้มีสิทธิ์แก้ไขข้อมูลต้องเป็นบุคคลที่ได้รับอนุมัติจาก Data Owner เท่านั้น

4.4.2 หากเป็นข้อมูลสำคัญ เช่น งบประมาณ หรือข้อมูลทางบัญชี ต้องมีการตรวจสอบและอนุมัติการเปลี่ยนแปลงโดยผ่านระบบ Work Flow (E-memo)

4.5 การทำลายและการเก็บรักษาข้อมูล (Data Retention & Disposal)

4.5.1 ข้อมูลที่หมดอายุการใช้งานหรือไม่จำเป็นต้องเก็บรักษาอีกต่อไป ต้องดำเนินการทำลายอย่างปลอดภัย โดยใช้วิธีการที่ไม่สามารถกู้คืนได้ เช่น การลบถาวร (Permanent Delete) , การทำลายสื่อบันทึก (เช่น HDD, USB) อย่างถูกวิธี

4.5.2 ฝ่ายเทคโนโลยีสารสนเทศจะต้องให้คำแนะนำแก่แต่ละแผนกเกี่ยวกับวิธีการทำลายข้อมูลที่ถูกต้องและปลอดภัย

4.6 การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)

4.6.1 การดาวน์โหลดหรือส่งออกข้อมูลจำนวนมากจากระบบ ERP หรือ Shared Drive ต้องได้รับการอนุมัติล่วงหน้าจาก Data Owner

4.6.2 สามารถใช้สื่อบันทึกข้อมูลภายนอก เช่น Flash Drive, External HDD ได้ โดยจะต้องทำการเข้ารหัสข้อมูล หรือใส่รหัสผ่านในการเปิดไฟล์ต่างๆ

4.7 ความรับผิดชอบของผู้ใช้งาน

4.7.1 พนักงานทุกคนมีหน้าที่ดูแลความปลอดภัยของข้อมูลที่อยู่ในความรับผิดชอบของตนเอง

4.7.2 ต้องปฏิบัติตามนโยบายมาตรการในการป้องกันการรั่วไหลของข้อมูล และรายงานต่อฝ่ายเทคโนโลยีสารสนเทศ หากพบเหตุการณ์ที่อาจส่งผลต่อความปลอดภัยของข้อมูล

5. การรักษาความมั่นคงของระบบ (System Security)

หลักการ

บริษัทฯ ต้องดำเนินมาตรการเพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ทั้งภายในและภายนอก

แนวทางปฏิบัติ

1. ฝ่ายเทคโนโลยีสารสนเทศจะต้องติดตั้งระบบป้องกันภัย เช่น Firewall, Antivirus, Endpoint Protection
2. ต้องมีการอัปเดต Patch และซอฟต์แวร์ระบบอย่างสม่ำเสมอ และจะต้องเป็นเวอร์ชั่นที่มีความเสถียร
3. ฝ่ายเทคโนโลยีสารสนเทศจะต้องปฏิบัติตามคู่มือการรักษาความปลอดภัยด้านเทคโนโลยีภายในบริษัทอย่างเคร่งครัด
4. มีการบันทึก Log การเข้าใช้งาน ทั้งระบบ Shared Drive , Work Flow , ERP ของบริษัท

6. การจัดการเหตุการณ์ด้านความปลอดภัย (Incident Management)

หลักการ

เพื่อให้บริษัทสามารถตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพและลดผลกระทบจากเหตุการณ์ที่เกิดขึ้น

แนวทางปฏิบัติ

1. พนักงานทุกคนมีหน้าที่รายงานเหตุการณ์ด้านความปลอดภัย (Security Incident) ทันที เช่น การสงสัยว่าข้อมูลรั่วไหล การได้รับอีเมลปลอม (Phishing) ระบบไม่สามารถเข้าถึงได้โดยไม่ทราบสาเหตุ
2. ฝ่ายเทคโนโลยีสารสนเทศต้องบันทึกและประเมินเหตุการณ์ พร้อมดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชาและพนักงานที่เกี่ยวข้อง ภายใน 24 ชั่วโมง
3. ต้องมีการวิเคราะห์หาสาเหตุ (Root Cause Analysis) และวางมาตรการป้องกันไม่ให้เกิดซ้ำ
4. เก็บหลักฐานทางเทคนิคอย่างปลอดภัย เพื่อใช้ในการตรวจสอบภายหลังหรือตามกฎหมาย

7. การสอบทานสิทธิ์การใช้งานระบบสารสนเทศ (User Profile Review)

หลักการ

การกำหนดสิทธิ์การเข้าถึงต้องสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งาน มีการสอบทานสิทธิ์ผู้ใช้งานเป็นระยะเพื่อลดสิทธิ์ที่เกินจำเป็น และมีการอนุมัติและรับรองสิทธิ์จากเจ้าของชุดข้อมูล (Data Owner) หรือหัวหน้าแผนก

ความรับผิดชอบ (Responsibilities)

หน่วยงาน / บุคคล	หน้าที่หลัก
เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ	- จัดทำรายการผู้ใช้งาน (User List) สำหรับแต่ละระบบ - ดำเนินการสอบทานสิทธิ์ตามรอบเวลา - บันทึกและเก็บหลักฐานการสอบทานสิทธิ์ทุกครั้ง - ดำเนินการปรับสิทธิ์หรือยกเลิกบัญชีตามผลการสอบทาน
หัวหน้าแผนก / Data Owner	- ตรวจสอบรายชื่อผู้ใช้งานและสิทธิ์ที่ได้รับ - ยืนยันความถูกต้อง หรือเสนอให้ปรับ / ยกเลิกสิทธิ์ - ลงนามรับรองผลการสอบทานสิทธิ์ในแบบฟอร์มที่กำหนด ผ่านอีเมลหรือระบบ Work Flow (E-memo)
ผู้บริหารระดับสูง	- รับรองผลการสอบทานสิทธิ์ภาพรวมประจำปี - กำกับดูแลให้ทุกหน่วยงานดำเนินการสอบทานสิทธิ์ตามนโยบาย
ผู้ใช้งาน (User)	- ตรวจสอบสิทธิ์ของตนเองให้สอดคล้องกับงานที่ได้รับมอบหมาย - แจ้งฝ่ายเทคโนโลยีสารสนเทศ หากพบสิทธิ์ที่ไม่เกี่ยวข้องหรือไม่จำเป็น

แนวทางปฏิบัติ

1. การสอบทานสิทธิ์ต้องดำเนินการอย่างน้อย ปีละ 1 ครั้ง และจะต้องมีการสอบทานสิทธิ์เพิ่มเติมเมื่อเกิดเหตุการณ์ต่อไปนี้
   - 7.1.1 พนักงานลาออก หรือพ้นสภาพการเป็นพนักงาน
   - 7.1.2 พนักงานเปลี่ยนตำแหน่ง / ย้ายแผนก
   - 7.1.3 มีการปรับโครงสร้างแผนก หรือเปลี่ยนเจ้าของข้อมูล (Data Owner)
   - 7.1.4 ระบบมีการเปลี่ยนแปลงฟังก์ชันหรือเพิ่มโมดูลใหม่
2. ขั้นตอนการสอบทานสิทธิ์ (Review Process)
   - 7.2.1 จัดทำรายชื่อผู้ใช้งาน (User Access List) เจ้าหน้าที่เทคโนโลยีสารสนเทศ จะดึงข้อมูลรายชื่อผู้ใช้งานจากแต่ละระบบ พร้อมรายละเอียด เช่น ชื่อผู้ใช้งาน แผนก / ตำแหน่ง สิทธิ์การเข้าถึง (Read / Edit / Admin / Approval)
   - 7.2.2 ส่งรายชื่อให้หัวหน้าแผนกหรือ Data Owner ตรวจสอบ เจ้าหน้าที่เทคโนโลยีสารสนเทศ จะส่งแบบฟอร์ม "User Profile Review Form" ให้หัวหน้าแผนกหรือ Data Owner เพื่อดำเนินการตรวจสอบ ผ่าน E-mail หรือระบบ Workflow (E-memo)
   - 7.2.3 การตรวจสอบและรับรองสิทธิ์ (Review & Sign-off) หัวหน้าแผนก หรือ Data Owner จะต้องตรวจสอบแต่ละชื่อผู้ใช้งาน พิจารณาลงนามหากข้อมูลถูกต้อง

8. การฝึกอบรมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness & Training)

หลักการ

บริษัทตระหนักถึงความสำคัญของการสร้างความรู้ ความเข้าใจ และจิตสำนึกด้านความมั่นคงปลอดภัยสารสนเทศให้กับพนักงานทุกระดับ เพื่อป้องกันความเสี่ยงที่เกิดจากความประมาท ความไม่รู้ หรือการละเมิดนโยบายโดยไม่ได้ตั้งใจ การฝึกอบรมและให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ ถือเป็นส่วนหนึ่งของมาตรการเชิงป้องกัน (Preventive Control) ที่ช่วยเสริมสร้างวัฒนธรรมความปลอดภัยของข้อมูลภายในองค์กร

วัตถุประสงค์

1. เพื่อให้พนักงานทุกคนเข้าใจนโยบายและมาตรการด้านความมั่นคงปลอดภัยของบริษัท
2. เพื่อสร้างความตระหนักรู้ในการปกป้องข้อมูลสำคัญของบริษัท ลูกค้า และพันธมิตรทางธุรกิจ
3. เพื่อให้พนักงานรู้จักภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น และสามารถตอบสนองได้อย่างเหมาะสม

4. เพื่อให้สอดคล้องกับข้อกฎหมายที่เกี่ยวข้อง เช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)

แนวทางปฏิบัติ

8.1 การจัดอบรมประจำปี

8.1.1 บริษัทฯ กำหนดให้มีการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง สำหรับพนักงานทุกระดับ

8.1.2 การอบรมจะจัดในรูปแบบ Classroom, Online Training หรือ e-Learning ตามความเหมาะสม

8.1.3 พนักงานใหม่ทุกคนต้องผ่านการอบรมเบื้องต้นเกี่ยวกับภัยคุกคามทางไซเบอร์และ ข้อห้ามรวมถึงข้อควรระวังในการใช้งานระบบสารสนเทศ ภายใน 30 วันหลังจากเริ่มงาน

8.2 หัวข้อการอบรม (Training Topics) เนื้อหาการอบรมควรครอบคลุมหัวข้อหลักดังต่อไปนี้

8.2.1 นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy)

8.2.2 นโยบายการใช้ระบบปัญญาประดิษฐ์ (AI)

8.2.3 นโยบายควบคุมการใช้งานโปรแกรมควบคุมคอมพิวเตอร์ระยะไกล

8.2.4 นโยบายการไม่ละเมิดทรัพย์สินทางปัญญา ลิขสิทธิ์ และโปรแกรมคอมพิวเตอร์

8.2.5 การใช้รหัสผ่านอย่างปลอดภัย (Password Security & MFA)

8.2.6 การจัดการสิทธิ์ผู้ใช้งาน (User Access Management)

8.2.7 การรักษาความลับของข้อมูล (Data Confidentiality)

8.2.8 การป้องกันอีเมลฟิชชิ่งและมัลแวร์ และภัยคุกคามทางไซเบอร์(Phishing & Malware Awareness)

8.2.9 การใช้ Internet อย่างปลอดภัยในที่ทำงาน และนอกสถานที่ทำงาน

8.2.10 แนวทางการใช้ Shared Drive และ Cloud Service อย่างปลอดภัย

8.2.11 การรายงานเหตุการณ์ด้านความปลอดภัย (Incident Reporting Process)

8.2.12 ภาระหน้าที่ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA Awareness)

8.2.13 หัวข้ออื่นๆตามความเหมาะสม

การติดตามและประเมินผล

8.3 ฝ่ายเทคโนโลยีสารสนเทศ (ร่วมกับฝ่ายทรัพยากรบุคคล) ต้องเก็บบันทึก หลักฐานการเข้าร่วมอบรม (Training Record) ของพนักงานทุกคน

8.4 พนักงานจะต้องทำแบบทดสอบหลังการอบรม (Post-Training Assessment) เพื่อวัดความเข้าใจ

8.5 ในกรณีที่พนักงานไม่ผ่านเกณฑ์การทดสอบ ต้องเข้ารับการอบรมซ้ำภายใน 30 วัน

การทบทวนและปรับปรุงโปรแกรมการฝึกอบรม

8.6 ฝ่ายเทคโนโลยีสารสนเทศต้องทบทวนเนื้อหาการอบรมอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับภัยคุกคามและเทคโนโลยีที่เปลี่ยนแปลง

8.7 หากมีเหตุการณ์ด้านความปลอดภัยร้ายแรง หรือการละเมิดนโยบาย บริษัทอาจจัดอบรมเพิ่มเติมเฉพาะกิจ\

การบังคับใช้

8.8 พนักงานทุกคนต้องเข้าร่วมการอบรมตามรอบที่บริษัทกำหนด หากไม่ปฏิบัติตามจะถือเป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และอาจมีผลต่อการประเมินผลการปฏิบัติงานหรือระเบียบวินัยของบริษัท

9. การบริหารจัดการและรายงานผู้ใช้งานสิทธิ์ระดับสูง (Privilege User & Access Management)

หลักการ

เพื่อควบคุมและลดความเสี่ยงจากการใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์ระดับสูง (Privilege User) บริษัทกำหนดให้มีการบริหารจัดการสิทธิ์ดังกล่าวอย่างเข้มงวด โปร่งใส และตรวจสอบได้ โดยมีการบันทึก ติดตาม และรายงานการใช้งานสิทธิ์เหล่านี้อย่างต่อเนื่อง

วัตถุประสงค์

1. เพื่อกำหนดแนวทางการบริหารจัดการบัญชีผู้ใช้งานที่มีสิทธิ์ระดับสูงในระบบสารสนเทศของบริษัท
2. เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
3. เพื่อให้สามารถตรวจสอบและรายงานการใช้งานสิทธิ์ได้อย่างมีระบบและโปร่งใส

ขอบเขต

9.1 ครอบคลุมถึงผู้ใช้งานที่มีสิทธิ์ระดับสูงในทุกระบบสารสนเทศของบริษัท เช่น

9.1.1 ระบบ ERP

9.1.2 ระบบ Workflow (E-memo)

9.1.3 Shared Drive ของบริษัท

9.1.4 ระบบเครือข่าย เช่น Server, Firewall, Router, Switch , Windows Server

9.1.5 ระบบบริหารทรัพยากรบุคคล (Human Resource Management System)

9.1.6 ระบบอื่น ๆ ที่เกี่ยวข้องกับข้อมูลสำคัญหรือการบริหารจัดการผู้ใช้งาน

แนวทางปฏิบัติ

9.2 การกำหนดผู้ใช้งานสิทธิ์ระดับสูง

9.2.1 การมอบหมายสิทธิ์ระดับสูง (Administrator, Super User, Root Access) ต้องได้รับอนุมัติจากผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายอย่างเป็นทางการ

9.2.2 สิทธิ์ระดับสูงต้องมอบให้เฉพาะบุคลากรที่มีความจำเป็นต่อการปฏิบัติงานเท่านั้น และต้องกำหนดช่วงเวลาในการถือสิทธิ์ เช่น Temporary Admin Access

9.2.3 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำทะเบียนบัญชีผู้ใช้งานสิทธิ์ระดับสูง (Privilege User Register) โดยระบุชื่อผู้ถือสิทธิ์ ระบบที่เข้าถึงได้ และวันที่เริ่มต้น-สิ้นสุดการใช้งาน

9.3 การใช้งานบัญชี Privilege

9.3.1 บัญชีผู้ใช้งานสิทธิ์ระดับสูงต้องเป็น บัญชีเฉพาะบุคคล ห้ามใช้บัญชีร่วมกัน

9.3.2 ห้ามใช้บัญชี Privilege เพื่อทำงานทั่วไป เช่น การส่งอีเมล หรือเข้าถึงเอกสารภายใน

9.3.3 การเข้าถึงระบบด้วยสิทธิ์ Privilege ต้องผ่านช่องทางที่ปลอดภัย เช่น VPN หรือเครือข่ายภายในของบริษัทฯ

9.4 การบันทึกและติดตามการใช้งาน (Logging & Monitoring)

9.4.1 ระบบที่มีผู้ถือสิทธิ์ระดับสูงต้องจัดเก็บบันทึกการใช้งาน (Access Log)

9.4.2 Log ต้องระบุข้อมูลสำคัญ เช่น วันที่และเวลาที่เข้าสู่ระบบ กิจกรรมที่ดำเนินการ (เช่น การเพิ่ม/ลบผู้ใช้ การปรับสิทธิ์ การแก้ไขข้อมูลระบบ) รวมไปถึงชื่อผู้ใช้งาน (Username)

9.4.3 ฝ่ายเทคโนโลยีสารสนเทศต้องตรวจสอบ Log การใช้งานของบัญชี Privilege

9.4.4 หากพบกิจกรรมผิดปกติ ต้องรายงานต่อผู้บริหารภายใน 24 ชั่วโมง

9.5 การจัดทำรายงานและการสอบทานสิทธิ์ (Privilege Access Review & Reporting)

9.5.1 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำรายงาน "Privilege Access Report" อย่างน้อยปีละ 2 ครั้ง เพื่อแสดงข้อมูลต่อไปนี้

9.5.1.1 รายชื่อผู้ถือสิทธิ์ระดับสูงในแต่ละระบบ

9.5.1.2 รายละเอียดสิทธิ์ที่ได้รับ และวันที่อนุมัติ

9.5.1.3 กิจกรรมที่ดำเนินการโดยผู้ถือสิทธิ์ (เช่น การเพิ่มผู้ใช้ใหม่ การเปลี่ยนค่าในระบบ)

9.5.1.4 สรุปผลการตรวจสอบเหตุการณ์ผิดปกติ หรือการใช้งานที่เกินขอบเขต

9.5.1.5 มาตรการปรับปรุง หรือข้อเสนอแนะจากฝ่ายเทคโนโลยีสารสนเทศ

9.5.2 รายงานดังกล่าวต้องเสนอผู้บริหารระดับสูงเพื่อรับทราบ และจัดเก็บไว้เป็นหลักฐาน

9.5.3 การสอบทานสิทธิ์ของผู้ถือสิทธิ์ Privilege ต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง โดยร่วมกับหัวหน้าแผนกที่เกี่ยวข้อง

9.6 การเพิกถอนสิทธิ์ (Revocation)

9.6.1 เมื่อผู้ถือสิทธิ์ Privilege ลาออก เปลี่ยนตำแหน่ง เสียชีวิตหรือสิ้นสุดความจำเป็นในการใช้งาน ต้องเพิกถอนสิทธิ์ทันที โดยอ้างอิงข้อมูลจากฝ่ายทรัพยากรบุคคลและวันที่มีผล

9.7 การเก็บรักษาหลักฐานและการตรวจติดตาม

9.7.1 ฝ่ายเทคโนโลยีสารสนเทศต้องเก็บรักษาหลักฐานที่เกี่ยวข้องกับบัญชี Privilege ทั้งหมด ได้แก่

9.7.1.1 แบบฟอร์มอนุมัติสิทธิ์ (Privilege Access Request Form)

9.7.1.2 รายงาน Privilege Access Report

9.7.1.3 Log การใช้งานระบบ

9.7.2 ระยะเวลาเก็บรักษาหลักฐานไม่น้อยกว่า 1 ปี

9.8 การจัดการกรณีฉุกเฉิน (Emergency Privilege Credential Handling)

ในกรณีที่เกิดเหตุฉุกเฉิน เช่น ระบบไม่สามารถเข้าถึงได้ตามปกติ ผู้ดูแลระบบหลักไม่อยู่ หรือเกิดเหตุภัยพิบัติ (Disaster Recovery) บริษัทอาจดำเนินการจัดเก็บข้อมูลรหัสผ่านของบัญชีผู้ใช้งานสิทธิ์ระดับสูง (Privilege Account) ชั่วคราว เพื่อใช้ในการเข้าถึงระบบอย่างจำกัดภายใต้เงื่อนไขต่อไปนี้

9.8.1 การดำเนินการสำรองข้อมูลรหัสผ่าน

9.8.1.1 ฝ่ายเทคโนโลยีสารสนเทศต้องรวบรวมรหัสผ่านของบัญชี Privilege ทุกระบบที่จำเป็น เช่น ERP, Server, Firewall, Database, Network Equipment

9.8.1.2 บันทึกข้อมูลรหัสผ่านลงในไฟล์เอกสารเข้ารหัส (Encrypted File) และจัดเก็บไว้ใน USB Drive ที่มีระบบเข้ารหัส (Encrypted USB / Hardware Encryption)

9.8.2 การส่งมอบและการเก็บรักษา

9.8.2.1 เมื่อดำเนินการเข้ารหัสเรียบร้อยแล้ว ให้บันทึก แบบฟอร์มส่งมอบรหัสผ่าน (Privilege Credential Custody Form) โดยระบุระบบ / รายชื่อบัญชี / วันที่เข้ารหัส / ผู้รับผิดชอบ

9.8.2.2 USB Drive ที่เข้ารหัสต้องส่งมอบให้ ผู้บริหารสูงสุด (CEO) หรือ ผู้ที่ได้รับมอบหมายโดยเป็นลายลักษณ์อักษร

9.8.2.3 ผู้รับมอบและผู้ส่งมอบต้องลงนามในแบบฟอร์มรับส่ง เพื่อเป็นหลักฐานการควบคุม (Chain of Custody)

9.8.2.4 USB Drive ที่เข้ารหัสต้องเก็บรักษาใน ตู้เซฟของบริษัทฯ

9.8.3 การเข้าถึงในกรณีฉุกเฉิน (Break-glass Process)

9.8.3.1 การเปิดใช้งานรหัสผ่านใน USB Drive ต้องได้รับอนุมัติจาก CEO หรือผู้บริหารสูงสุด

9.8.3.2 ทุกการเปิดใช้งานต้องบันทึกเหตุผล วันเวลา ผู้เข้าถึง และระบบที่ดำเนินการไว้ใน "แบบฟอร์มการเข้าถึงฉุกเฉิน (Emergency Access Log)"

9.8.4 การอัปเดตและทำลาย

9.8.4.1 ต้องดำเนินการอัปเดตรหัสผ่านใน USB Drive ที่เข้ารหัสอย่างน้อย ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนรหัสผ่านระบบใดระบบหนึ่ง

9.8.4.2 เมื่อ USB เดิมหมดอายุการใช้งาน หรือมีการออกใหม่ ต้องทำลายสื่อเดิมอย่างปลอดภัย (Secure Erase / Physical Destruction) และบันทึกการทำลายเป็นลายลักษณ์อักษร

การทบทวนนโยบาย

บริษัทฯ จะทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) ของบริษัทฯ และบริษัทย่อย อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงของปัจจัยเสี่ยงต่างๆ ที่มีผลต่อธุรกิจของบริษัทฯ และบริษัทย่อย อย่างมีนัยสำคัญ

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) นี้ ได้จัดทำใหม่และพิจารณาในการประชุมคณะกรรมการบริษัทครั้งที่ 5/2568 เมื่อวันที่ 12 พฤศจิกายน 2568 และมีผลบังคับใช้ตั้งแต่วันที่ 12 พฤศจิกายน 2568 เป็นต้นไป

ประกาศ ณ วันที่ 12 พฤศจิกายน 2568

.....

(รองศาสตราจารย์มานพ พงศทัต)

ประธานกรรมการ

บริษัท แอสเซท ไฟว์ กรุ๊ป จำกัด (มหาชน)