



บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด

Grandway Capital Group Limited | Private Fund Management Licensee

OFFICIAL MASTER GOVERNANCE & OPERATIONS MANUAL

คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศ

และความมั่นคงปลอดภัยไซเบอร์เล่มหลัก

Master Information Security Management System (ISMS) & IT Operations Manual

รหัสเอกสารหลัก: GW-IT-MANUAL-2026	ฉบับที่ (Revision): 2.0 (Official Release)
หน่วยงานรับผิดชอบ: ฝ่ายเทคโนโลยีสารสนเทศ (IT)	วันที่มีผลบังคับใช้: 01 พฤศจิกายน 2569
ระดับชั้นความลับ: ลับเฉพาะภายใน (Confidential)	มาตรฐานกำกับ: ก.ล.ต. สธ. 38/2565 / ISO 27001

ตารางบันทึกการจัดทำ ตรวจสอบ และอนุมัติ (Sign-off & Approvals)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
IT Specialist นายคณาธิปไตย ก้านจักร วันที่: / / 2569	Chief Investment Officer / Compliance นายโสราห์ ตั้งลิขานนท์ วันที่: / / 2569	กรรมการผู้จัดการ (Managing Director) นายเอกณัฐ กุณทลบุตร วันที่: / / 2569

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 2 / 107
--	--	--

สารบัญชุดเอกสารแม่บทด้านเทคโนโลยีสารสนเทศ (Master Suite Index)

รหัสเอกสาร	ชื่อเอกสารระเบียบปฏิบัติการ / ข้อกำหนดทางเทคนิค	สถานะ
หมวดที่ 1: จริยธรรมและนโยบายแม่บทระดับสูง (Governance & Policies)		หมวดหมู่
GW-ETH-01	กฎระเบียบและจริยธรรมในการทำงานสำหรับฝ่ายไอที	บังคับใช้
GW-POL-01	นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	บังคับใช้
GW-POL-02	นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ	บังคับใช้
GW-BCP-01	นโยบายการบริหารความต่อเนื่องทางธุรกิจ (BCM Policy)	บังคับใช้
หมวดที่ 2: ระเบียบขั้นตอนปฏิบัติการมาตรฐาน (Standard Operating Procedures: SOPs)		หมวดหมู่
GW-SOP-01	ขั้นตอนการบริหารความเสี่ยงทางเทคโนโลยีสารสนเทศ	บังคับใช้
GW-SOP-02	ขั้นตอนการประเมินและคัดเลือกผู้ให้บริการคลาวด์	บังคับใช้
GW-SOP-03	การบริหารจัดการทรัพย์สินทางปัญญาและลิขสิทธิ์ซอฟต์แวร์	บังคับใช้
GW-SOP-04	การจัดการทรัพย์สินสารสนเทศและล้างข้อมูลถาวร	บังคับใช้
GW-SOP-05	การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ (IAM)	บังคับใช้
GW-SOP-06	การแบ่งระดับชั้นของข้อมูลและการเข้ารหัส	บังคับใช้
GW-SOP-07	การใช้งานอุปกรณ์เคลื่อนที่และสื่อบันทึกข้อมูล	บังคับใช้
GW-SOP-08	การบันทึก จัดเก็บหลักฐาน และติดตามตรวจสอบ (Audit Log)	บังคับใช้
GW-SOP-09	การบริหารการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ (Change)	บังคับใช้
GW-SOP-10	การพัฒนาระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย (Secure SDLC)	บังคับใช้
GW-SOP-11	การสำรองข้อมูลและการทดสอบกู้คืน (3-2-1 Backup & Restore)	บังคับใช้
GW-SOP-12	แผนรับมือเหตุการณ์ฉุกเฉินและกู้คืนระบบจากภัยพิบัติ (IT DRP)	บังคับใช้
GW-SOP-13	การบริหารจัดการผู้ให้บริการภายนอกด้านไอที (IT Outsourcing)	บังคับใช้
GW-SOP-14	การจัดการเหตุการณ์ไม่พึงประสงค์และรายงานภัยไซเบอร์ (24h SEC)	บังคับใช้

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 3 / 107
--	--	--

GW-SOP-15	การควบคุมการเข้าถึงห้องแม่ข่ายทางกายภาพ (Server Room)	บังคับใช้
GW-BCP-02	แผนความต่อเนื่องทางธุรกิจและการประเมินผลกระทบ (BCP & BIA)	บังคับใช้
หมวดที่ 3: สถาปัตยกรรมเทคนิคและทะเบียนคุม (Technical Specifications & Registers)		หมวดหมู่
GW-TEC-01	ผังแปลนและการจัดวางอุปกรณ์ห้องแม่ข่าย 42U วัน แบงค็อก	บังคับใช้
GW-TEC-02	ตารางมาตรฐานนโยบายความปลอดภัย Active Directory (GPO Matrix)	บังคับใช้
GW-TEC-03	ข้อกำหนดระบบสำรองข้อมูลคลาวด์และการแจ้งเตือนอัตโนมัติ	บังคับใช้
GW-TEC-04	เมทริกซ์สิทธิ์การใช้งานระบบงานหลักกองทุน (Bonanza RBAC Matrix)	บังคับใช้
GW-TEC-05	ข้อกำหนดรูปแบบ Audit Trail และการบันทึกประวัติธุรกรรมระบบกองทุน	บังคับใช้
GW-TEC-06	ทะเบียนคุมทรัพย์สินอุปกรณ์เทคโนโลยีสารสนเทศหลัก (Asset Register)	บังคับใช้
GW-TEC-07	ผังโครงสร้างเครือข่ายความมั่นคงปลอดภัยและการแยก VLAN (8 VLANs)	บังคับใช้

[GW-ETH-01] กฎระเบียบและจริยธรรมในการทำงานสำหรับฝ่ายไอที

รหัสเอกสาร	GW-ETH-01	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาสิทธิ์ ก้านจักร IT Specialist	นายโสธชา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณศลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด ดำเนินธุรกิจการจัดการกองทุนส่วนบุคคล (Private Fund Management)

ซึ่งต้องอาศัยความไว้วางใจจากผู้ลงทุน ข้อมูลทางการเงิน ความลับของพอร์ตการลงทุน

และความมั่นคงปลอดภัยของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศเป็นหัวใจสำคัญ เอกสารระเบียบฉบับนี้กำหนดขึ้นเพื่อ:

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 4 / 107
--	--	--

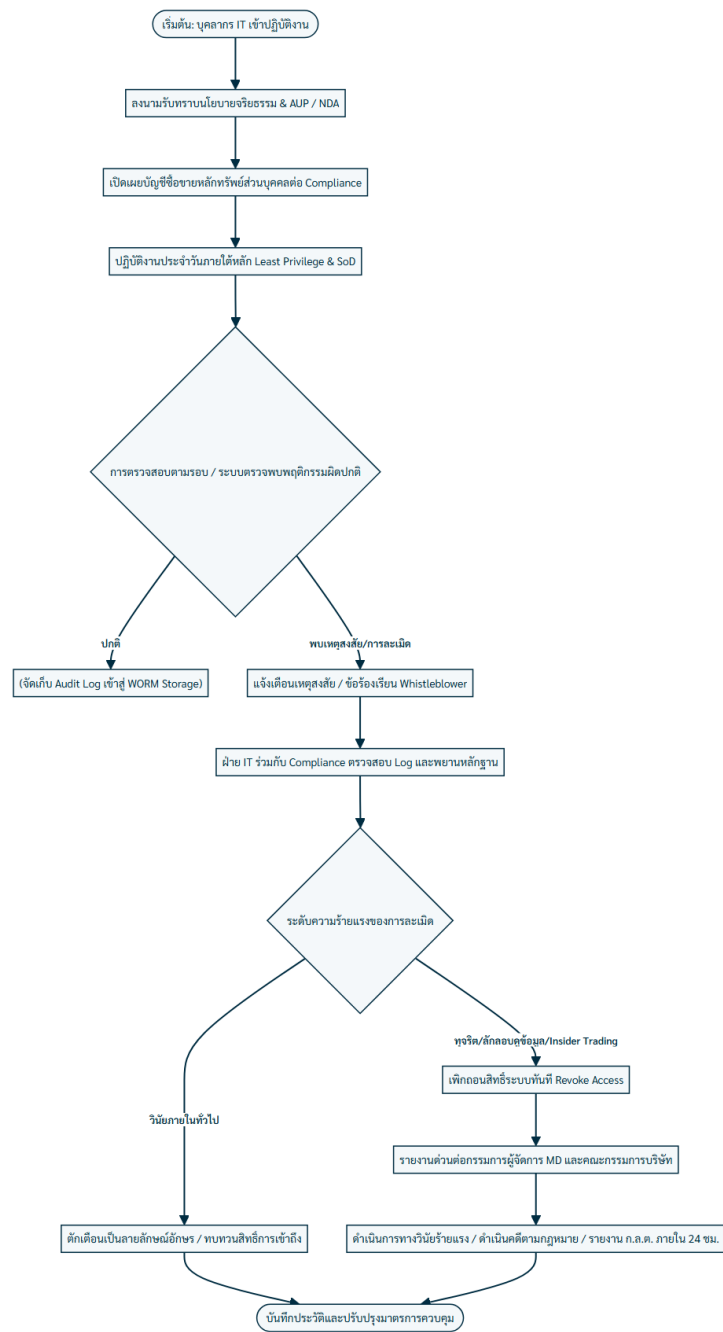
- กำหนดกรอบความประพฤติ จรรยาบรรณวิชาชีพ และมาตรฐานการปฏิบัติงานของบุคลากรฝ่าย IT ทุกคน
- ป้องกันความขัดแย้งทางผลประโยชน์ (Conflict of Interest) และการแสวงหาประโยชน์โดยมิชอบจากสิทธิ์การเข้าถึงข้อมูลระบบ (Privileged Access)
- ป้องกันการล่วงรู้หรือการใช้ประโยชน์จากข้อมูลภายใน (Insider Information) ในการซื้อขายหลักทรัพย์
- กำหนดแนวทางปฏิบัติที่สอดคล้องกับพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์, ประกาศสำนักงาน ก.ล.ต. (สธ. 38/2565 และ สธ. 33/2567), พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

2. ขอบเขตการบังคับใช้ (Scope)

ระเบียบจรรยาบรรณนี้มีผลบังคับใช้กับ:

- บุคลากรฝ่ายเทคโนโลยีสารสนเทศทุกคน ทั้งพนักงานประจำ พนักงานสัญญาจ้าง และผู้ฝึกงาน
- ผู้ดูแลระบบ (System Administrator, Network Administrator, Database Administrator)
- ที่ปรึกษาภายนอก (IT Consultants) และคู่ค้าผู้ให้บริการด้าน IT (IT Vendors / Outsourcers) ที่ได้รับสิทธิ์เข้าถึงระบบ เครือข่าย หรือห้องแม่ข่ายคอมพิวเตอร์ (Server Room) ของบริษัท

3. ผังกระบวนการกำกับดูแลจริยธรรมและการรายงานเหตุละเมิด (Ethical Oversight & Escalation Flow)



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-ETH-01 กฎระเบียบและจริยธรรมในการทำงานสำหรับฝ่ายไอที

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 6 / 107
--	---	--

4. หลักจริยธรรมและข้อพึงปฏิบัติ 7 ประการ (Core Ethical Principles)

4.1 การรักษาความลับของข้อมูลลูกค้าและพอร์ตการลงทุน (Confidentiality & Non-Disclosure)

- บุคลากร IT ต้องถือว่าข้อมูลพอร์ตการลงทุน ยอดเงินลงทุน กลยุทธ์การจัดพอร์ต คำสั่งซื้อขาย และข้อมูลส่วนบุคคลของลูกค้าทั้งหมดเป็น **"ข้อมูลความลับสูงสุด (Strictly Confidential)"**
- ห้ามเปิดเผย คัดลอก ส่งต่อ นำออกจากระบบ หรือถ่ายภาพหน้าจอข้อมูลดังกล่าวไปให้บุคคลภายนอก หรือพนักงานที่ไม่เกี่ยวข้องโดยเด็ดขาด
- ต้องลงนามในสัญญาการรักษาความลับ (Non-Disclosure Agreement: NDA) และข้อตกลงการใช้งานเทคโนโลยีสารสนเทศที่ยอมรับได้ (Acceptable Use Policy: AUP) ก่อนเริ่มงาน

4.2 การป้องกันการรั่วไหลข้อมูลภายในเพื่อการซื้อขายหลักทรัพย์ (Insider Trading Prevention)

- บุคลากรฝ่าย IT มีสิทธิ์เข้าถึงระบบจัดการกองทุนหลัก (ระบบ Bonanza Investment), ระบบฐานข้อมูล และรายงานคำสั่งซื้อขาย ซึ่งอาจทำให้ล่วงรู้ข้อมูลคำสั่งซื้อขายของพอร์ตลูกค้า (Front-Running Risk)
- ข้อห้ามเด็ดขาด:** ห้ามนำข้อมูลคำสั่งซื้อขายหรือสถานะพอร์ตการลงทุนของกองทุนไปใช้ในการซื้อขายหลักทรัพย์เพื่อประโยชน์ส่วนตน ครอบครัว หรือบุคคลใกล้ชิด
- พนักงาน IT ทุกคนต้องเปิดเผยบัญชีซื้อขายหลักทรัพย์ส่วนบุคคล และต้องได้รับอนุมัติจากฝ่ายกำกับดูแลการปฏิบัติงาน (Compliance) ก่อนทำการซื้อขายหลักทรัพย์ตามระเบียบ Employee Trading Policy ของบริษัท

4.3 การใช้สิทธิ์ผู้ดูแลระบบอย่างเคร่งครัด (Privileged Access Integrity)

- บุคลากร IT ที่ถือบัญชีสิทธิ์สูง (Administrative / Root Accounts) ต้องใช้สิทธิ์เพื่อการปฏิบัติหน้าที่ที่ได้รับมอบหมายเท่านั้น
- ห้ามใช้สิทธิ์แอดมินในการเข้าใช้อ่านอีเมล แชท หรือไฟล์ส่วนบุคคลของพนักงานท่านอื่น เว้นแต่จะได้รับคำสั่งเป็นลายลักษณ์อักษรจากกรรมการผู้จัดการ (MD) เพื่อประโยชน์ในการตรวจสอบทุจริต
- ต้องเปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ทุกครั้ง และต้องยอมรับให้ระบบบันทึก Session Logging และ Activity Audit Trail แบบเรียลไทม์

4.4 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties: SoD)

- บุคลากรฝ่าย IT จะต้องไม่มีส่วนเกี่ยวข้องกับการตัดสินใจลงทุน การส่งคำสั่งซื้อขายหลักทรัพย์ (Trader Function) หรือการตรวจรับเงิน/ชำระราคา (Settlement Function)
- การปฏิบัติงานด้าน IT ต้องมีการควบคุมแบบ Maker-Checker ในงานสำคัญ เช่น การสร้างบัญชีผู้ใช้งานระดับ Admin, การแก้ไขโครงสร้าง Database ระบบ Bonanza, และการแก้ไข Firewall Policy

4.5 การเคารพทรัพย์สินทางปัญญาและลิขสิทธิ์ซอฟต์แวร์ (Intellectual Property Compliance)

- บุคลากร IT ต้องติดตั้งและใช้งานเฉพาะซอฟต์แวร์ที่ได้รับอนุญาตและมีลิขสิทธิ์ถูกต้องตามกฎหมายของบริษัทเท่านั้น
- ห้ามนำโปรแกรมละเมิดลิขสิทธิ์ ซอฟต์แวร์ Crack ซอฟต์แวร์ดาวน์โหลดแบบ P2P/BitTorrent หรือโปรแกรมที่ไม่ผ่านการตรวจสอบด้านความปลอดภัยมาติดตั้งบนอุปกรณ์ของบริษัท

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 7 / 107
--	---	--

- ซอร์สโค้ด สคริปต์ ฐานข้อมูล ผังระบบ และเอกสารทั้งหมดที่บุคลากร IT พัฒนาขึ้นขณะปฏิบัติงานให้แก่บริษัท ถือเป็นทรัพย์สินทางปัญญาของบริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด แต่เพียงผู้เดียว

4.6 ความซื่อสัตย์และการไม่รับอามิสสินจ้าง (Anti-Bribery & Corruption)

- ห้ามบุคลากร IT เรียก รับ หรือยินยอมจะรับเงิน ของขวัญ ทริพท่องเที่ยว หรือผลประโยชน์อื่นใดจากผู้ขายอุปกรณ์ IT ผู้ให้บริการคลาวด์ หรือผู้รับเหมา ที่อาจส่งผลกระทบต่อความเที่ยงธรรมในการคัดเลือกคู่ค้า (Vendor Procurement)
- การจัดซื้อจัดจ้างด้าน IT ทุกโครงการต้องปฏิบัติตามขั้นตอน Bidding Comparison Matrix อย่างโปร่งใส ตรวจสอบได้

4.7 การแจ้งเหตุการณ์ผิดปกติและความร่วมมือในการตรวจสอบ (Incident Reporting & Transparency)

- หากบุคลากร IT พบเห็นช่องโหว่ความปลอดภัย การพยายามบุกรุก พฤติกรรมทุจริต หรือข้อผิดพลาดในระบบ ต้องรายงานต่อผู้บังคับบัญชาและ Compliance ทันที โดยห้ามปกปิดข้อเท็จจริง
- ต้องให้ความร่วมมืออย่างเต็มที่ต่อผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก (เช่น ผู้ตรวจสอบอิสระภายนอก) และเจ้าพนักงานของสำนักงาน ก.ล.ต.

5. บทลงโทษทางวินัยและผลกระทบทางกฎหมาย (Disciplinary & Legal Actions)

การฝ่าฝืนหรือไม่ปฏิบัติตามกฎระเบียบและจรรยาบรรณฉบับนี้ จะถูกพิจารณาบทลงโทษตามระดับความร้ายแรง:

1. การตักเตือนด้วยวาจาและบันทึกประวัติ (สำหรับการกระทำผิดเล็กน้อยที่ไม่ได้เกิดจากเจตนาทุจริต)
2. การตักเตือนเป็นลายลักษณ์อักษรและสั่งพักงาน
3. การเลิกจ้างทันทีโดยไม่จ่ายค่าชดเชย (สำหรับการทุจริต การนำข้อมูลความลับลูกค้าไปเผยแพร่ หรือการใช้สิทธิ์แอดมินเพื่อแสวงหาผลประโยชน์ส่วนตน)
4. การดำเนินคดีแพ่งและอาญา: บริษัทจะดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์, และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) จนถึงที่สุด

6. เอกสารอ้างอิงและแบบฟอร์มที่เกี่ยวข้อง (Related Forms & Policies)

1. GW-POL-01: นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
2. GW-POL-02: นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ
3. GW-TMP-01: สัญญาข้อตกลงการใช้งานระบบคอมพิวเตอร์ที่ยอมรับได้ (Acceptable Use Policy: AUP)
4. GW-TMP-02: สัญญารักษาความลับทางการค้าและข้อมูลสารสนเทศ (Non-Disclosure Agreement: NDA)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 8 / 107
--	---	--

[GW-POL-01] นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(Information Security Policy)

รหัสเอกสาร	GW-POL-01	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งลิขิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกฉัตร ภูมชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

นโยบายฉบับนี้กำหนดขึ้นเพื่อเป็นกรอบแม่บทในการบริหารจัดการและกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- ปกป้องความลับ (Confidentiality), ความถูกต้องครบถ้วนสมบูรณ์ (Integrity), และความพร้อมใช้งาน (Availability) ของข้อมูลทรัพย์สินสารสนเทศ พอร์ตการลงทุน และระบบจัดการกองทุนส่วนบุคคล (Private Fund Management)
- บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ให้อยู่ในระดับที่บริษัทสามารถยอมรับได้ (Risk Appetite)
- ปฏิบัติตามกฎหมายและกฎเกณฑ์ของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ตามประกาศที่ สธ. 38/2565, สธ. 33/2567 และประกาศแนวปฏิบัติที่ นป. 6/2567, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- สร้างความเชื่อมั่นแก่ผู้ลงทุน พันธมิตรทางธุรกิจ และผู้มีส่วนได้เสียทุกฝ่ายต่อการดำเนินงานของบริษัท

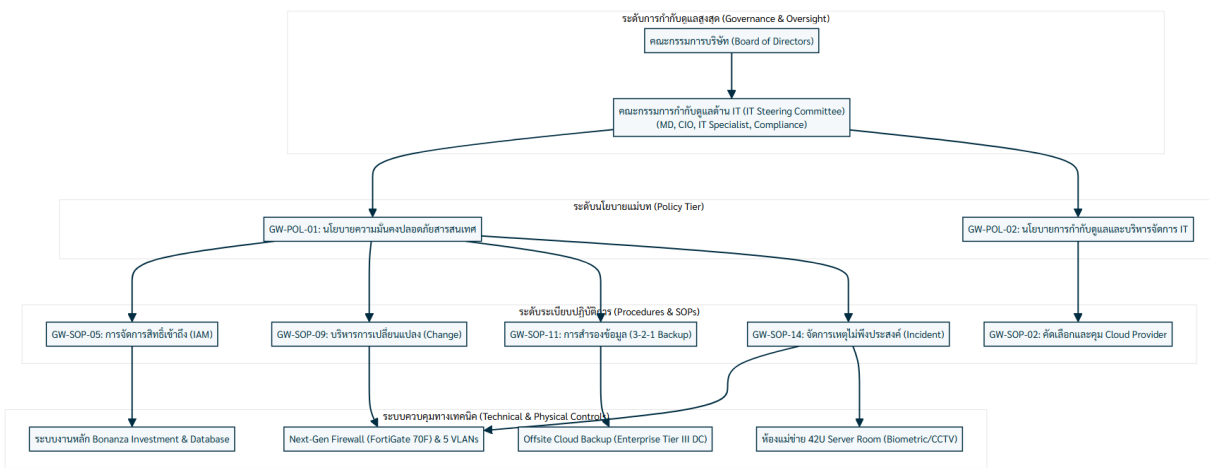
2. ขอบเขตการบังคับใช้ (Scope)

นโยบายฉบับนี้มีผลบังคับใช้ครอบคลุม:

- บุคลากร: กรรมการบริษัท ผู้บริหาร พนักงานประจำ พนักงานสัญญาจ้าง ที่ปรึกษา และบุคคลภายนอก (Contractors/Vendors) ทุกคนที่เข้าถึงหรือใช้งานระบบของบริษัท

2. ระบบและโครงสร้างพื้นฐาน: ระบบคอมพิวเตอร์แม่ข่าย (Server Room 42U ณ วัน แบงค็อก ทาวเวอร์ 4 ชั้น 38), ระบบเครือข่ายสำนักงาน (FortiGate Firewall, UniFi Switches), ระบบคลาวด์ (Offsite Hybrid Cloud Backup), เครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์สื่อสารทั้งหมด
3. ข้อมูลสารสนเทศ: ข้อมูลพอร์ทลูกค้า, ข้อมูลธุรกรรมการซื้อขาย, ข้อมูลการวิเคราะห์การลงทุน, ข้อมูลการเงิน และข้อมูลส่วนบุคคลทั้งหมดไม่ว่าจะจัดเก็บในรูปแบบดิจิทัลหรือเอกสารกระดาษ

3. สถาปัตยกรรมการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ (Information Security Architecture)



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-POL-01
นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 10 / 107
--	---	---

4. เสาหลักด้านความมั่นคงปลอดภัยสารสนเทศ (Core Security Principles)

4.1 การรักษาความลับ (Confidentiality)

- การเข้าถึงข้อมูลของบริษัทจะอนุญาตเฉพาะผู้ที่มีความจำเป็นในการปฏิบัติงานเท่านั้น (Need-to-Know Basis)
- ต้องมีการจำแนกชั้นความลับของข้อมูล (Data Classification) ออกเป็น: ข้อมูลลับสูงสุด (Strictly Confidential), ข้อมูลลับ (Confidential), ข้อมูลใช้ภายใน (Internal Use), และข้อมูลสาธารณะ (Public)
- ข้อมูลที่มีความสำคัญสูงต้องได้รับการเข้ารหัส (Encryption) ทั้งในขณะจัดเก็บ (Data at Rest) ด้วยอัลกอริทึม AES-256 และในขณะรับส่ง (Data in Transit) ด้วยโปรโตคอล TLS 1.3

4.2 ความถูกต้องครบถ้วนสมบูรณ์ (Integrity)

- ข้อมูลธุรกรรมพอร์ตการลงทุนและคำสั่งซื้อขายต้องได้รับการปกป้องจากการแก้ไข เปลี่ยนแปลง หรือลบทิ้งโดยมิชอบ
- ระบบงานหลักต้องใช้การควบคุมแบบ Maker-Checker ในขั้นตอนการกรดยอดและการเปลี่ยนแปลงสถานะพอร์ต
- มีการคำนวณค่าแฮช (Cryptographic Hash) หรือใช้ฟังก์ชัน WORM (Write Once, Read Many) สำหรับข้อมูล Audit Log และไฟล์สำรองข้อมูลเพื่อป้องกันการดัดแปลงย้อนหลัง

4.3 ความพร้อมใช้งาน (Availability)

- ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญต่อธุรกิจกองทุน (Mission-Critical Systems) เช่น ระบบ Bonanza Investment และระบบเครือข่ายหลัก ต้องมีค่าความพร้อมใช้งาน (Availability SLA) ไม่ต่ำกว่า 99.9% ในเวลาทำการ
- โครงสร้างพื้นฐานระบบไฟฟ้า ณ อาคาร วัน แบงค็อก ต้องมีระบบไฟฟ้าสำรองฉุกเฉิน True Online UPS และการเชื่อมต่ออินเทอร์เน็ตแบบ Dual ISP Active-Backup
- มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) และแผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan: DRP) ที่มีการซักซ้อมอย่างน้อยปีละ 1 ครั้ง

5. นโยบายการควบคุมเชิงเทคนิคและกายภาพ (Technical & Physical Security Policies)

5.1 การควบคุมการเข้าถึงระบบและอัตลักษณ์ (Identity & Access Control)

- บัญชีผู้ใช้งานต้องเป็นรายบุคคล (Individual Accounts) ห้ามใช้บัญชีร่วม (Generic/Shared Accounts)
- การกำหนดสิทธิ์ต้องยึดหลักสิทธิ์เท่าที่จำเป็น (Least Privilege) ตามตำแหน่งงาน (Role-Based Access Control: RBAC)
- การเข้าถึงระบบจากระยะไกล (Remote Access) หรือการใช้สิทธิ์ระดับผู้ดูแลระบบ (Privileged Account) ต้องผ่านการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ทุกครั้ง
- นโยบายรหัสผ่านต้องมีความซับซ้อนตามมาตรฐาน และระบบต้องล็อกบัญชีอัตโนมัติหากใส่รหัสผ่านผิดเกิน 5 ครั้งติดต่อกัน

5.2 ความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security & Segmentation)

- ระบบเครือข่ายสำนักงานใหญ่ต้องได้รับการปกป้องด้วย Next-Generation Firewall (FortiGate) ที่เปิดใช้งานระบบ Intrusion Prevention System (IPS), Anti-Malware และ Web Filtering

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 11 / 107
--	--	---

- ต้องแบ่งแยกเครือข่ายออกเป็น VLAN อิสระ 5 วงอย่างเด็ดขาด:
 1. VLAN 10 (Management): อุปกรณ์ควบคุมเครือข่ายและสวิตช์
 2. VLAN 20 (Corporate): เครื่องคอมพิวเตอร์พนักงานประจำ
 3. VLAN 30 (Core Fund System): เซิร์ฟเวอร์ระบบจัดการกองทุน Bonanza
 4. VLAN 40 (CCTV & Facilities): กล้องวงจรปิดและระบบควบคุมอาคาร
 5. VLAN 50 (Guest Wi-Fi): เครือข่ายผู้มาติดต่อ ซึ่งถูกตัดขาดจากระบบภายใน 100%

5.3 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical Security)

- ห้องแม่ข่าย (Server Room 42U) ณ ชั้น 38 อาคาร วัน แบงค็อก เป็นพื้นที่ควบคุมระดับสูงสุด
- การเข้า-ออกต้องผ่านระบบสแกนชีวมิติ (Biometric Facial/Fingerprint Scan) หรือคีย์การ์ดเฉพาะผู้ได้รับอนุมัติ
- มีกล้องวงจรปิด (CCTV) บันทึกภาพตลอด 24 ชั่วโมง และจัดเก็บประวัติภาพบันทึกไม่น้อยกว่า 90 วัน
- มีระบบควบคุมอุณหภูมิ (20-22°C), ระบบตรวจจับควันไฟ และรายการอุปกรณ์ดับเพลิงอัตโนมัติติดเพดาน SUNSAFETY Clean Agent (NON CFC) 10 ปอนด์ (การติดตั้งและเอกสารผู้ผลิตรอยืนยัน)

5.4 การสำรองข้อมูลและการกู้คืน (Backup & Data Protection)

- ยึดถือกลยุทธ์การสำรองข้อมูลแบบ 3-2-1 Backup Strategy: เก็บข้อมูลอย่างน้อย 3 ชุด ในสื่อบันทึก 2 ประเภท โดย 1 ชุดต้องถูกส่งไปเก็บไว้ที่ศูนย์ข้อมูลสำรองภายนอก (Offsite Cloud Backup)
- ข้อมูลสำรองบนระบบคลาวด์ต้องตั้งอยู่ในศูนย์ข้อมูลมาตรฐาน Tier III ในประเทศไทย และได้รับการเข้ารหัส AES-256
- กำหนดเป้าหมายเวลาการกู้ระบบ (RTO) ไม่เกิน 4 ชั่วโมง และเป้าหมายการสูญเสียข้อมูล (RPO) ไม่เกิน 24 ชั่วโมงสำหรับระบบงานสำคัญ

5.5 การจัดเก็บและตรวจสอบบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Logging & Monitoring)

- ต้องเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ (Log Files) และประวัติการทำธุรกรรม (Audit Trails) ของระบบงานหลัก, ไฟร์วอลล์, และ Active Directory ย้อนหลังไม่น้อยกว่า 90 วันตาม พ.ร.บ.คอมพิวเตอร์ และเกณฑ์ ก.ล.ด.
- มีการซิงโครไนซ์เวลาของระบบทั้งหมดด้วยโปรโตคอล Network Time Protocol (NTP) จากแหล่งอ้างอิงเวลามาตรฐานสากลที่น่าเชื่อถือ
- บันทึก Log ต้องจัดเก็บในรูปแบบที่ไม่สามารถแก้ไขหรือลบทำลายได้ (Tamper-Proof / Read-Only Storage)

6. การตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Incident Response)

- หากเกิดเหตุการณ์บุกรุก ข้อมูลรั่วไหล หรือการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ ต้องปฏิบัติตามระเบียบ GW-SOP-14: Cyber Incident Management ทันที
- กรณีที่เหตุการณ์มีระดับความรุนแรงสูง (High / Critical) ซึ่งส่งผลกระทบต่อระบบงานสำคัญหรือข้อมูลลูกค้า บริษัทมีหน้าที่ต้องรายงานต่อสำนักงาน ก.ล.ต. ภายใน 24 ชั่วโมงนับแต่วันที่ตรวจพบเหตุการณ์ตามเกณฑ์ประกาศ สธ. 38/2565

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้า: 12 / 107
--	---	--

7. การบริหารจัดการผู้ให้บริการภายนอกและคลาวด์ (Third-Party & Cloud Oversight)

- การว่าจ้างผู้ให้บริการภายนอก (Outsourcers) หรือผู้ให้บริการคลาวด์ ต้องผ่านกระบวนการคัดกรอง Due Diligence และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยตามระเบียบ GW-SOP-02
- สัญญาว่าจ้างต้องระบุข้อกำหนดด้านการรักษาความลับ (NDA), สิทธิของบริษัทและ ก.ล.ต. ในการเข้าตรวจสอบ (Right to Audit), และข้อตกลงระดับการให้บริการ (SLA) อย่างเคร่งครัด

8. การทบทวนและการปรับปรุงนโยบาย (Policy Review & Continuous Improvement)

นโยบายฉบับนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้งโดยฝ่ายเทคโนโลยีสารสนเทศร่วมกับฝ่ายกำกับดูแลการปฏิบัติงาน และต้องนำเสนอขออนุมัติจากคณะกรรมการบริษัท (Board of Directors) หากมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในโครงสร้างพื้นฐานเทคโนโลยี หรือข้อกำหนดทางกฎหมาย

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 13 / 107
--	---	---

[GW-POL-02] นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ

รหัสเอกสาร	GW-POL-02	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุลชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

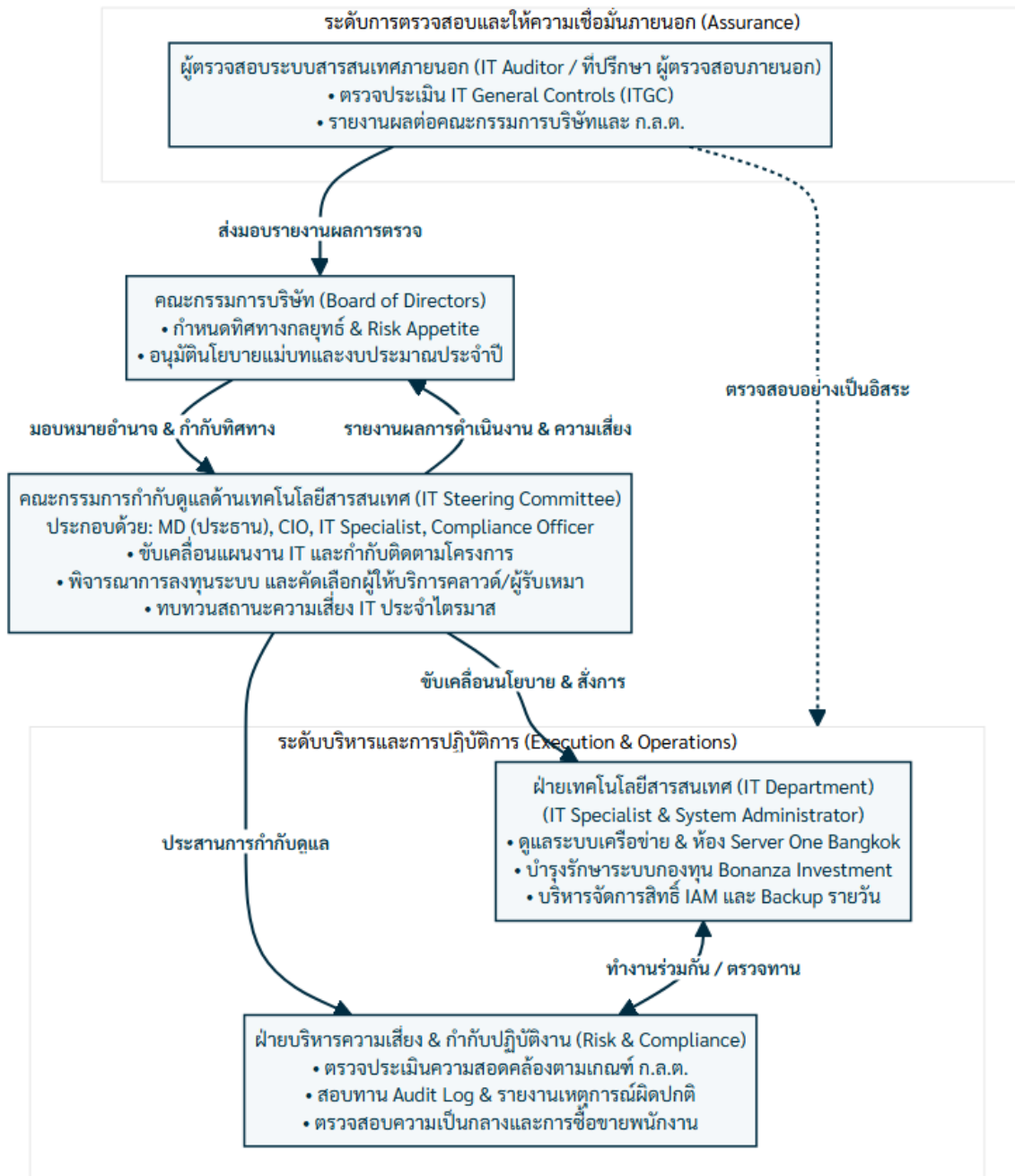
นโยบายฉบับนี้กำหนดขึ้นเพื่อวางกรอบโครงสร้างการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance Framework) และแนวทางการบริหารจัดการทรัพยากรสารสนเทศของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด ให้บรรลุเป้าหมายดังต่อไปนี้:

- ขับเคลื่อนและสนับสนุนเป้าหมายเชิงกลยุทธ์ทางธุรกิจการจัดการกองทุนส่วนบุคคล (Business & IT Strategic Alignment)
- สร้างความมั่นใจว่าการลงทุนด้านเทคโนโลยีสารสนเทศและการจัดซื้อจัดจ้างเกิดประโยชน์สูงสุด มีความคุ้มค่า และบริหารต้นทุนได้อย่างมีประสิทธิภาพ (Value Delivery & Resource Optimization)
- กำหนดสายการบังคับบัญชา อำนาจหน้าที่ความรับผิดชอบ และการตัดสินใจด้าน IT ให้โปร่งใส ตรวจสอบได้ (Accountability & Transparency)
- ควบคุมความเสี่ยงด้าน IT ให้อยู่ภายใต้กรอบความเสี่ยงที่คณะกรรมการบริษัทยอมรับได้ (Risk Governance) สอดคล้องกับประกาศ ก.ล.ต. สช. 38/2565 และ สช. 33/2567

2. ขอบเขตการบังคับใช้ (Scope)

นโยบายฉบับนี้มีผลบังคับใช้กับการตัดสินใจเชิงกลยุทธ์ โครงการพัฒนาเทคโนโลยีสารสนเทศ การจัดสรรงบประมาณ การบริหารความเสี่ยง การควบคุมการปฏิบัติการ และการตรวจสอบระบบสารสนเทศทั้งหมดของบริษัท

3. ผังโครงสร้างธรรมาภิบาลและการตัดสินใจด้าน IT (IT Governance & Decision Framework)



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-POL-02

นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 15 / 107
--	--	---

4. โครงสร้างองค์กรและบทบาทหน้าที่ความรับผิดชอบ (Roles & Responsibilities)

4.1 คณะกรรมการบริษัท (Board of Directors: BoD)

- รับผิดชอบสูงสุดในการกำกับดูแลให้บริษัทมีระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัยและมีประสิทธิภาพ
- พิจารณานุมัตินโยบายแม่บทด้าน IT, แผนกลยุทธ์เทคโนโลยีสารสนเทศระยะ 3 ปี, และระดับความเสี่ยงด้าน IT ที่ยอมรับได้ (Risk Appetite)
- จัดสรรทรัพยากรและงบประมาณด้านความมั่นคงปลอดภัยไซเบอร์อย่างเพียงพอ (Cyber Security Budget)
- รับทราบรายงานสถานะความเสี่ยง รายงานผลการตรวจสอบระบบ และรายงานเหตุการณ์ภัยคุกคามที่สำคัญ

4.2 คณะกรรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Steering Committee: ITSC)

จัดตั้งขึ้นโดยประกอบด้วย กรรมการผู้จัดการ (MD) เป็นประธาน, ประธานเจ้าหน้าที่ฝ่ายการลงทุน (CIO), ผู้เชี่ยวชาญด้าน IT (IT Specialist), และเจ้าหน้าที่กำกับดูแลการปฏิบัติงาน (Compliance Officer) โดยมีการประชุมอย่างน้อยไตรมาสละ 1 ครั้ง มีหน้าที่:

- กำหนดทิศทางและแผนปฏิบัติการด้าน IT ให้สอดคล้องกับกลยุทธ์ของส่วนบุคคล
- พิจารณาและกลั่นกรองโครงการจัดซื้อระบบ โครงการสร้างห้องเซิร์ฟเวอร์ และการคัดเลือกผู้ให้บริการคลาวด์ (เช่น INET หรือ True IDC)
- ติดตามผลการดำเนินงานของโครงการ IT และการปฏิบัติตามเกณฑ์ SLA ของผู้รับเหมา
- ทบทวนแผนความต่อเนื่องทางธุรกิจ (BCP) และแผนกู้คืนระบบจากภัยพิบัติ (DRP) ประจำปี
- กำกับดูแลและติดตามการแก้ไขข้อบกพร่องที่พบจากรายงานของผู้ตรวจสอบภายนอก

4.3 ผู้เชี่ยวชาญด้าน IT และทีมปฏิบัติการ (IT Specialist & Operations)

- รับผิดชอบการบริหารจัดการและบำรุงรักษาระบบโครงสร้างพื้นฐาน ฮาร์ดแวร์ เครือข่าย และระบบจัดการกองทุน Bonanza ให้มีความพร้อมใช้งาน 99.9%
- ดำเนินการตามระเบียบขั้นตอนปฏิบัติงาน (SOPs) ทั้ง 15 ฉบับอย่างเคร่งครัด
- เผื่อระวังภัยคุกคามทางไซเบอร์ ควบคุมการเข้าถึงระบบ และทดสอบการสำรองข้อมูล (Backup Verification)
- จัดทำรายงานสรุปประสิทธิภาพระบบและสถานะความเสี่ยงเสนอต่อคณะกรรมการกำกับดูแลด้าน IT

4.4 ฝ่ายกำกับดูแลการปฏิบัติงานและบริหารความเสี่ยง (Compliance & Risk Management)

- ติดตามประกาศ กฎระเบียบ และข้อสั่งการใหม่ของสำนักงาน ก.ล.ต. และหน่วยงานกำกับดูแล เพื่อนำมาปรับปรุงนโยบาย IT
- ร่วมตรวจสอบการกำหนดสิทธิ์ผู้ใช้งาน (Access Rights Review) และบันทึกประวัติการใช้งาน (Audit Trail)
- ทำหน้าที่เป็นผู้ประสานงานหลักในการรายงานเหตุการณ์ผิดปกติด้านความปลอดภัยต่อสำนักงาน ก.ล.ต. ภายใน 24 ชั่วโมง

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 16 / 107
--	---	---

5. การวางแผนกลยุทธ์และการจัดสรรงบประมาณด้าน IT (Strategy & Budgeting)

- แผนกลยุทธ์ IT (IT Strategic Plan):** ฝ่าย IT ต้องจัดทำแผนพัฒนาระบบเทคโนโลยีสารสนเทศระยะ 1-3 ปี
เสนอต่อคณะกรรมการบริษัท โดยต้องครอบคลุมการพัฒนาระบบ Bonanza, การเสริมความแข็งแกร่งของระบบไซเบอร์
และการปรับปรุงโครงสร้างห้องแม่ข่าย ณ One Bangkok
- งบประมาณความมั่นคงปลอดภัย (Cyber Security Budget):**
บริษัทต้องจัดสรรงบประมาณประจำปีเฉพาะสำหรับความมั่นคงปลอดภัยไซเบอร์ (การต่ออายุ License FortiGuard, การสำรองข้อมูล
Cloud, การตรวจประเมินช่องโหว่ Vulnerability Assessment, และการซักซ้อม DRP Drill) อย่างเหมาะสม
- การควบคุมต้นทุน (Cost Optimization):** การจัดซื้ออุปกรณ์หรือระบบมูลค่าเกินเกณฑ์ที่กำหนด
ต้องผ่านการเปรียบเทียบข้อเสนออย่างน้อย 3 ราย (Vendor Bidding Comparison) ผ่านเกณฑ์การคัดเลือกที่โปร่งใส

6. การบริหารจัดการผลการดำเนินงานและการตรวจสอบ (Performance & Assurance)

- ดัชนีชี้วัดผลการดำเนินงาน (Key Performance Indicators: KPIs):**
 - อัตราความพร้อมใช้งานของระบบงานหลัก (System Uptime): ไม่น้อยกว่า 99.9% ในเวลาทำการ
 - อัตราความสำเร็จของการสำรองข้อมูล (Backup Success Rate): 100%
 - เวลาในการกู้คืนระบบสำคัญเมื่อเกิดเหตุขัดข้อง (RTO): ไม่เกิน 4 ชั่วโมง
 - การแก้ไขช่องโหว่ความปลอดภัยระดับร้ายแรง (Critical Patch Deployment): ภายใน 7 วันทำการ
- การตรวจสอบระบบสารสนเทศ (Independent IT Audit):**
 - บริษัทต้องจัดให้มีการตรวจสอบระบบเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระ (เช่น
ผู้ตรวจสอบอิสระภายนอก) อย่างน้อยปีละ 1 ครั้ง
 - รายงานผลการตรวจสอบและข้อเสนอแนะในการปรับปรุง (Management Letter) ต้องนำเสนอต่อคณะกรรมการบริษัทโดยตรง

7. เอกสารและระเบียบปฏิบัติที่เกี่ยวข้อง (Related Procedures)

- GW-POL-01: นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
- GW-SOP-01: ขั้นตอนการบริหารความเสี่ยงทางเทคโนโลยีสารสนเทศ
- GW-SOP-02: ขั้นตอนการประเมินและคัดเลือกผู้ให้บริการคลาวด์
- GW-SOP-09: ขั้นตอนการบริหารการเปลี่ยนแปลงระบบ (Change Management)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 17 / 107
--	---	---

[GW-BCP-01] นโยบายการบริหารความต่อเนื่องทางธุรกิจ (BCM Policy)

(Business Continuity Management Policy: BCM)

รหัสเอกสาร	GW-BCP-01	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายบริหารความเสี่ยงและฝ่ายไอที	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธชา ตั้งลิขิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

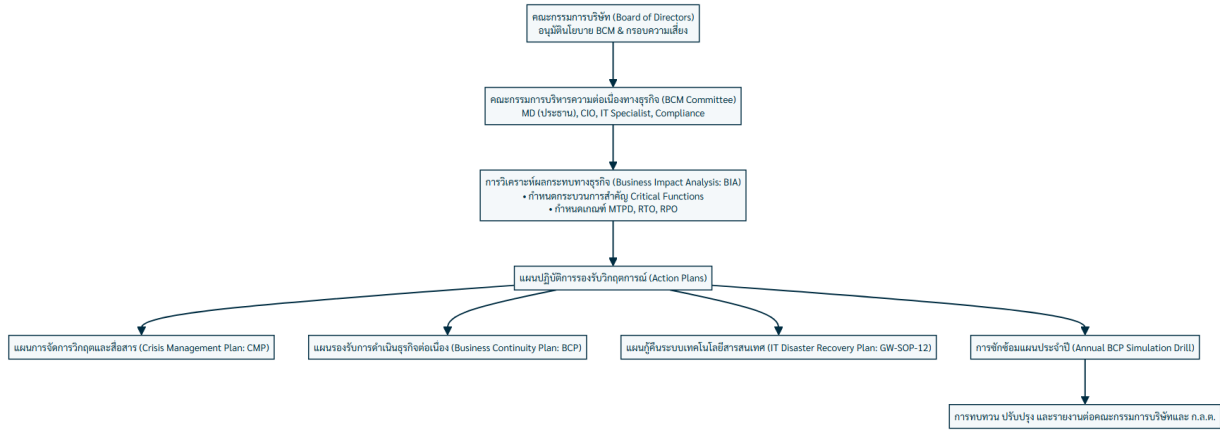
1. วัตถุประสงค์ (Objective)

นโยบายฉบับนี้กำหนดขึ้นเพื่อเป็นกรอบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- สร้างความมั่นใจว่าบริษัทสามารถดำเนินกระบวนการทางธุรกิจที่สำคัญยิ่งยวด (Critical Business Functions) ของการจัดการกองทุนส่วนบุคคลได้อย่างต่อเนื่องเมื่อเกิดวิกฤตการณ์ ภัยพิบัติ หรือเหตุการณ์ไม่คาดคิด
- ปกป้องชีวิตและความปลอดภัยของพนักงาน ทรัพย์สินของลูกค้า และชื่อเสียงองค์กร
- กำหนดให้มีการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) และการประเมินความเสี่ยงต่อความต่อเนื่องทางธุรกิจ (BCM Risk Assessment) อย่างสม่ำเสมอ
- ปฏิบัติตามประกาศ ก.ล.ต. สธ. 38/2565 และแนวปฏิบัติเรื่องการบริหารความต่อเนื่องทางธุรกิจของผู้ประกอบธุรกิจหลักทรัพย์

2. ขอบเขตและกลยุทธ์ความต่อเนื่อง (Scope & BCM Strategy)

ครอบคลุมทุกสายงานหลักของบริษัท ได้แก่: การบริหารการลงทุน (Portfolio Management), การส่งคำสั่งซื้อขาย (Trading Execution), การปฏิบัติการกองทุนและชำระราคา (Settlement & Operations), งานเทคโนโลยีสารสนเทศ (IT & Infrastructure), และงานกำกับดูแลการปฏิบัติงาน (Compliance & Risk)



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-BCP-01 นโยบายการบริหารความต่อเนื่องทางธุรกิจ (BCM Policy)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 19 / 107
---	--	--

3. เป้าหมายและเกณฑ์ความต่อเนื่องทางธุรกิจ (BCM Key Metrics)

- **Maximum Tolerable Period of Disruption (MTPD):**
ระยะเวลาหยุดชะงักสูงสุดที่ธุรกิจยอมรับได้ก่อนเกิดความเสียหายร้ายแรงต่อธุรกิจกองทุน กำหนดไว้ไม่เกิน **8 ชั่วโมง**
- **Recovery Time Objective (RTO):** ระยะเวลาเป้าหมายในการฟื้นฟูกระบวนการสำคัญกลับมาดำเนินการได้ กำหนดไว้ไม่เกิน **4 ชั่วโมง**
- **Recovery Point Objective (RPO):** ปริมาณข้อมูลธุรกรรมสูงสุดที่ยอมให้สูญหายได้ กำหนดไว้ไม่เกิน **24 ชั่วโมง** (หรือ 1 ชั่วโมงสำหรับคำสั่งซื้อขาย)

4. กลยุทธ์สถานที่ทำงานสำรองและระบบเทคโนโลยี (Alternative Worksite & Tech)

- 1. สถานที่ทำงานสำรอง (Alternative Site):** ในกรณีที่ไม่สามารถเข้าใช้อาคาร วัน แบงค็อก ทาวเวอร์ 4 ได้ ให้พนักงานกลุ่มสำคัญ (Key Personnel) ปฏิบัติงานผ่านระบบการทำงานระยะไกล (Work from Home / Remote Working) ที่ปลอดภัยผ่าน FortiGate SSL-VPN
- 2. ระบบสำรองบนคลาวด์ (Cloud Standby System):** ระบบจัดการกองทุน Bonanza และฐานข้อมูลลูกค้าสามารถเปิดใช้งานบนศูนย์ข้อมูลคลาวด์สำรอง (INET / True IDC) ได้ทันทีตามระเบียบ **GW-SOP-12 (IT DRP)**
- 3. การซักซ้อมแผน BCP (Annual BCP Exercise):** บริษัทต้องจัดให้มีการซักซ้อมแผน BCP แบบจำลองสถานการณ์จริง (Simulation Drill) อย่างน้อยปีละ 1 ครั้ง และรายงานผลต่อสำนักงาน ก.ล.ต.

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 20 / 107
--	---	---

[GW-SOP-01] ขั้นตอนการบริหารความเสี่ยงทางเทคโนโลยีสารสนเทศ

รหัสเอกสาร	GW-SOP-01	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาสิทธิ์ ก้านจักร IT Specialist	นายโสธรา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุลชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

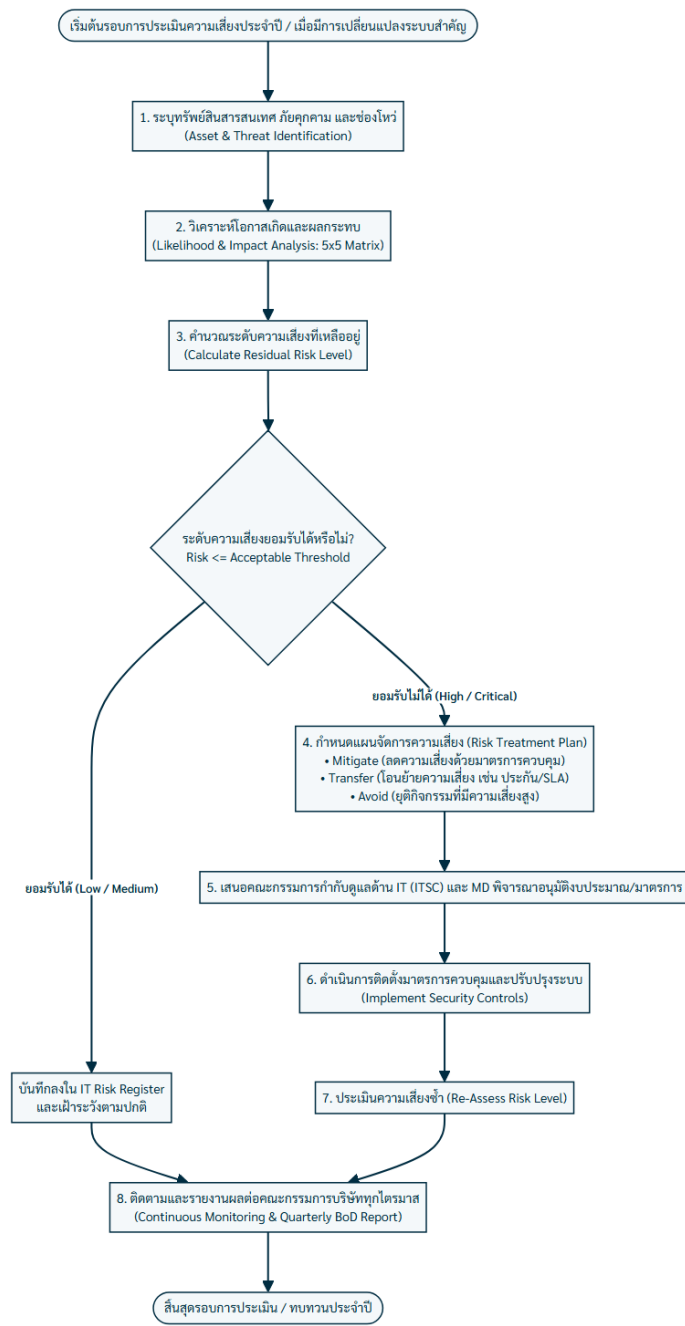
ระเบียบปฏิบัติงานฉบับนี้กำหนดขั้นตอนมาตรฐานในการระบุ ประเมิน จัดลำดับความสำคัญ จัดการ และติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- ป้องกันและลดผลกระทบจากภัยคุกคามไซเบอร์ ความผิดพลาดของระบบ และภัยพิบัติที่อาจทำให้ธุรกิจจัดการกองทุนส่วนบุคคลหยุดชะงัก
- ควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่ยอมรับได้ (Risk Appetite) ตามความเห็นชอบของคณะกรรมการบริษัท
- ปฏิบัติตามข้อกำหนดของสำนักงาน ก.ล.ต. ตามประกาศที่ สธ. 38/2565 และประกาศแนวปฏิบัติที่ นป. 6/2567 เรื่องการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมทรัพย์สินสารสนเทศ โครงสร้างพื้นฐานระบบเครือข่าย ระบบเซิร์ฟเวอร์ห้องแม่ข่าย (Server Room 42U วัน แบงค็อก ชั้น 38) ระบบจัดการกองทุนหลัก Bonanza Investment การเชื่อมต่อบริบทคลาวด์ภายนอก และกระบวนการปฏิบัติงานที่เกี่ยวข้องกับข้อมูลของบริษัททั้งหมด

3. ฟังก์กระบวนการบริหารความเสี่ยงด้าน IT (Operational Process Flow)



รูปภาพ: ฟังก์กระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-01 ขั้นตอนการบริหารความเสี่ยงทางเทคโนโลยีสารสนเทศ

4. ตารางความรับผิดชอบ (RACI Matrix)

กิจกรรม / ขั้นตอนการทำงาน	IT Specialist	CIO / Compliance	กรรมการผู้จัดการ (MD)	คณะกรรมการบริษัท (BoD)
1. รวบรวมรายการทรัพย์สินและระบุภัยคุกคาม	R / A	C	I	I
2. ประเมินความเสี่ยงด้วยเมทริกซ์ 5x5	R	A	I	I
3. จัดทำแผนจัดการความเสี่ยง (Risk Treatment Plan)	R	C	A	I
4. จัดสรรงบประมาณและอนุมัติมาตรการควบคุม	C	C	R / A	A
5. ดำเนินการปรับปรุงและติดตั้งระบบความปลอดภัย	R / A	C	I	I
6. รายงานสรุปสถานะความเสี่ยงประจำไตรมาส/ปี	R	C	C	A

(หมายเหตุ: R = Responsible ผู้ปฏิบัติงานหลัก, A = Accountable ผู้รับผิดชอบสูงสุด/ผู้อนุมัติ, C = Consulted ผู้ให้คำปรึกษา, I = Informed ผู้รับทราบรายงาน)

5. ขั้นตอนการปฏิบัติงานโดยละเอียด (Step-by-Step Procedure)

ขั้นตอนที่ 1: การระบุทรัพย์สิน ภัยคุกคาม และช่องโหว่ (Identification)

- สำรวจทรัพย์สิน (Asset Inventory):** IT Specialist ดึงข้อมูลจากทะเบียนทรัพย์สินสารสนเทศ (IT Asset Register) แบ่งเป็น ฮาร์ดแวร์, ซอฟต์แวร์, ระบบเครือข่าย, ฐานข้อมูลกองทุน Bonanza, ข้อมูลลูกค้า และบุคลากร
- ระบุภัยคุกคาม (Threats):** เช่น การโจมตีด้วย Ransomware, การเจาะระบบผ่านช่องโหว่ Firewall, การลักลอบนำข้อมูลออกไปภายนอก (Data Leakage), ไฟฟ้าดับเกินพิกัดแบตเตอรี่ UPS, หรือความผิดพลาดของผู้ดูแลระบบ
- ระบุช่องโหว่ (Vulnerabilities):** จากรายงานการตรวจสอบช่องโหว่ประจำงวด (Vulnerability Scan), พอร์ตเปิดที่ไม่ได้ใช้งาน, หรือการไม่ได้อัปเดต Firmware ของ FortiGate

ขั้นตอนที่ 2: การวิเคราะห์และประเมินระดับความเสี่ยง (Risk Analysis & Evaluation)

ประเมินความเสี่ยงโดยใช้เกณฑ์เมทริกซ์ 5x5 แบ่งเป็น:

- ระดับโอกาสเกิด (Likelihood: 1 - 5):**
 - 1 = เกิดขึ้นได้ยากมาก (Rare: อาจเกิดมากกว่า 3 ปีต่อครั้ง)
 - 2 = เกิดขึ้นได้น้อย (Unlikely: เกิดขึ้น 1-3 ปีต่อครั้ง)
 - 3 = มีโอกาสเกิดขึ้นปานกลาง (Possible: เกิดขึ้นปีละครั้ง)
 - 4 = มีโอกาสเกิดขึ้นบ่อย (Likely: เกิดขึ้นไตรมาสละครั้ง)
 - 5 = เกิดขึ้นเกือบแน่นอน (Almost Certain: เกิดขึ้นบ่อยครั้งในรอบเดือน)
- ระดับความรุนแรงของผลกระทบ (Impact: 1 - 5):**
 - 1 = ไม่มีผลกระทบหรือน้อยมาก (Insignificant: ระบบช้าลงเล็กน้อย ไม่กระทบคำสั่งซื้อขาย)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 23 / 107
--	--	---

- 2 = ผลกระทบต่ำ (Minor: ระบบใช้งานไม่ได้สั้นกว่า 30 นาที กระทบผู้ใช้กลุ่มเล็ก)
- 3 = ผลกระทบปานกลาง (Moderate: ชัดข้อง 1-2 ชั่วโมง ไม่มีความเสียหายทางการเงิน)
- 4 = ผลกระทบสูง (Major: ระบบ Bonanza หยุดชะงักระหว่างตลาดเปิด มีความเสียหายต่อธุรกรรม)
- 5 = ผลกระทบวิกฤต (Catastrophic: ข้อมูลลูกค้ารั่วไหลเป็นวงกว้าง หรือระบบขัดข้องเกิน 4 ชม. ต้องรายงาน ก.ล.ต.)
- **สูตรการคำนวณ:** 'ระดับความเสี่ยง (Risk Score) = โอกาสเกิด (Likelihood) × ผลกระทบ (Impact)'
- **1 - 4 (สีเขียว - Low):** ยอมรับได้ เฝ้าระวังตามปกติ
- **5 - 9 (สีเหลือง - Medium):** กำหนดมาตรการควบคุมเพิ่มเติมตามรอบปกติ
- **10 - 15 (สีส้ม - High):** ต้องจัดทำแผนลดความเสี่ยงอย่างเร่งด่วนภายใน 30 วัน
- **16 - 25 (สีแดง - Critical):** ความเสี่ยงวิกฤต ต้องระงับความเสี่ยงและรายงาน MD ทันที ดำเนินการแก้ไขภายใน 7 วัน

ขั้นตอนที่ 3: การกำหนดแผนจัดการความเสี่ยง (Risk Treatment)

สำหรับความเสี่ยงระดับ High และ Critical ให้เลือกกลยุทธ์จัดการข้อใดข้อหนึ่ง:

- 1. การลดความเสี่ยง (Mitigate):** ติดตั้งอุปกรณ์ควบคุมเพิ่มเติม เช่น เปิดใช้งาน IPS บน FortiGate, บังคับใช้ MFA บนระบบ Bonanza, หรือยกระดับสถาปัตยกรรมสำรองไฟ
- 2. การโอนย้ายความเสี่ยง (Transfer):** จัดทำประกันภัยความเสี่ยงทางไซเบอร์ (Cyber Insurance) หรือกำหนดข้อตกลง SLA ชดเชยความเสียหายกับผู้ให้บริการคลาวด์
- 3. การหลีกเลี่ยงความเสี่ยง (Avoid):** ยกเลิกการใช้งานซอฟต์แวร์หรือบริการที่มีช่องโหว่ร้ายแรงและไม่สามารถแก้ไขได้
- 4. การยอมรับความเสี่ยง (Accept):** ใช้เฉพาะกรณีที่ต้นทุนการจัดการสูงกว่ามูลค่าความเสียหายที่อาจเกิดขึ้น และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากคณะกรรมการบริษัทเท่านั้น

ขั้นตอนที่ 4: การติดตามและรายงานผล (Monitoring & Reporting)

1. IT Specialist บันทึกข้อมูลความเสี่ยง แผนจัดการ และผู้รับผิดชอบลงใน **ทะเบียนความเสี่ยงด้าน IT (IT Risk Register)**
2. ติดตามความคืบหน้าของแผนจัดการความเสี่ยงทุกเดือน
3. สรุปรายงานสถานะความเสี่ยง (Risk Dashboard) เสนอต่อคณะกรรมการกำกับดูแลด้าน IT (ITSC) และรายงานต่อคณะกรรมการบริษัท (BoD) ทุกไตรมาส

6. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

1. GW-TMP-03: ทะเบียนความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Register)
2. GW-TMP-04: รายงานผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง (Risk Treatment Plan)
3. รายงานการประชุมคณะกรรมการกำกับดูแลด้าน IT (ITSC Meeting Minutes)
4. รายงานผลการสแกนช่องโหว่ความปลอดภัยประจำไตรมาส (Quarterly Vulnerability Assessment Report)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 24 / 107
--	---	---

[GW-SOP-02] ขั้นตอนการประเมินและคัดเลือกผู้ให้บริการคลาวด์

(Cloud Service Provider Selection and Due Diligence Procedure)

รหัสเอกสาร	GW-SOP-02	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาศิลป์ ก้านจักร IT Specialist	นายโสธชา ตั้งลิदानนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดเกณฑ์และขั้นตอนการตรวจสอบความพร้อม (Due Diligence), การประเมินความเสี่ยง, การคัดเลือก และการกำกับดูแลผู้ให้บริการระบบคลาวด์ (Cloud Service Provider: CSP) ทั้งในส่วนของการสำรองข้อมูลนอกสถานที่ (Offsite Cloud Backup) และบริการโครงสร้างพื้นฐานบนคลาวด์ (IaaS/PaaS) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

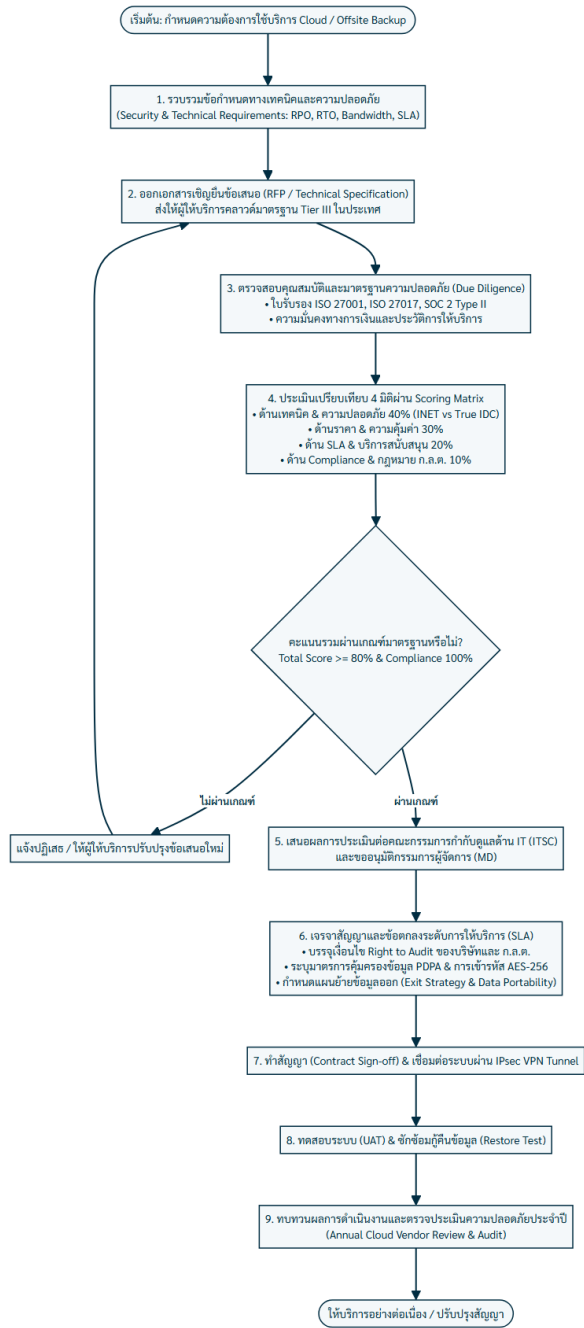
- มั่นใจว่าผู้ให้บริการคลาวด์มีมาตรฐานความมั่นคงปลอดภัยสากล สามารถรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูลกองทุนและข้อมูลลูกค้าได้อย่างมีประสิทธิภาพ
- กำหนดเกณฑ์เปรียบเทียบเชิงลึกในการคัดเลือกผู้ให้บริการชั้นนำระดับ Enterprise Data Center ในประเทศไทย (เช่น การเปรียบเทียบข้อเสนอระหว่าง INET Cloud และ True IDC) ให้มีความโปร่งใส คำนวณ และตอบโต้ทางเทคนิค
- ปฏิบัติตามประกาศ ก.ล.ต. สช. 38/2565, ประกาศแนวปฏิบัติ นป. 6/2567
เรื่องการใช้บริการเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing & Cloud Computing), และ
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)

2. ขอบเขตการบังคับใช้ (Scope)

มีผลบังคับใช้กับการจัดหา คัดเลือก ทำสัญญา ใช้งาน

และตรวจสอบประเมินผู้ให้บริการระบบคลาวด์ทุกประเภทที่เชื่อมต่อกับระบบสารสนเทศของบริษัท โดยเฉพาะระบบ Hybrid Cloud Backup ที่เชื่อมต่อระหว่างตู้แร็ค 42U ขึ้น 38 วัน แบงก์ค็อก และศูนย์ข้อมูลคลาวด์ภายนอก

3. ฟังก์กระบวนการประเมินและคัดเลือกผู้ให้บริการคลาวด์ (Operational Process Flow)



รูปภาพ: ฟังก์กระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-02 ขั้นตอนการประเมินและคัดเลือกผู้ให้บริการคลาวด์

4. ตารางความรับผิดชอบ (RACI Matrix)

กิจกรรม / ขั้นตอนการทำงาน	IT Specialist	CIO / Compliance	กรรมการผู้จัดการ (MD)	ผู้ให้บริการ (CSP)
1. จัดทำข้อกำหนดทางเทคนิค (TOR / RFP)	R / A	C	I	-
2. ตรวจสอบใบรับรองและเกณฑ์ Due Diligence	R	A	I	C (ส่งเอกสาร)
3. เปรียบเทียบข้อเสนอทางเทคนิคและราคา	R	C	A	C (ส่งราคา)
4. ตรวจสอบร่างสัญญาและเงื่อนไข ก.ล.ต.	C	R / A	A	C (เจรจา)
5. อนุมัติจัดจ้างและลงนามสัญญา	I	C	R / A	R / A
6. ติดตั้ง ทดสอบระบบเครือข่าย VPN และ Backup	R / A	C	I	R (ประสานงาน)
7. ประเมินผล SLA และตรวจสอบประจำปี	R	A	I	C

5. เกณฑ์การประเมินความพร้อมและคัดเลือกผู้ให้บริการคลาวด์ (Evaluation Criteria)

การประเมินผู้ให้บริการ (เช่น การเปรียบเทียบระหว่าง INET Cloud และ True IDC) ต้องใช้ตารางคะแนนมาตรฐาน 4 ด้าน น้ำหนักรวม 100%:

5.1 ด้านความมั่นคงปลอดภัยและสถาปัตยกรรมระบบ (40%)

- มาตรฐานศูนย์ข้อมูล (Data Center Tier):** ต้องตั้งอยู่ในประเทศไทย และได้รับการรับรองมาตรฐานอย่างน้อย Tier III (Uptime Institute) หรือเทียบเท่า
- การรับรองความมั่นคงปลอดภัยสากล:** ต้องมีใบรับรองมาตรฐาน ISO/IEC 27001 (ISMS), ISO/IEC 27017 (Cloud Security), และรายงานผลการตรวจรับรอง SOC 2 Type II
- การเข้ารหัสข้อมูล (Encryption Standard):** ต้องรองรับการเข้ารหัสข้อมูลขณะจัดเก็บ (Encryption at Rest) ด้วย AES-256 และการส่งผ่านข้อมูล (Encryption in Transit) ผ่าน IPsec VPN หรือ TLS 1.3
- การแบ่งแยกการเข้าถึงข้อมูล (Logical Isolation / Multi-Tenancy):**
ข้อมูลของบริษัทต้องถูกแยกส่วนจากลูกค้ารายอื่นอย่างเด็ดขาด

5.2 ด้านความคุ้มค่าและโครงสร้างราคา (30%)

- ต้นทุนค่าบริการรายเดือน (OpEx) และค่าติดตั้งเริ่มต้น (Setup Fee)
- ค่าใช้จ่ายในการรับส่งข้อมูลออก (Egress Data Transfer Fee) ต้องมีความชัดเจนและสมเหตุสมผล
- ความยืดหยุ่นในการปรับขยายขนาดพื้นที่จัดเก็บ (Scalability on Demand)

5.3 ด้านความพร้อมใช้งานและข้อตกลงระดับบริการ SLA (20%)

- เกณฑ์ความพร้อมใช้งาน (Service Availability):** ไม่ต่ำกว่า 99.95% ต่อเดือน

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 27 / 107
--	---	---

2. การตอบสนองเมื่อเกิดเหตุขัดข้อง (Support Response Time): ทีมวิศวกร Support ดูแลตลอด 24 ชั่วโมง 7 วัน (24x7) ตอบสนองเหตุวิกฤตภายใน 15-30 นาที

3. มาตรการชดเชย (Penalty / Service Credit): มีการชดเชยค่าบริการหากระดับการให้บริการต่ำกว่า SLA ที่ตกลงไว้

5.4 ด้านความสอดคล้องกับกฎหมายและข้อกำหนด ก.ล.ต. (10%)

- สิทธิในการเข้าตรวจสอบ (Right to Audit):** ผู้ให้บริการต้องยินยอมให้บริษัท ผู้ตรวจสอบอิสระ (เช่น ผู้ตรวจสอบอิสระภายนอก) และเจ้าหน้าที่สำนักงาน ก.ล.ต. เข้าตรวจสอบระบบหรือขอเอกสารหลักฐานการควบคุมความปลอดภัยได้
- ถิ่นที่อยู่ของข้อมูล (Data Sovereignty):** ข้อมูลต้องจัดเก็บอยู่ภายในราชอาณาจักรไทยเท่านั้น ห้ามถ่ายโอนออกนอกประเทศโดยไม่ได้รับความเห็นชอบเป็นลายลักษณ์อักษร
- แผนการย้ายข้อมูลออก (Exit Strategy):** ผู้ให้บริการต้องมีกระบวนการส่งมอบข้อมูลกลับคืนให้แก่บริษัทในรูปแบบมาตรฐาน (Open Standard Format) และมีขั้นตอนการลบทำลายข้อมูล (Data Sanitization) อย่างปลอดภัยเมื่อสิ้นสุดสัญญา

6. ข้อกำหนดในสัญญาว่าจ้างผู้ให้บริการคลาวด์ (Mandatory Contract Clauses)

สัญญาว่าจ้างผู้ให้บริการคลาวด์ต้องมีข้อกำหนดบังคับตามเกณฑ์ ก.ล.ต. ดังต่อไปนี้อย่างครบถ้วน:

- ข้อสัญญาการรักษาความลับ (Confidentiality & Non-Disclosure):** ห้ามนำข้อมูลไปเปิดเผยหรือใช้ประโยชน์อื่นใด
- ข้อสัญญาสิทธิในการเข้าตรวจสอบ (Right to Audit Clause):** ครอบคลุมการตรวจสอบโดยบริษัทและสำนักงาน ก.ล.ต.
- ข้อสัญญาการแจ้งเหตุการณ์ละเมิด (Incident Notification SLA):** หากเกิดเหตุข้อมูลรั่วไหลหรือถูกโจมตีทางไซเบอร์ ผู้ให้บริการต้องแจ้งเตือนบริษัทภายใน 2 ชั่วโมง
- ข้อสัญญาการคุ้มครองข้อมูลส่วนบุคคล (PDPA Data Processing Agreement: DPA):** ผู้ให้บริการทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ต้องปฏิบัติตามคำสั่งของบริษัทเท่านั้น
- ข้อสัญญาแผนสำรองและการยกเลิกสัญญา (Exit Plan):** การรับประกันการส่งมอบข้อมูลและการลบทำลายข้อมูลอย่างสมบูรณ์ภายใน 30 วันหลังสิ้นสุดสัญญา

7. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

- GW-TMP-05: ตารางประเมินเปรียบเทียบผู้ให้บริการคลาวด์ (Cloud Vendor Assessment Scoring Matrix)
- สำเนาใบรับรองมาตรฐาน ISO 27001, ISO 27017, SOC 2 Type II ของผู้ให้บริการ
- สัญญาว่าจ้างพร้อมเอกสารข้อตกลงระดับการให้บริการ (SLA) และสัญญาการประมวลผลข้อมูล (DPA)
- รายงานผลการทดสอบการเชื่อมต่อ VPN และผลการทดสอบกู้คืนข้อมูล (Cloud Backup & Restore UAT Report)
- รายงานผลการประเมินทบทวนผู้ให้บริการประจำปี (Annual Cloud Vendor Evaluation Report)

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 28 / 107
--	---	---

[GW-SOP-03] การบริหารจัดการทรัพย์สินทางปัญญาและลิขสิทธิ์ซอฟต์แวร์

(Software Intellectual Property & License Compliance Procedure)

รหัสเอกสาร	GW-SOP-03	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งสินานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกฉัตร ภูมิพลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดขึ้นเพื่อควบคุม กำกับดูแล และบริหารจัดการลิขสิทธิ์ซอฟต์แวร์ ทรัพย์สินทางปัญญา

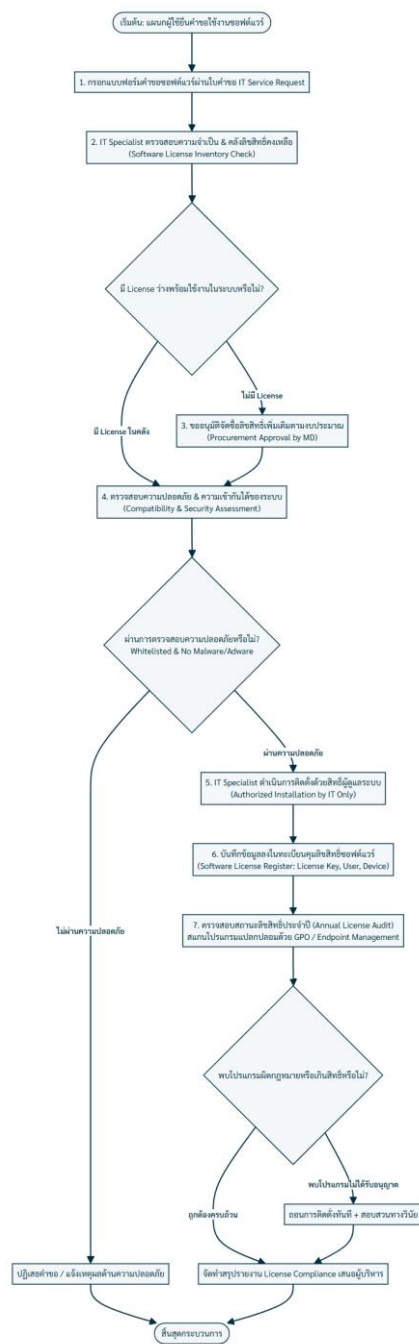
และสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ทั้งหมดของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- ป้องกันการใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์ (Unlicensed / Pirated Software) ในองค์กรโดยเด็ดขาด
- คุ้มครองทรัพย์สินทางปัญญา ซอร์สโค้ด สูตรการค้า ความลับทางการเงิน และฐานข้อมูลของบริษัทมิให้รั่วไหลหรือถูกละเมิด
- ปฏิบัติตามพระราชบัญญัติลิขสิทธิ์, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, และเกณฑ์การกำกับดูแลของสำนักงาน ก.ล.ต. ตามประกาศที่ สธ. 38/2565
- บริหารต้นทุนการจัดซื้อและการต่ออายุสัญญาลิขสิทธิ์ซอฟต์แวร์ (License Optimization) ให้เกิดความคุ้มค่าสูงสุด

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมซอฟต์แวร์เชิงพาณิชย์ (Commercial Software), ซอฟต์แวร์แบบบริการ (SaaS เช่น Microsoft 365), ระบบงานหลักกองทุน (ระบบ Bonanza Investment), ระบบปฏิบัติการ (Windows OS / Server), ซอฟต์แวร์โอเพนซอร์ส (Open Source), และโค้ดโปรแกรมทั้งหมดที่ทำงานบนอุปกรณ์คอมพิวเตอร์และเซิร์ฟเวอร์ของบริษัท

3. ฟังก์กระบวนการบริหารจัดการลิขสิทธิ์ซอฟต์แวร์ (Operational Process Flow)



รูปภาพ: ฟังก์กระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-03
การบริหารจัดการทรัพย์สินทางปัญญาและลิขสิทธิ์ซอฟต์แวร์

4. ตารางความรับผิดชอบ (RACI Matrix)

กิจกรรม / ขั้นตอนการทำงาน	พนักงานผู้ขอใช้	IT Specialist	CIO / Compliance	กรรมการผู้จัดการ (MD)
1. ร้องขอซอฟต์แวร์เพื่อการปฏิบัติงาน	R	C	I	I
2. ตรวจสอบความปลอดภัยและความถูกต้องของ License	I	R / A	C	I
3. อนุมัติจัดซื้อซอฟต์แวร์เพิ่มเติม	I	C	C	R / A
4. ติดตั้งและเปิดใช้งานสิทธิ์ลิขสิทธิ์	I	R / A	I	I
5. บันทึกและปรับปรุงทะเบียนคุมซอฟต์แวร์	I	R / A	C	I
6. ตรวจสอบลิขสิทธิ์ประจำปี (Software Audit)	I	R	A	I

5. มาตรการควบคุมการใช้งานซอฟต์แวร์ (Operational Control Rules)

5.1 สิทธิ์ในการติดตั้งซอฟต์แวร์ (Installation Rights)

- พนักงานทั่วไปไม่มีสิทธิ์ติดตั้งซอฟต์แวร์ด้วยตนเอง: เครื่องคอมพิวเตอร์พนักงานทุกเครื่องต้องถูกตั้งค่าผ่าน Active Directory Group Policy (GPO) โดยตัวสิทธิ์ Local Administrator เพื่อป้องกันการลักลอบติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต
- การติดตั้ง อัปเดต หรือถอนการติดตั้งซอฟต์แวร์ ต้องดำเนินการโดย ฝ่ายเทคโนโลยีสารสนเทศ เท่านั้น

5.2 มาตรการควบคุมซอฟต์แวร์โอเพนซอร์สและฟรีแวร์ (Open-Source & Freeware Policy)

- ซอฟต์แวร์ประเภทฟรีแวร์ หรือ Open-Source ต้องได้รับการตรวจสอบประเภทสัญญาอนุญาต (License Type) เช่น MIT, Apache 2.0, BSD หรือ GNU GPL ก่อนนำมาใช้งาน
- ห้ามนำซอฟต์แวร์ที่ระบุว่า "Free for Personal / Non-Commercial Use Only" มาใช้ในการดำเนินธุรกิจของบริษัทโดยเด็ดขาด

5.3 การคุ้มครองทรัพย์สินทางปัญญาของบริษัท (Company Intellectual Property)

- ซอร์สโค้ด สูตรการคำนวณทางการเงิน กลยุทธ์การจัดพอร์ตการลงทุน และผังโครงสร้างฐานข้อมูลของระบบจัดการกองทุน Bonanza ถือเป็นความลับทางการค้าและทรัพย์สินทางปัญญาของบริษัทแต่เพียงผู้เดียว
- ห้ามบุคลากรคัดลอก นำโค้ดขึ้น Public Repository (เช่น GitHub สาธารณะ) หรือนำไปใช้ส่วนตัวโดยไม่ได้รับอนุมัติเป็นลายลักษณ์อักษรจากกรรมการผู้จัดการ

5.4 การตรวจสอบลิขสิทธิ์ประจำปี (Annual Software Audit)

- ฝ่าย IT ต้องจัดทำตรวจสอบซอฟต์แวร์ที่ติดตั้งอยู่บนอุปกรณ์ทั้งหมดอย่างน้อยปีละ 1 ครั้ง โดยเปรียบเทียบระหว่าง:
 - จำนวนสิทธิ์การใช้งานที่มีหลักฐานการซื้อถูกต้อง (Purchased Licenses)
 - จำนวนเครื่องที่ติดตั้งจริง (Active Installed Instances)
- หากตรวจพบส่วนต่าง (Discrepancy) ต้องดำเนินการจัดซื้อเพิ่มหรือถอดถอนออกจากเครื่องทันทีภายใน 7 วันทำการ

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 31 / 107
---	--	--

6. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

1. GW-TMP-06: ทะเบียนคุมลิขสิทธิ์ซอฟต์แวร์ (Software License Register)
2. เอกสารใบอนุญาติสิทธิ์ (Certificate of Authenticity: COA), ใบเสร็จรับเงิน, และใบแจ้งหนี้การสั่งซื้อลิขสิทธิ์
3. ใบคำขอใช้บริการและติดตั้งซอฟต์แวร์ (IT Service Request Ticket)
4. รายงานผลการตรวจสอบลิขสิทธิ์ซอฟต์แวร์ประจำปี (Annual Software License Compliance Audit Report)

[GW-SOP-04] การจัดการทรัพย์สินสารสนเทศและล้างข้อมูลถาวร

รหัสเอกสาร	GW-SOP-04	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุลชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดขั้นตอนการบริหารจัดการวงจรชีวิตทรัพย์สินสารสนเทศ (IT Asset Lifecycle) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

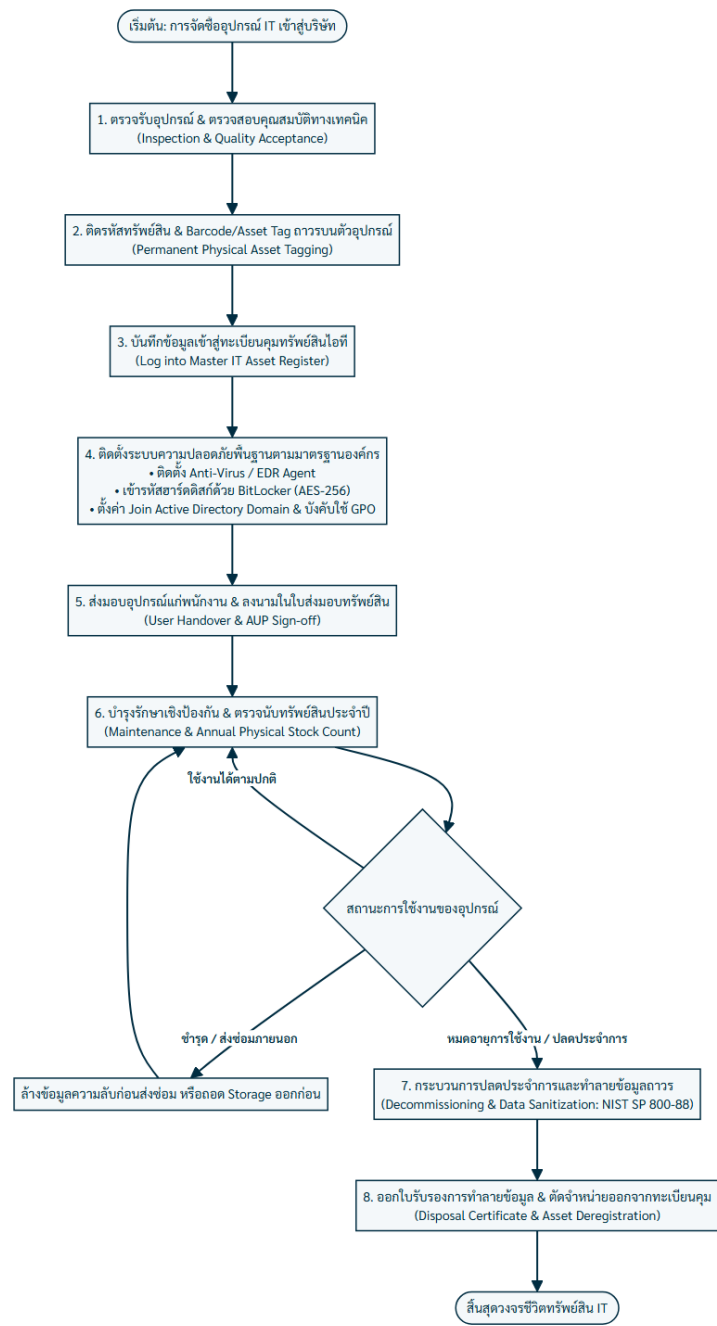
- ควบคุม บันทึก และติดตามทรัพย์สินฮาร์ดแวร์ อุปกรณ์เครือข่าย และโครงสร้างพื้นฐานไอทีทั้งหมดอย่างแม่นยำ
 - ป้องกันการสูญหาย ถูกโจรกรรม หรือการนำทรัพย์สินของบริษัทไปใช้งานโดยไม่ได้รับอนุญาต
 - กำหนดมาตรฐานการทำลายข้อมูลความลับ (Data Sanitization) ก่อนการจำหน่าย ปลดประจำการ หรือส่งซ่อมอุปกรณ์
 - ปฏิบัติตามมาตรฐานสากล ISO/IEC 27001 และประกาศสำนักงาน ก.ล.ต. สธ. 38/2565
- เรื่องการคุ้มครองความมั่นคงปลอดภัยของระบบและข้อมูลสารสนเทศ

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมอุปกรณ์ฮาร์ดแวร์ทั้งหมดของบริษัท ได้แก่:

- อุปกรณ์ในห้องแม่ข่าย (Server Room 42U ณ วัน แบงค็อก ทาวเวอร์ 4 ชั้น 38): เซิร์ฟเวอร์, ตู้แร็ค 42U, ไฟร์วอลล์ FortiGate 70F, สวิตช์ UniFi PoE, อุปกรณ์สำรองไฟ True Online UPS, และระบบกล้อง CCTV NVR
- อุปกรณ์สำหรับผู้ใช้งาน: เครื่องคอมพิวเตอร์ตั้งโต๊ะ, โน้ตบุ๊ก, แท็บเล็ต, หน้าจอ, คีย์บอร์ด, และโทรศัพท์สำนักงาน
- อุปกรณ์จัดเก็บข้อมูล: Hard Disk Drive (HDD), Solid State Drive (SSD), USB Flash Drive, และ Backup Tape/Storage Media

3. ฟังก์กระบวนการจัดการทรัพย์สินสารสนเทศ (Operational Process Flow)



รูปภาพ: ฟังก์กระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-04 การจัดการทรัพย์สินสารสนเทศและล้างข้อมูลถาวร

4. ตารางความรับผิดชอบ (RACI Matrix)

กิจกรรม / ขั้นตอนการทำงาน	IT Specialist	พนักงานผู้ครอบครอง	CIO / Compliance	กรรมการผู้จัดการ (MD)
1. ตรวจสอบอุปกรณ์และติด Asset Tag	R / A	I	I	I
2. ลงทะเบียนใน IT Asset Register	R / A	I	C	I
3. ลงนามรับมอบและยอมรับข้อตกลง AUP	I	R	I	I
4. ตรวจสอบทรัพย์สินประจำปี (Asset Audit)	R	C	A	I
5. ล้างข้อมูลถาวร (Sanitization) ก่อนปลดประจำการ	R / A	I	C	I
6. อนุมัติตัดจำหน่ายทรัพย์สินออกจากบัญชี	C	I	C	R / A

5. ขั้นตอนการปฏิบัติงานโดยละเอียด (Step-by-Step Procedure)

ขั้นตอนที่ 1: การตรวจรับและติดฉลากทรัพย์สิน (Receiving & Tagging)

- เมื่ออุปกรณ์มาถึงบริษัท IT Specialist ต้องตรวจสอบความถูกต้องของสเปกเทียบกับใบสั่งซื้อ (PO) และบันทึก Serial Number
- ติดแผ่นป้ายฉลากทรัพย์สิน (Asset Tag) ที่มีรหัสเฉพาะ (เช่น 'GW-HW-NB-001' สำหรับโน้ตบุ๊ก หรือ 'GW-HW-SRV-001' สำหรับเซิร์ฟเวอร์) บนตำแหน่งที่มองเห็นได้ชัดเจนและทนทานต่อการลอกออก
- บันทึกข้อมูลลงใน ทะเบียนคุมทรัพย์สินสารสนเทศ (IT Asset Register) ภายใน 24 ชั่วโมง

ขั้นตอนที่ 2: การเตรียมความปลอดภัยก่อนส่งมอบ (Security Hardening Baseline)

ก่อนส่งมอบอุปกรณ์ให้ผู้ใช้งาน IT Specialist ต้องดำเนินการ Hardening:

- อัปเดต Patch ระบบปฏิบัติการและ Firmware เป็นเวอร์ชันล่าสุดที่เสถียร
- เปิดใช้งานระบบเข้ารหัสพื้นที่จัดเก็บข้อมูล (BitLocker Drive Encryption) โดยใช้กุญแจเข้ารหัสความยาว 256-bit
- บันทึก Recovery Key เก็บไว้ใน Active Directory หรือตู้เซฟความปลอดภัยของฝ่าย IT
- ติดตั้ง Anti-Virus/EDR, ปิดพอร์ตที่ไม่ได้ใช้งาน, และบังคับใช้ GPO ตามมาตรฐานองค์กร

ขั้นตอนที่ 3: การส่งมอบและการยืมคืน (Handover & Return)

- พนักงานผู้รับอุปกรณ์ต้องลงนามใน แบบฟอร์มส่งมอบและรับคืนทรัพย์สินสารสนเทศ (IT Asset Handover Form) และลงนามรับทราบนโยบายการใช้งานที่ยอมรับได้ (AUP)
- เมื่อพนักงานลาออก โอนย้ายตำแหน่ง หรืออุปกรณ์ชำรุด ต้องส่งมอบอุปกรณ์คืนให้แก่ฝ่าย IT ภายในวันสุดท้ายของการทำงาน เพื่อตรวจสอบสภาพและทำการ Reset ค่ายระบบ

ขั้นตอนที่ 4: การตรวจนับทรัพย์สินประจำปี (Annual Physical Asset Verification)

- ฝ่าย IT ร่วมกับฝ่ายบัญชีและการเงิน ต้องจัดให้มีการเดินตรวจนับทรัพย์สินทางกายภาพ (Physical Count) อย่างน้อยปีละ 1 ครั้ง

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 35 / 107
--	--	---

- หากพบทรัพย์สินสูญหาย ขำรุ่ด หรือข้อมูลไม่ตรงกับทะเบียนคุม
ต้องจัดทำรายงานการสอบสวนหาสาเหตุเสนอต่อคณะกรรมการกำกับดูแลด้าน IT ภายใน 15 วัน

ขั้นตอนที่ 5: การปลดประจำการและการล้างทำลายข้อมูล (Disposal & Sanitization)

อุปกรณ์คอมพิวเตอร์และสื่อบันทึกข้อมูลที่จะจำหน่าย ปลดประจำการ หรือบริจาค ต้องผ่านกระบวนการล้างข้อมูลตามมาตรฐาน NIST SP 800-88 Rev. 1 (Guidelines for Media Sanitization):

- การล้างข้อมูลแบบปลอดภัย (Purge / Cryptographic Erase):** เขียนทับข้อมูลทั้งหมด (Zero-Fill / Multi-pass Overwrite) อย่างน้อย 3 รอบ หรือส่งคำสั่ง Secure Erase บนไดรฟ์ SSD
- การทำลายทางกายภาพ (Physical Destruction):** สำหรับสื่อบันทึกข้อมูลที่ไม่สามารถล้างข้อมูลได้
หรือมีข้อมูลความลับถูกค้ำระดับสูงสุด ต้องใช้วิธีการเจาะทำลายงานแม่เหล็ก (Degaussing / Shredding / Crushing)
ให้เสียหายจนไม่สามารถกู้คืนได้
- IT Specialist ต้องจัดทำ ใบรับรองการทำลายข้อมูลและปลดประจำการทรัพย์สิน (Data Sanitization & Disposal Certificate) เก็บไว้เป็นหลักฐานเพื่อการตรวจสอบ

6. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

- GW-TMP-07: ทะเบียนคุมทรัพย์สินสารสนเทศหลัก (Master IT Hardware Asset Register)
- GW-TMP-08: แบบฟอร์มการส่งมอบและรับคืนทรัพย์สินสารสนเทศ (IT Asset Handover & Return Form)
- GW-TMP-09: ใบรับรองการทำลายข้อมูลและตัดจำหน่ายทรัพย์สิน (Data Sanitization & Asset Disposal Certificate)
- รายงานผลการตรวจนับทรัพย์สินประจำปี (Annual Physical Asset Verification Report)

[GW-SOP-05] การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ (IAM)

(Identity and Access Management Procedure: IAM)

รหัสเอกสาร	GW-SOP-05	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งลิขิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกฉัตร ฤทธิกุลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดขั้นตอนมาตรฐานในการบริหารจัดการตัวตน บัญชีผู้ใช้งาน และสิทธิ์การเข้าถึงระบบสารสนเทศ (Identity and Access Management: IAM) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- บังคับใช้หลักการสิทธิ์เท่าที่จำเป็นในการปฏิบัติงาน (Least Privilege) และหลักการจำเป็นต้องรู้ (Need-to-Know)
- ป้องกันการเข้าถึง การแก้ไข หรือการลักลอบนำข้อมูลพอร์ทการลงทุนและข้อมูลลูกค้าออกจากระบบโดยมิชอบ
- กำหนดการแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties: SoD)

เพื่อป้องกันความขัดแย้งทางผลประโยชน์ระหว่างฝ่ายจัดการกองทุน (Fund Manager), ฝ่ายส่งคำสั่งซื้อขาย (Trader), ฝ่ายปฏิบัติการ (Operations/Settlement), ฝ่ายควบคุมความเสี่ยง (Risk/Compliance) และฝ่ายไอที (IT Specialist)

- ปฏิบัติตามประกาศ ก.ล.ต. สธ. 38/2565 และแนวปฏิบัติ นป. 6/2567

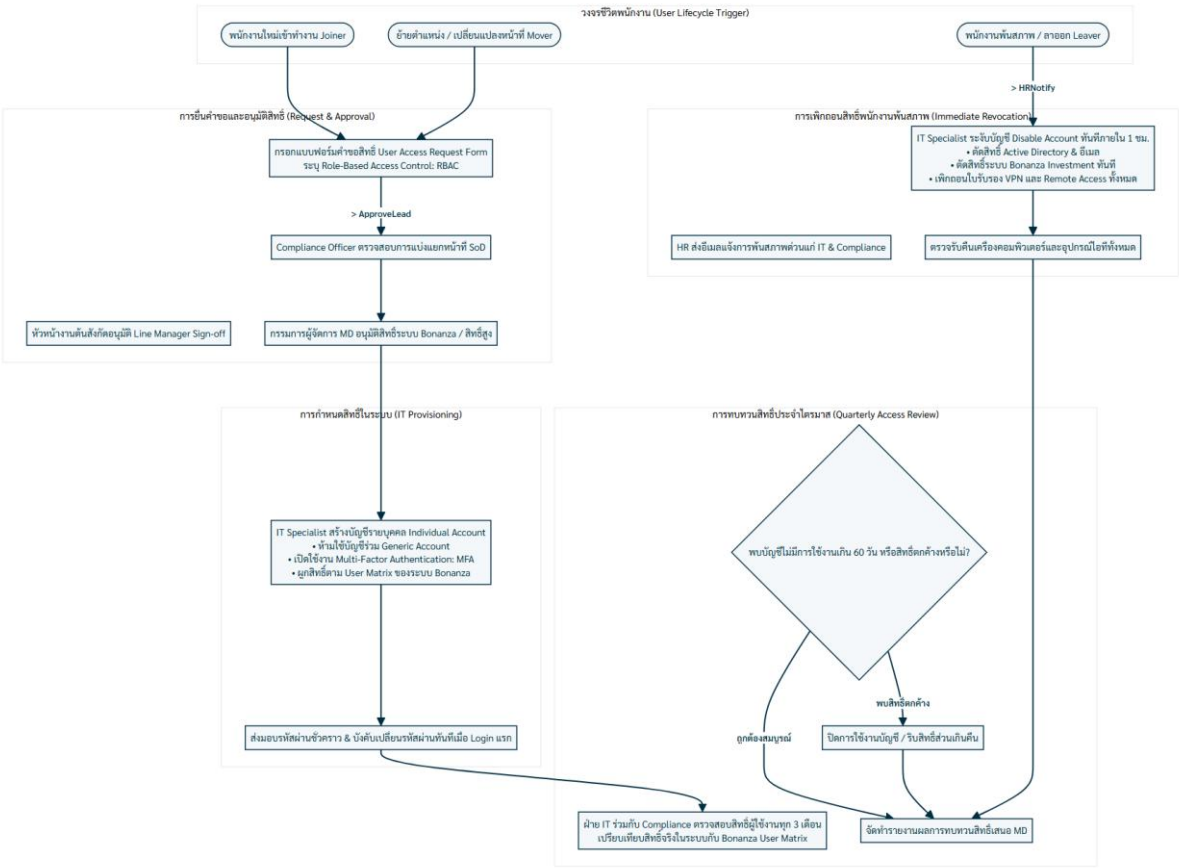
เรื่องการควบคุมการเข้าถึงระบบสารสนเทศของสถาบันการเงินและผู้ประกอบธุรกิจหลักทรัพย์

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมการจัดการสิทธิ์บนทุกระบบงานของบริษัท ได้แก่:

- ระบบจัดการกองทุนส่วนบุคคลหลัก: ระบบ Bonanza Investment
- ระบบจัดการบัญชีผู้ใช้และโดเมน: Active Directory Domain Services (AD DS)
- ระบบเครือข่ายและการเข้าถึงจากระยะไกล: FortiGate SSL-VPN / IPsec VPN
- ระบบคลาวด์และอิมเมจสำรอง: Microsoft 365 และ Hybrid Cloud Offsite Backup
- บัญชีผู้ดูแลระบบสิทธิ์สูง (Privileged / Administrative Accounts) ทั้งหมด

3. ฟังก์กระบวนการบริหารวงจรชีวิตผู้ใช้งาน (User Access Lifecycle: Joiner-Mover-Leaver Flow)



รูปภาพ: ฟังก์กระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-05 การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ (IAM)

4. เมทริกซ์การแบ่งแยกสิทธิ์ตามบทบาทในระบบ Bonanza Investment (Core RBAC Matrix)

แผนก / บทบาทหน้าที่ (Role)	บัญชี AD / PC	เข้าดูพอร์ตลูกค้า (View Portfolio)	สร้าง/แก้ไขพอร์ต (Edit Portfolio)	ส่งคำสั่งซื้อขาย (Execute Trade)	ยืนยันชำระราคา (Settlement)	สอบทาน Audit Log (Audit Review)	สิทธิ์ระดับแอดมิน (System Admin)
Fund Manager (ผู้จัดการกองทุน)	Yes	Yes	Yes (พอร์ตที่รับผิดชอบ)	No (Maker Only)	No	No	No
Trader (เจ้าหน้าที่ส่งคำสั่งซื้อขาย)	Yes	Yes (หน้าจอคำสั่ง)	No	Yes (Execute Only)	No	No	No
Back Office / Settlement	Yes	Yes	No	No	Yes	No	No
Risk / Compliance Officer	Yes	Yes (Read-Only)	No	No	No	Yes	No
IT Specialist / System Admin	Yes	No (ห้ามดูยอดเงิน)	No	No	No	Yes (System Log)	Yes (Configuration Only)
Managing Director (MD)	Yes	Yes (Full Dashboard)	Approval Role	Approval Role	Approval Role	Yes	No (บริหารจัดการ)

5. ขั้นตอนการปฏิบัติงานโดยละเอียด (Step-by-Step Procedure)

ขั้นตอนที่ 1: การขอสิทธิ์และสร้างบัญชีผู้ใช้งานใหม่ (Joiner)

- ฝ่ายทรัพยากรบุคคล (HR) หรือหัวหน้าแผนก กรอก แบบฟอร์มขอสิทธิ์การเข้าถึงระบบ (GW-TMP-02: User Access Request Form) ล่วงหน้าอย่างน้อย 3 วันทำการก่อนพนักงานเริ่มงาน
- ฝ่าย Compliance สอบทานว่าสิทธิ์ที่ขอไม่ขัดต่อหลักการ Segregation of Duties (SoD) เช่น ผู้ทำหน้าที่ส่งคำสั่งซื้อขาย (Trader) ต้องไม่มีสิทธิ์เป็นผู้ยืนยันยอดเงิน (Settlement)
- เมื่อได้รับอนุมัติจากกรรมการผู้จัดการ (MD) IT Specialist จึงทำการสร้างบัญชีผู้ใช้ใน Active Directory และระบบ Bonanza Investment โดยตั้งชื่อบัญชีตามรูปแบบทางการ: 'firstname.l@grandway.co.th'
- บัญชีใหม่ต้องถูกบังคับให้เปลี่ยนรหัสผ่านในครั้งแรกที่เข้าสู่ระบบ (Must change password at next logon) และต้องลงทะเบียนระบบ MFA ทันที

ขั้นตอนที่ 2: การปรับปรุงสิทธิ์เมื่อโยกย้ายตำแหน่ง (Mover)

- หากพนักงานย้ายแผนกหรือเปลี่ยนหน้าที่ ให้ยื่นแบบฟอร์มขอปรับปรุงสิทธิ์

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 39 / 107
--	--	---

2. IT Specialist ต้อง **เพิกถอนสิทธิ์เดิมออกทั้งหมดก่อน (Revoke Old Permissions)**
ก่อนที่จะกำหนดสิทธิ์ใหม่ตามบทบาทหน้าที่ใหม่ เพื่อป้องกันปัญหาการสะสมสิทธิ์เกินความจำเป็น (Privilege Creep)

ขั้นตอนที่ 3: การเพิกถอนสิทธิ์เมื่อพนักงานพ้นสภาพ (Leaver - Protocol ทันทันที)

- เมื่อพนักงานลาออก หรือถูกเลิกจ้าง ฝ่าย HR ต้องแจ้งฝ่าย IT และ Compliance ล่วงหน้า หรือทันทีที่มีผลเลิกจ้าง
- กรอบเวลาปฏิบัติการ (SLA):** IT Specialist ต้องทำการ **ระงับการใช้งานบัญชี (Disable Account)** ใน Active Directory, ระบบ Bonanza, และตัดสิทธิ์การเข้าถึง VPN / Cloud ทั้งหมด ภายในไม่เกิน **1 ชั่วโมง** นับจากได้รับแจ้ง
- ห้ามใช้วิธีลบบัญชีทันที (Do not delete) แต่ให้ระงับการใช้งาน (Disable) เพื่อเก็บบันทึกประวัติและ Audit Trail ไว้ตรวจสอบย้อนหลังอย่างน้อย 90 วัน

ขั้นตอนที่ 4: การบริหารจัดการบัญชีสิทธิ์สูง (Privileged Access Management: PAM)

- บัญชีระดับผู้ดูแลระบบ (Domain Admin, Database Admin, Firewall Admin) ต้องถูกแยกออกจากบัญชีใช้งานทั่วไป เช่น บัญชีทั่วไป 'khanasin.k' และบัญชีแอดมิน 'admin_khanasin'
- ห้ามใช้บัญชีแอดมินในการเปิดเว็บเบราว์เซอร์ทั่วไป หรือเปิดอีเมล เพื่อป้องกันความเสี่ยงจากมัลแวร์
- การใช้งานเซิร์ฟเวอร์ห้องแม่ข่าย (Server Room One Bangkok) หรือการ Config ไฟร์วอลล์ FortiGate ต้องผ่านการยืนยันตัวตน MFA และบันทึก Log การใช้งานทุกครั้ง

ขั้นตอนที่ 5: การทบทวนสิทธิ์การเข้าถึงประจำไตรมาส (Quarterly User Access Review)

- ในวันทำการสุดท้ายของทุกไตรมาส IT Specialist ต้องดึงรายงานบัญชีผู้ใช้งานที่ Active ทั้งหมดจากระบบ Active Directory, ระบบ Bonanza, และสิทธิ์ VPN
- ส่งรายงานให้หัวหน้าแต่ละแผนกและฝ่าย Compliance ตรวจสอบความถูกต้องของสิทธิ์
- หากพบบัญชีที่ไม่มีการใช้งานเกิน 60 วัน (Dormant Accounts) หรือพนักงานลาออกที่ยังคงมีสิทธิ์ค้างอยู่ ให้ระงับบัญชีทันที และจัดทำรายงานสรุปเสนอ MD

6. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

- GW-TMP-02:** แบบฟอร์มคำขอและเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบ (User and Privileged Access Request Form)
- GW-TEC-04:** เมทริกซ์สิทธิ์การใช้งานระบบงานหลัก (Master User Access Matrix for Bonanza Investment System)
- รายงานผลการทบทวนสิทธิ์ประจำไตรมาส (Quarterly User Access Review Report) พร้อมลายมือชื่อของ Compliance และ MD
- บันทึกประวัติการสร้าง ระบุ และเพิกถอนสิทธิ์ผู้ใช้งาน (Identity Management System Audit Trail)

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 40 / 107
--	---	---

[GW-SOP-06] การแบ่งระดับชั้นของข้อมูลและการเข้ารหัส

(Data Classification and Protection Procedure)

รหัสเอกสาร	GW-SOP-06	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งลิขิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณศลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดเกณฑ์การจำแนกประเภทระดับชั้นความลับของข้อมูล (Data Classification)

และขั้นตอนการคุ้มครองข้อมูลของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

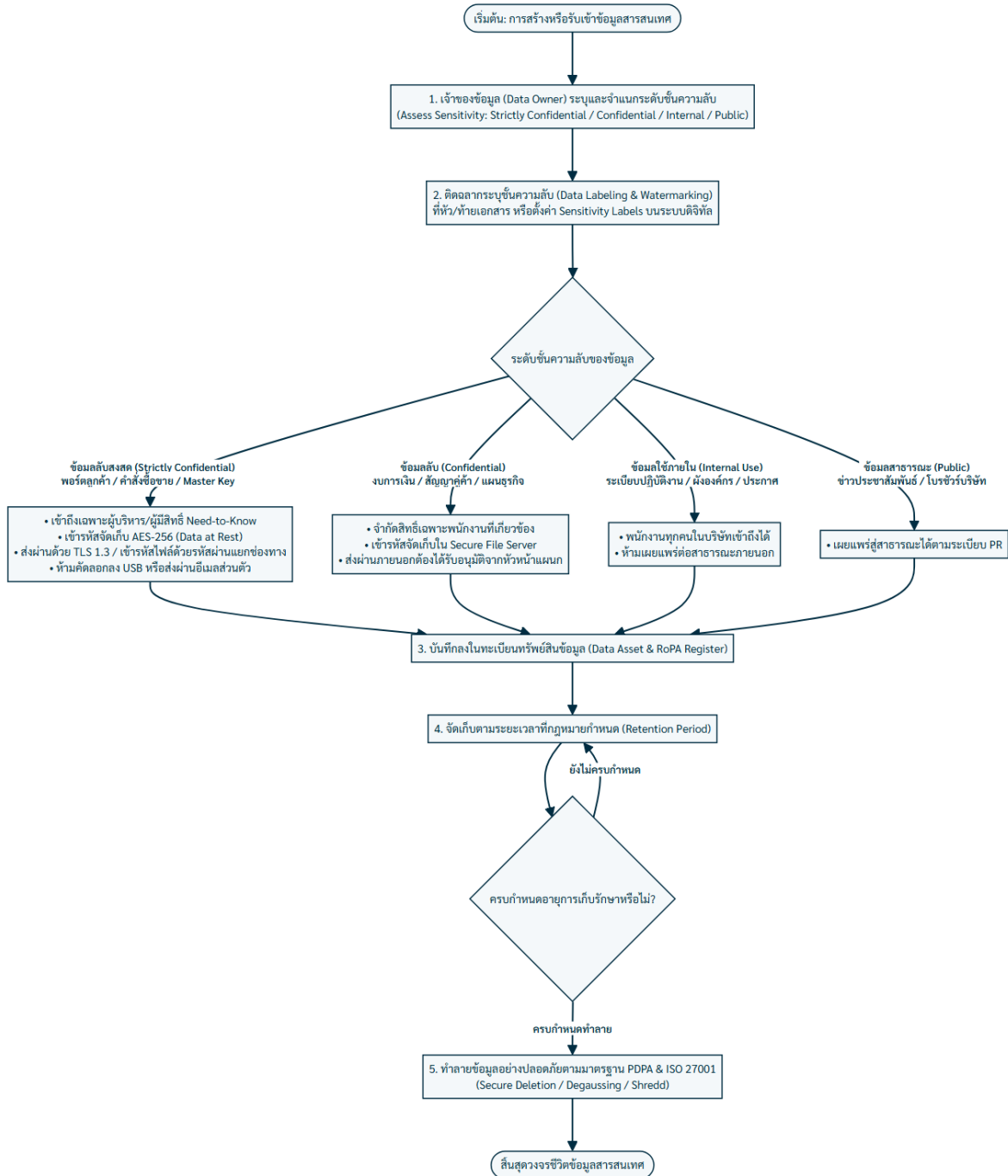
- ปกป้องข้อมูลพอร์ทการลงทุน ยอดทรัพย์สินลูกค้า ข้อมูลคำสั่งซื้อขาย และข้อมูลส่วนบุคคลมิให้รั่วไหลหรือถูกเปิดเผยโดยมิชอบ
- กำหนดมาตรการรักษาความมั่นคงปลอดภัยและการเข้ารหัสข้อมูล (Encryption) ให้เหมาะสมกับระดับความสำคัญของข้อมูลแต่ละประเภท
- ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และประกาศสำนักงาน ก.ล.ต. สธ. 38/2565 เรื่องการรักษาความลับของข้อมูลลูกค้าและข้อมูลภายในกองทุน

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมข้อมูลสารสนเทศทั้งหมดของบริษัท ทั้งในรูปแบบดิจิทัล (ไฟล์เอกสาร, ฐานข้อมูลระบบ Bonanza, อีเมล, ไฟล์สำรองข้อมูล)

และรูปแบบเอกสารกระดาษ ตลอดวงจรชีวิตของข้อมูล (สร้าง → จัดเก็บ → ใช้งาน → ส่งผ่าน → ทำลาย)

3. ผังกระบวนการแบ่งระดับชั้นและการคุ้มครองข้อมูล (Operational Process Flow)



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-06 การแบ่งระดับชั้นของข้อมูลและการเข้ารหัส

4. ตารางเกณฑ์การแบ่งระดับชั้นความลับของข้อมูล (Classification Matrix)

ระดับชั้นคว ามลับ	ตัวอย่างข้อมูลของบริษัท	สิทธิ์การเข้าถึง	การจัดเก็บ (Storage Security)	การส่งผ่านข้อมูล (Transmission)
1. ข้อมูลลับสูงสุ ด (Strictly Confidentia l)	- ข้อมูลพอร์ตและยอดเงินลงทุนของลูกค้า - คำสั่งซื้อขายหลักทรัพย์ (Trade Orders) - รหัสผ่านและ Private Key เข้าสู่ระบบ	ผู้บริหารระดับสูง และเจ้าหน้าที่ที่ได้รับอนุมัติเฉพาะเจาะจง (Strict Need-to-Know)	เข้ารหัส AES-256 ในฐานข้อมูล Bonanza และระบบ Storage / มีระบบบันทึก Audit Trail ทุกครั้งที่เปิดดู	บังคับใช้ TLS 1.3, ห้ามส่งทางอีเมลทั่วไปโดยไม่เข้ารหัสไ ฟ์, ห้ามนำออกจากระบบ
2. ข้อมูลลับ (Confidenti al)	- ข้อมูลบัญชีและการเงินของบ ริษัท - สัญญาเกี่ยวกับค่าและที่ปรึกษา (เช่น ผู้ตรวจสอบอิสระภายนอก) - ข้อมูลส่วนบุคคลพนักงาน (HR Records)	พนักงานในแผนกที่เกี่ยวข้อง และผู้บริหาร	จัดเก็บในโพลเดอร์เครือข่ายที่มีก ารจำกัดสิทธิ์ (Restricted File Share) และเข้ารหัส BitLocker	ส่งผ่านอีเมลองค์กรเท่านั้น หากส่งออกภายนอกต้องเข้ารหัสไฟล์ ด้วยรหัสผ่าน
3. ข้อมูลใช้ภายใน (Internal Use)	- คู่มือการปฏิบัติงาน (SOPs) - นโยบายบริษัท และผังองค์กร - บันทึกการประชุมภายในทั่วไป	พนักงานประจำและพนักงานสัญญาจ้างช องบริษัททุกคน	จัดเก็บในระบบแชร์ไฟล์ส่วนกลา งของบริษัท (Corporate Intranet / File Server)	อนุญาตให้ส่งผ่านอีเมลองค์กร ห้ามเผยแพร่สู่บุคคลภายนอก
4. ข้อมูลสาธารณะ (Public)	- เอกสารประชาสัมพันธ์บริษัท - ข้อมูลเผยแพร่บนเว็บไซต์ท างการ - ประกาศรับสมัครงาน	บุคคลภายนอกและสาธารณชนทั่วไป	จัดเก็บในระบบ Web Server หรือสื่อประชาสัมพันธ์	เผยแพร่ได้อย่างเปิดเผยผ่านช่องทาง ที่ได้รับอนุญาต

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 43 / 107
--	---	---

5. มาตรการเข้ารหัสข้อมูล (Encryption Policy Standards)

5.1 การเข้ารหัสข้อมูลขณะจัดเก็บ (Encryption at Rest)

- ฐานข้อมูลระบบ Bonanza Investment ต้องเปิดใช้งาน Transparent Data Encryption (TDE) หรือการเข้ารหัสระดับฟิลด์สำหรับข้อมูลอ่อนไหว
- คอมพิวเตอร์โน้ตบุ๊กและอุปกรณ์พกพาทุกเครื่อง ต้องเปิดใช้งาน BitLocker Drive Encryption (AES-256) เต็มรูปแบบ
- ไฟล์สำรองข้อมูล (Backup Archives) ที่ส่งไปเก็บยังศูนย์ข้อมูลภายนอก (INET Cloud หรือ True IDC) ต้องถูกเข้ารหัสด้วยรหัสผ่านความปลอดภัยสูงและอัลกอริทึม AES-256 ก่อนส่งออกจากระบบเสมอ

5.2 การเข้ารหัสข้อมูลขณะส่งผ่านเครือข่าย (Encryption in Transit)

- การเชื่อมต่อเข้าสู่ระบบภายในผ่านเครือข่ายภายนอก ต้องผ่านอุโมงค์สัญญาณเข้ารหัส FortiGate SSL-VPN หรือ IPsec VPN เท่านั้น
- การใช้งาน Web Applications และ Cloud Portal ทั้งหมด ต้องบังคับใช้โปรโตคอล HTTPS (TLS 1.3) และปิดการใช้งานโปรโตคอลเก่าที่ไม่ปลอดภัย (เช่น SSLv3, TLS 1.0, TLS 1.1)

6. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

1. GW-TMP-10: ทะเบียนทรัพย์สินข้อมูลและบันทึกกิจกรรมการประมวลผล (Data Asset & RoPA Register under PDPA)
2. นโยบายการติดฉลากข้อมูลความลับ (Sensitivity Labeling Policy Template)
3. รายงานบันทึกประวัติการเข้าถึงข้อมูลลับสูงสุด (Strictly Confidential Data Access Log)
4. ใบรับรองการทำลายข้อมูลความลับเมื่อครบอายุการจัดเก็บ (Data Destruction Certificate)

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 44 / 107
--	---	---

[GW-SOP-07] การใช้งานอุปกรณ์เคลื่อนที่และสื่อบันทึกข้อมูล

(Mobile Device & Removable Media Management Procedure)

รหัสเอกสาร	GW-SOP-07	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิป ก้านจักร IT Specialist	นายโสธชา ตั้งลิदानนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณฑลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

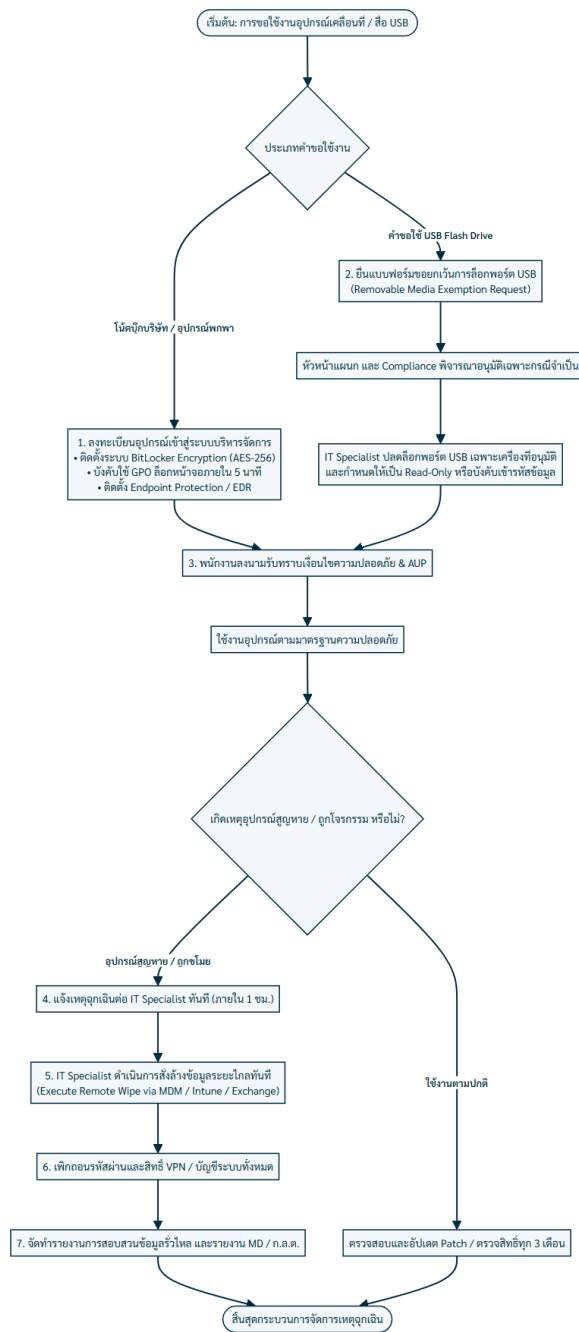
ระเบียบปฏิบัติงานฉบับนี้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยในการใช้งานอุปกรณ์คอมพิวเตอร์พกพา (โน้ตบุ๊ก, แท็บเล็ต, สมาร์ทโฟน) และสื่อบันทึกข้อมูลเคลื่อนที่ (USB Flash Drive, External Hard Drive) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- ป้องกันการรั่วไหลของข้อมูลความลับของลูกค้าและพอร์ตการลงทุนผ่านอุปกรณ์พกพาและพอร์ต USB
- ป้องกันภัยคุกคามจากมัลแวร์ ไวรัส หรือ Ransomware ที่อาจแพร่กระจายผ่านสื่อบันทึกข้อมูลภายนอก
- กำหนดขั้นตอนปฏิบัติเมื่ออุปกรณ์สูญหายหรือถูกโจรกรรม รวมถึงการสั่งล้างข้อมูลระยะไกล (Remote Wipe)
- ปฏิบัติตามประกาศ ก.ล.ต. สช. 38/2565 เรื่องการควบคุมอุปกรณ์สื่อสารและการเชื่อมต่อระบบสารสนเทศจากภายนอก

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมอุปกรณ์คอมพิวเตอร์โน้ตบุ๊กของบริษัท, อุปกรณ์ส่วนตัวที่ได้รับอนุญาตให้เชื่อมต่อบริษัท (Bring Your Own Device: BYOD), สื่อบันทึกข้อมูลแบบพกพาประเภท USB/External Storage, และการปฏิบัติงานนอกสถานที่ (Work from Home / Remote Working)

3. ฟังก์กระบวนการควบคุมอุปกรณ์เคลื่อนที่และสื่อบันทึกข้อมูล (Operational Process Flow)



รูปภาพ: ฟังก์กระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-07 การใช้งานอุปกรณ์เคลื่อนที่และสื่อบันทึกข้อมูล

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 46 / 107
--	---	---

4. มาตรการควบคุมความปลอดภัยอุปกรณ์เคลื่อนที่ (Mobile Device Security Controls)

4.1 การเข้ารหัสและการป้องกันทางกายภาพ (Encryption & Physical Security)

- เครื่องคอมพิวเตอร์โน้ตบุ๊กของบริษัททุกเครื่อง ต้องเปิดใช้งานการเข้ารหัสฮาร์ดดิสก์แบบ **BitLocker Drive Encryption (AES-256)** โดยอัตโนมัติ
- ต้องตั้งคำรหัสผ่านเข้าสู่ระบบ (PIN / Password) ที่มีความซับซ้อน และห้ามตั้งค่าให้เข้าสู่ระบบโดยอัตโนมัติ (Auto-login)
- บังคับใช้ระบบล็อกหน้าจออัตโนมัติ (Screen Lock Timeout) เมื่อไม่มีการใช้งานเกิน **5 นาที** ผ่านคำสั่ง Active Directory GPO

4.2 การควบคุมสื่อบันทึกข้อมูลเคลื่อนที่ (Removable Media Restriction via GPO)

- **นโยบายมาตรฐาน (Default Block Policy):** พอร์ต USB บนเครื่องคอมพิวเตอร์พนักงานทุกเครื่อง ต้องถูก **ปิดกั้นการเขียนข้อมูล (Block USB Write Access)** หรือบล็อกอุปกรณ์ USB Storage ทั้งหมดผ่าน Active Directory GPO
- หากพนักงานมีความจำเป็นต้องแลกเปลี่ยนข้อมูลกับภายนอก ให้ใช้บริการ Secure Cloud File Sharing ที่ได้รับอนุญาตของบริษัทแทน
- กรณีที่มีความจำเป็นอย่างยี่งวดทางธุรกิจ ต้องยื่นแบบฟอร์มขออนุมัติเป็นรายกรณี (Exception Request) และสื่อบันทึกข้อมูล USB นั้นต้องได้รับการสแกนไวรัสโดยฝ่าย IT ก่อนเสียบใช้งานทุกครั้ง

4.3 โพรโทคอลกรณีอุปกรณ์สูญหายหรือถูกโจรกรรม (Lost / Stolen Protocol)

- หากอุปกรณ์ของบริษัท หรืออุปกรณ์ที่มีข้อมูล/อีเมลบริษัทสูญหาย พนักงานต้องรายงานต่อ **ฝ่าย IT Specialist ทันทีภายในไม่เกิน 1 ชั่วโมง** นับแต่ทราบเหตุ
- ฝ่าย IT Specialist มีอำนาจสั่งการ **ล้างข้อมูลระยะไกล (Remote Wipe)** ผ่านระบบบริหารจัดการอุปกรณ์ เพื่อลบข้อมูลบริษัท อีเมล และการตั้งค่าเครือข่ายทั้งหมดออกจากตัวเครื่องทันที
- ฝ่าย IT ร่วมกับ Compliance ทำการประเมินว่ามีข้อมูลส่วนบุคคลของลูกค้าหรือข้อมูลความลับหลุดรอดหรือไม่ เพื่อดำเนินการรายงานตามเกณฑ์ PDPA และ ก.ล.ต. ต่อไป

5. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

1. **GW-TMP-11:** ทะเบียนลงทะเบียนอุปกรณ์เคลื่อนที่และพกพา (Mobile Device Registration Register)
2. **GW-TMP-12:** แบบฟอร์มขออนุญาตใช้งานสื่อบันทึกข้อมูลเคลื่อนที่ (Removable Media Exemption Request Form)
3. รายงานการสั่งล้างข้อมูลระยะไกลกรณีอุปกรณ์สูญหาย (Remote Wipe Execution Log)
4. รายงานผลการตรวจสอบอุปกรณ์พกพาประจำงวด (Quarterly Endpoint Security Audit Report)

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev.): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 47 / 107
--	---	--

[GW-SOP-08] การบันทึก จัดเก็บหลักฐาน และติดตามตรวจสอบ (Audit Log)

(Audit Logging, Monitoring & Evidence Retention Procedure)

รหัสเอกสาร	GW-SOP-08	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิป ก้านจักร IT Specialist	นายโสธชา ตั้งลิขิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุศลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดมาตรฐานการบันทึก บันทึก ฝ้าระวัง และเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log Files)

และร่องรอยการตรวจสอบการทุจริต (Audit Trails) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

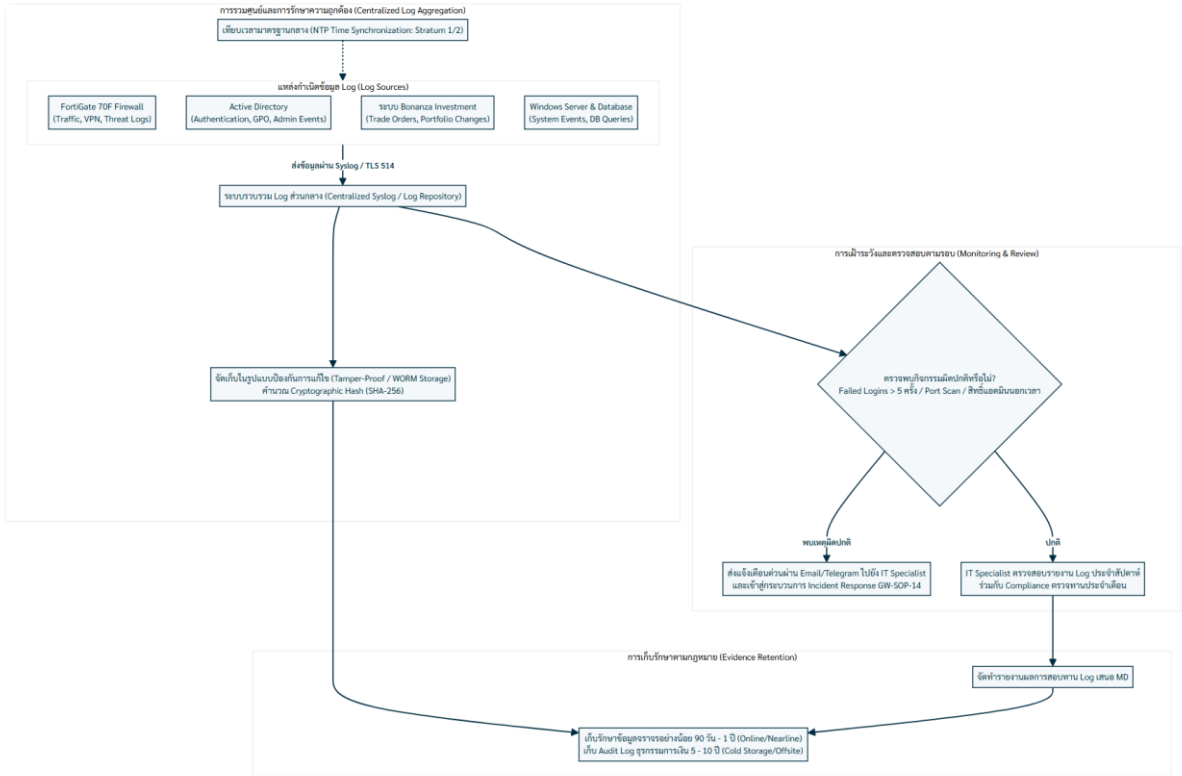
- รองรับการตรวจสอบย้อนหลังเมื่อเกิดเหตุการณ์ไม่พึงประสงค์ ข้อมูลรั่วไหล หรือการทุจริตในระบบจัดการกองทุน
- ป้องกันการแก้ไข ลบ หรือทำลายหลักฐานทางอิเล็กทรอนิกส์ (Evidence Tampering)
- ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และฉบับแก้ไขเพิ่มเติม) มาตรา 26 ซึ่งกำหนดให้เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า 90 วัน
- สอดคล้องกับประกาศ ก.ล.ต. สธ. 38/2565 และแนวปฏิบัติ นป. 6/2567
เรื่องการจัดเก็บหลักฐานการทำธุรกรรมและการเข้าถึงระบบสารสนเทศ

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมบันทึก Log จากแหล่งกำเนิดข้อมูลทั้งหมดของบริษัท ได้แก่:

- อุปกรณ์รักษาความปลอดภัยเครือข่าย: FortiGate 70F Firewall (Traffic Log, Security Event, VPN Login)
- ระบบพิสูจน์ตัวตนส่วนกลาง: Active Directory Domain Controller (Logon/Logoff, Kerberos, Privilege Use)
- ระบบจัดการกองทุนส่วนบุคคล: ระบบ Bonanza Investment (User Activity Log, Trade Execution, Account Modification)
- ระบบปฏิบัติการและเซิร์ฟเวอร์: Windows Server, Database Server, และ Syslog Server
- ระบบความปลอดภัยกายภาพ: บันทึกการเข้า-ออกห้อง Server Room One Bangkok และกล้อง CCTV

3. ผังกระบวนการบันทึก จัดเก็บ และตรวจสอบ Log (Operational Process Flow)



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-08 การบันทึก จัดเก็บหลักฐาน และติดตามตรวจสอบ (Audit Log)

4. รายการเหตุการณ์ที่ต้องเก็บบันทึก (Mandatory Audit Log Events)

ระบบงาน	รายการเหตุการณ์ที่ต้องบันทึก (Logged Events)	ระยะเวลาจัดเก็บขั้นต่ำ
FortiGate Firewall	- การเชื่อมต่อเครือข่ายเข้า-ออก (Traffic Session) - การพยายามล็อกอินเข้าใช้ VPN (สำเร็จ/ล้มเหลว) - การตรวจจับภัยคุกคาม IPS, Antivirus, และ Web Filter Block	1 ปี (Online ≥ 90 วัน)
Active Directory	- การเข้าสู่ระบบของพนักงาน (User Logon / Logoff) - การพยายามใส่รหัสผ่านผิดเกินกำหนด (Account Lockout) - การสร้าง ลบ หรือแก้ไขสิทธิ์บัญชีผู้ใช้ และสิทธิ์กลุ่มแอดมิน	1 ปี
ระบบ Bonanza Investment	- ประวัติการล็อกอินและการใช้งานของพนักงานทุกคน - คำสั่งซื้อขายหลักทรัพย์ (ผู้ส่ง, เวลา, ปริมาณ, ราคา) - การสร้าง แก้ไข หรือลบข้อมูลพอร์ตลูกค้า - การเปลี่ยนแปลงสิทธิ์ผู้ใช้งานบนระบบกองทุน	5 - 10 ปี (ตามกฎหมาย ก.ล.ต. ด้านพอร์ต)
ห้องแม่ข่าย (Server Room)	- บันทึกเวลาการสแกนใบหน้า/คีย์การ์ดเข้า-ออกประตู - สัญญาณเตือนอุณหภูมิ/ควันไฟ/ระบบไฟฟ้า UPS - ภาพบันทึกจากกล้องวงจรปิด CCTV	90 วัน (ภาพ CCTV) 1 ปี (Access Log ประตู)

5. มาตรการควบคุมความถูกต้องและความปลอดภัยของ Log (Log Integrity & Protection)

5.1 การเทียบเวลามาตรฐานสากล (Time Synchronization via NTP)

- เซิร์ฟเวอร์ อุปกรณ์เครือข่าย ไฟร์วอลล์ และเครื่องคอมพิวเตอร์ทั้งหมด
- ต้องตั้งค่าเทียบเวลากับแหล่งเวลามาตรฐานเดียวกันผ่านโปรโตคอล **Network Time Protocol (NTP)**
- ใช้แหล่งอ้างอิงเวลาแห่งชาติ เช่น `time.navy.mi.th` หรือ `time1.nimt.or.th` (สถาบันมาตรวิทยาแห่งชาติ)
- เพื่อให้เวลาในทุกระบบตรงกันในระดับมิลลิวินาที สามารถใช้เป็นพยานหลักฐานในชั้นศาลได้

5.2 การป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล Log (Tamper-Proof WORM Storage)

- ข้อมูล Log ที่ถูกส่งเข้ามายังระบบจัดเก็บส่วนกลาง ต้องถูกกำหนดสิทธิ์เป็น **อ่านอย่างเดียว (Read-Only)**
 - ห้ามผู้ดูแลระบบคนใด แม้กระทั่งบัญชี Admin สูงสุด ทำการแก้ไข แก้ต่าง หรือลบข้อความในไฟล์ Log โดยเด็ดขาด
 - มีการสร้างผลรวมตรวจสอบเชิงรหัสวิทยา (Cryptographic Hash: SHA-256) สำหรับไฟล์ Log ประจำวัน
- เพื่อพิสูจน์ความแท้จริงว่าไม่มีการดัดแปลงย้อนหลัง

5.3 วงจรการตรวจสอบและวิเคราะห์ Log (Log Review Routine)

- การตรวจสอบรายวัน (Daily Review):** IT Specialist ตรวจสอบแจ้งเตือนจากระบบเกี่ยวกับความพยายามเจาะระบบ การล็อกอินผิดพลาดซ้ำๆ และสถานะของไฟร์วอลล์

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 50 / 107
--	--	---

- **การสอบทานประจำเดือน (Monthly Formal Review):** IT Specialist สรุปรายงานพฤติกรรมการใช้งานระบบ Bonanza และการใช้สิทธิ์แอตมิน เพื่อให้ฝ่าย Compliance และ MD ลงนามรับทราบ

6. **แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)**

1. **GW-TEC-05:** ข้อกำหนดรูปแบบการจัดเก็บ Log ระบบกองทุน (Bonanza Activity Log Technical Specification)
2. รายงานสรุปผลการสอบทานบันทึกข้อมูลจราจรประจำเดือน (Monthly Log Review Report)
3. บันทึกผลการเทียบเวลามาตรฐาน (NTP Synchronization Status Report)
4. รายงานการสำรองไฟล์ Log ประจำรอบเพื่อการเก็บรักษาระยะยาว (Long-Term Log Archive Manifest)

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 51 / 107
--	---	---

[GW-SOP-09] การบริหารการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ (Change)

รหัสเอกสาร	GW-SOP-09	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาสีลป์ ก้านจักร IT Specialist	นายโสธรา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

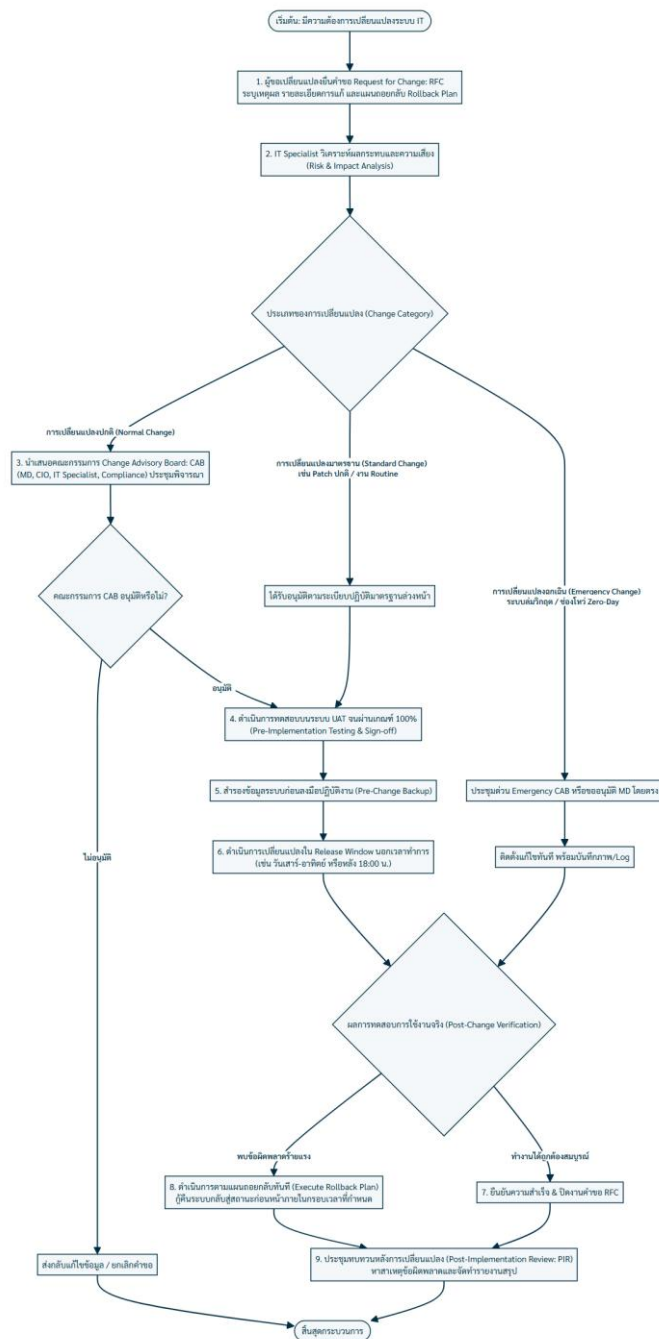
ระเบียบปฏิบัติงานฉบับนี้กำหนดกรอบกระบวนการบริหารจัดการ ควบคุม ทดสอบ และอนุมัติการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ (IT Change Management) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- ป้องกันผลกระทบหรือความขัดข้องที่อาจเกิดขึ้นต่อระบบการจัดการกองทุนหลัก (ระบบ Bonanza Investment) และการทำธุรกรรมของลูกค้า
- มั่นใจว่าทุกการเปลี่ยนแปลงได้รับการทดสอบอย่างเพียงพอบนสภาพแวดล้อมทดสอบ (UAT) และมีแผนรองรับการถอยกลับ (Rollback Plan) อย่างชัดเจน
- กำหนดให้มีคณะกรรมการพิจารณาการเปลี่ยนแปลง (Change Advisory Board: CAB) ในการกลั่นกรองและอนุมัติอย่างเป็นทางการ
- ปฏิบัติตามมาตรฐาน ISO/IEC 27001 และประกาศ ก.ล.ต. สช. 38/2565 เรื่องการควบคุมการเปลี่ยนแปลงระบบงานสำคัญ

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมการเปลี่ยนแปลงระบบฮาร์ดแวร์, ระบบปฏิบัติการ, กฎไฟร์วอลล์ (FortiGate Policy), การอัปเกรดเวอร์ชันซอฟต์แวร์ Bonanza, การแก้ไขโครงสร้างฐานข้อมูล (Database Schema), โครงสร้างพื้นฐานระบบเครือข่าย และระบบ Cloud Backup ทั้งหมด

3. ฟังก์กระบวนการบริหารการเปลี่ยนแปลงระบบ (Operational Process Flow)



รูปภาพ: ฟังก์กระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-09 การบริหารการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ (Change)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 53 / 107
--	--	---

4. ประเภทของการเปลี่ยนแปลง (Categories of IT Change)

1. การเปลี่ยนแปลงมาตรฐาน (Standard Change):

- เป็นการเปลี่ยนแปลงที่มีความเสี่ยงต่ำ เป็นงานประจำ และมีขั้นตอนชัดเจน เช่น การเพิ่ม VLAN สำหรับแผนกใหม่ตามมาตรฐานเดิม, การอัปเดต Signature ของ Antivirus/IPS บน FortiGate
- สามารถดำเนินการได้โดย IT Specialist โดยไม่ต้องผ่านที่ประชุม CAB ทุกครั้ง แต่ต้องบันทึกประวัติการเปลี่ยนแปลง

2. การเปลี่ยนแปลงปกติ (Normal Change):

- การเปลี่ยนแปลงที่ส่งผลกระทบต่อระบบงานสำคัญ มีความเสี่ยงปานกลางถึงสูง เช่น การอัปเกรดเวอร์ชันระบบ Bonanza Investment, การเปลี่ยน Core Switch, การปรับปรุง Firewall Rule หลัก, การย้ายเซิร์ฟเวอร์
 - ต้องผ่านการประเมินความเสี่ยง ยื่นเอกสาร RFC และได้รับอนุมัติจากคณะกรรมการ CAB
- เป็นลายลักษณ์อักษรล่วงหน้าอย่างน้อย 3 วันทำการ

3. การเปลี่ยนแปลงฉุกเฉิน (Emergency Change):

- การเปลี่ยนแปลงเพื่อกู้คืนระบบที่หยุดชะงักอย่างรุนแรง (System Outage) หรือการติดตั้ง Patch เพื่ออุดช่องโหว่ความปลอดภัยระดับวิกฤต (Zero-Day Exploit)
- สามารถขออนุมัติด้วยวาจาหรือข้อความอิเล็กทรอนิกส์จากกรรมการผู้จัดการ (MD) หรือประธาน CAB และต้องจัดทำเอกสารบันทึกย้อนหลัง (Post-Documentation) ภายใน 24 ชั่วโมง

5. องค์ประกอบสำคัญของคำขอเปลี่ยนแปลง (Mandatory RFC Requirements)

ทุกคำขอเปลี่ยนแปลงระดับ Normal Change ต้องมีเอกสารประกอบครบถ้วน 4 รายการ:

- รายละเอียดทางเทคนิค (Technical Details):** ระบุเหตุผล ระบบที่ได้รับผลกระทบ วันและเวลาดำเนินการ
- ผลการทดสอบบน UAT (UAT Test Results):** หลักฐานการทดสอบบนสภาพแวดล้อมจำลองที่แยกจากระบบจริง พร้อมลายมือชื่อตรวจรับจากเจ้าของระบบ (Business Owner Sign-off)
- แผนการถอยกลับ (Rollback Plan):** ลำดับขั้นตอนและเวลาที่ใช้ในการกู้ระบบกลับสู่สถานะเดิม หากเกิดเหตุขัดข้องระหว่างติดตั้ง โดยต้องกำหนดจุดตัดสินใจถอยกลับ (Go / No-Go Decision Point)
- การสำรองข้อมูลล่วงหน้า (Pre-Implementation Backup):** ต้องทำการสำรองข้อมูลฐานข้อมูลและ Configuration ของระบบก่อนลงมือดำเนินการทุกครั้ง

6. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

- GW-TMP-13:** แบบฟอร์มขอเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ (Request for Change: RFC Form)
- รายงานการประชุมคณะกรรมการพิจารณาการเปลี่ยนแปลง (Change Advisory Board: CAB Minutes)
- เอกสารรับรองผลการทดสอบระบบ (UAT Sign-off Certificate)
- รายงานการทบทวนหลังการเปลี่ยนแปลง (Post-Implementation Review: PIR Report)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 54 / 107
--	--	---

[GW-SOP-10] การพัฒนาระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย (Secure SDLC)

(Secure System Development Life Cycle Procedure: Secure SDLC)

รหัสเอกสาร	GW-SOP-10	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิป ก้านจักร IT Specialist	นายโสธชา ตั้งลิदानนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

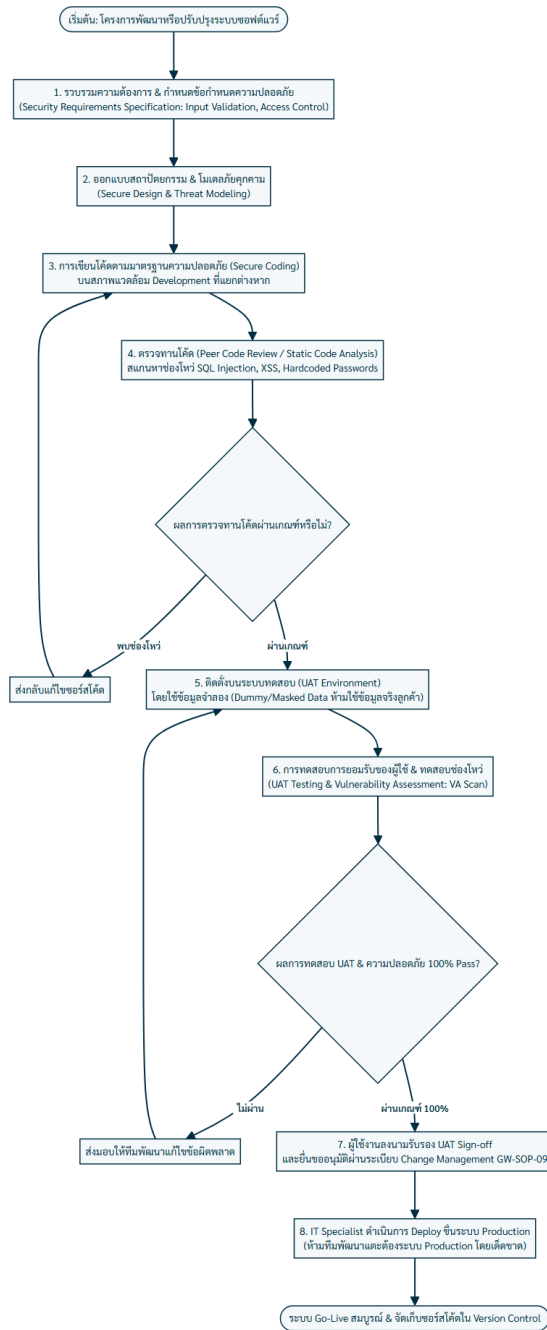
ระเบียบปฏิบัติงานฉบับนี้กำหนดกรอบการพัฒนา ปรับปรุง และบำรุงรักษาระบบซอฟต์แวร์ แอปพลิเคชัน สคริปต์อัตโนมัติ และการปรับแต่งระบบจัดการกองทุน (Customization on Bonanza System) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- ป้องกันช่องโหว่ความปลอดภัยตามมาตรฐานสากล (เช่น OWASP Top 10) ตั้งแต่ขั้นตอนการออกแบบและการเขียนโค้ด (Security by Design & Security by Default)
- กำหนดการแบ่งแยกสภาพแวดล้อมระบบพัฒนา (Development), ระบบทดสอบ (UAT), และระบบใช้งานจริง (Production) อย่างเด็ดขาด
- บังคับใช้การแบ่งแยกหน้าที่ (SoD) โดยห้ามผู้พัฒนาโปรแกรมมีสิทธิ์นำโค้ดขึ้นระบบใช้งานจริงด้วยตนเอง
- สอดคล้องกับประกาศ ก.ล.ต. สธ. 38/2565 เรื่องการควบคุมวงจรชีวิตการพัฒนาระบบเทคโนโลยีสารสนเทศ

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมการพัฒนาโปรแกรมภายในองค์กร (In-house Development), การเขียนสคริปต์เชื่อมต่อ API, การปรับแต่งโมดูลของระบบ Bonanza Investment, และการว่าจ้างบริษัทภายนอก (Software Vendor / SI) พัฒนาระบบให้แก่บริษัท

3. ฟังก์ชันการพัฒนาระบบอย่างปลอดภัย (Operational Process Flow)



รูปภาพ: ฟังก์ชันการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-10 การพัฒนาระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย (Secure SDLC)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 56 / 107
--	--	---

4. เสาหลักการพัฒนากระบวนการอย่างปลอดภัย 5 ประการ (Core Secure SDLC Controls)

4.1 การแบ่งแยกสภาพแวดล้อมระบบ (Strict Separation of Environments)

- บริษัทต้องแบ่งแยกสภาพแวดล้อมระบบออกเป็น 3 ระดับอย่างเด็ดขาด:
 1. Development Environment (Dev): สภาพแวดล้อมสำหรับเขียนโค้ดและทดสอบเบื้องต้น
 2. User Acceptance Testing Environment (UAT): สภาพแวดล้อมจำลองเหมือนระบบจริงสำหรับผู้ใช้ทดสอบ
 3. Production Environment (Prod): สภาพแวดล้อมจริงที่มีข้อมูลทรัพย์สินลูกค้าและคำสั่งซื้อขาย
- มีระบบไฟร์วอลล์ (FortiGate) กั้นระหว่างแต่ละสภาพแวดล้อมอย่างชัดเจน

4.2 การคุ้มครองข้อมูลที่ใช้ในการทดสอบ (Test Data Privacy)

- ห้ามนำข้อมูลจริงของลูกค้า (เช่น เลขบัตรประชาชน, เลขบัญชีธนาคาร, พอร์ตการลงทุน) มาใช้ในการทดสอบระบบบน Dev หรือ UAT โดยเด็ดขาด
- หากจำเป็นต้องใช้ข้อมูลที่มีโครงสร้างเหมือนจริง ต้องผ่านกระบวนการแปลงข้อมูลเพื่อปกปิดตัวตน (Data Masking / Anonymization) ตามเกณฑ์ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)

4.3 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties: SoD)

- นักพัฒนาซอฟต์แวร์ (Developers) หรือบริษัทคู่ค้าภายนอก **ต้องไม่มีสิทธิ์เข้าถึง (No Direct Access)** เซิร์ฟเวอร์และฐานข้อมูลระบบ Production
- การนำซอฟต์แวร์ขึ้นระบบ Production ต้องดำเนินการโดย ฝ่ายเทคโนโลยีสารสนเทศ เท่านั้น หลังจากได้รับเอกสารอนุมัติจากคณะกรรมการ CAB ครบถ้วน

4.4 การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment & PenTest)

- ก่อนที่จะนำระบบงานใหม่ขึ้นใช้งานจริง หรือเมื่อมีการปรับปรุงระบบ Bonanza ครั้งใหญ่ ต้องจัดให้มีการสแกนหาช่องโหว่ (Vulnerability Assessment) และ/หรือ การทดสอบเจาะระบบ (Penetration Testing) โดยผู้เชี่ยวชาญด้านความปลอดภัย
- หากพบช่องโหว่ระดับ High หรือ Critical ต้องดำเนินการแก้ไขและทดสอบซ้ำจนปลอดภัย 100% ก่อนได้รับอนุญาตให้เปิดใช้งาน

4.5 การจัดเก็บซอร์สโค้ด (Source Code Repository & Version Control)

- ซอร์สโค้ดและสคริปต์ของบริษัททั้งหมด ต้องจัดเก็บในระบบควบคุมเวอร์ชันที่ปลอดภัย (Secure Version Control เช่น Private Git) มีการเข้ารหัส และกำหนดสิทธิ์เข้าถึงเฉพาะผู้ที่เกี่ยวข้อง
- มีการสำรองข้อมูลซอร์สโค้ดเป็นประจำตามนโยบายการสำรองข้อมูลของบริษัท

5. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

1. GW-TMP-14: แบบฟอร์มขออนุมัติโครงการและข้อกำหนดความปลอดภัยของระบบ (System Security Requirements Specification)
2. รายงานผลการตรวจทานโค้ด (Code Review Checklist & Sign-off)

 GRANDWAY บจ. แกรนด์เวย์ แคปปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 57 / 107
---	---	---

3. เอกสารการตรวจรับผลการทดสอบระบบ (UAT Acceptance Certificate)
4. รายงานผลการสแกนช่องโหว่ความปลอดภัยก่อนขึ้นระบบจริง (Pre-Deployment Vulnerability Assessment Report)

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 58 / 107
--	--	---

[GW-SOP-11] การสำรองข้อมูลและการทดสอบกู้คืน (3-2-1 Backup & Restore)

(Backup & Data Restoration Procedure)

รหัสเอกสาร	GW-SOP-11	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิป ก้านจักร IT Specialist	นายโสรชา ตั้งลิदानนท์ Chief Investment Officer (CIO) / Compliance	นายเอกฉัตร ภูมชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดมาตรฐานและขั้นตอนการสำรองข้อมูล (Data Backup) การจัดเก็บข้อมูลสำรองนอกสถานที่ (Offsite Cloud Replication) และการซึ่กซ้อมทดสอบกู้คืนข้อมูล (Restore Drill) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- ป้องกันการสูญหายของข้อมูลพอร์ตการลงทุน ฐานข้อมูลลูกค้า และการตั้งค่าระบบ จากภัยคุกคามไซเบอร์ (เช่น Ransomware), อุปกรณ์ฮาร์ดแวร์ชำรุด หรือภัยพิบัติ
- กำหนดเป้าหมายเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) ไม่เกิน **4 ชั่วโมง** และเป้าหมายการสูญเสยข้อมูลสูงสุด (Recovery Point Objective: RPO) ไม่เกิน **24 ชั่วโมง**
- บังคับใช้กลยุทธ์การสำรองข้อมูลมาตรฐานสากล **3-2-1 Backup Strategy**
- สอดคล้องกับประกาศ ก.ล.ต. สธ. 38/2565 และแนวปฏิบัติ นป. 6/2567
เรื่องการสำรองข้อมูลและการเตรียมความพร้อมเพื่อการกู้คืนระบบสารสนเทศ

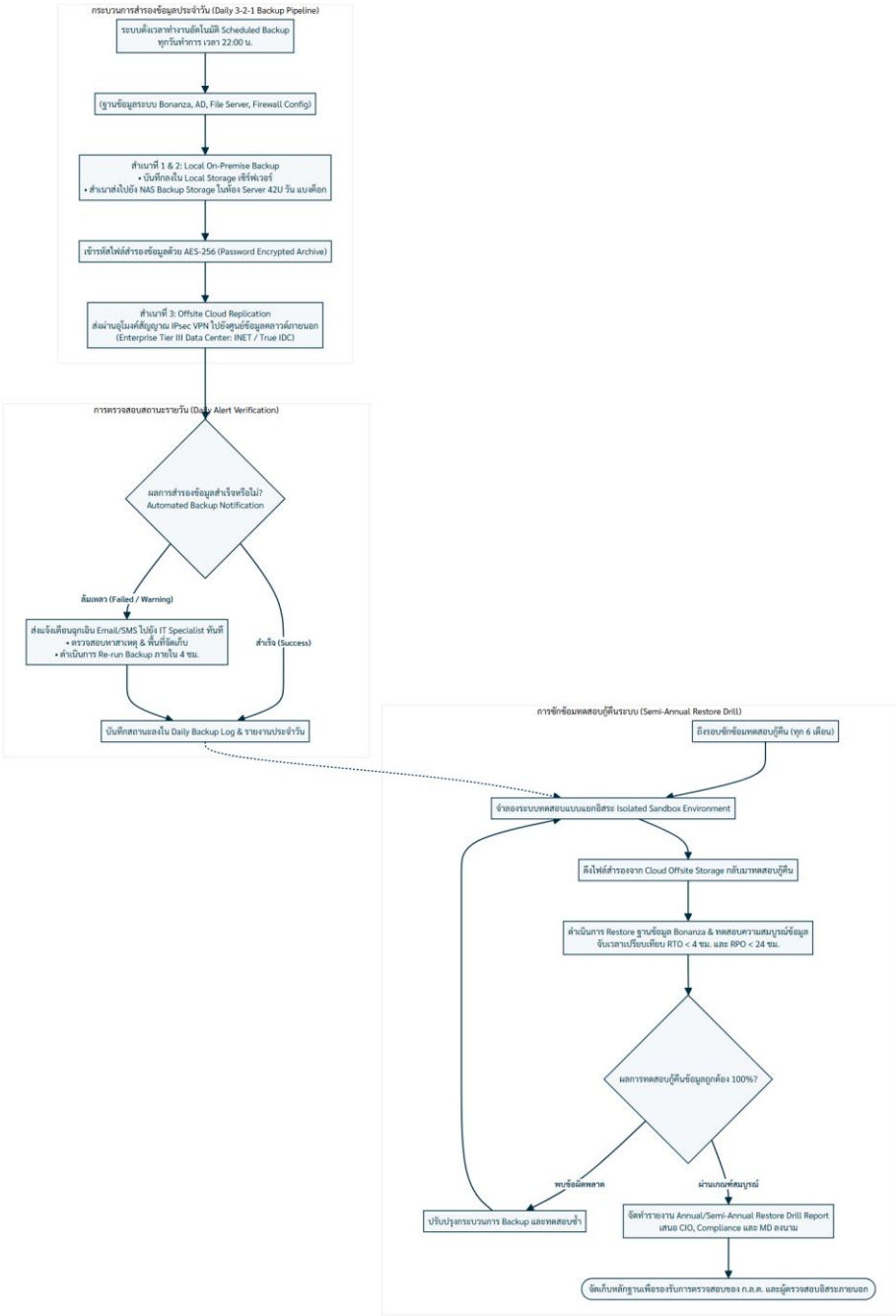
2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมข้อมูลและระบบงานสำคัญทั้งหมดของบริษัท:

- ฐานข้อมูลและโปรแกรมระบบจัดการกองทุนส่วนบุคคล: **ระบบ Bonanza Investment (SQL Database & Transaction Logs)**
- สภาพแวดล้อมระบบพิสูจน์ตัวตน: **Active Directory System State & GPO**
- ระบบจัดเก็บไฟล์ข้อมูลเอกสารสัญญาและบัญชี: **Corporate File Server**
- ค่าคอนฟิกูเรชันอุปกรณ์เครือข่ายและความปลอดภัย: **FortiGate 70F Firewall Config & UniFi Controller Config**

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 59 / 107
---	--	--

3. ผังกระบวนการสำรองข้อมูลและทดสอบกู้คืน (Operational Process Flow)



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-11 การสำรองข้อมูลและการทดสอบกู้คืน (3-2-1 Backup & Restore)

4. ตารางกำหนดการสำรองข้อมูลและระยะเวลาจัดเก็บ (Backup & Retention Schedule)

ลำดับ	รายการระบบ / ข้อมูล	วิธีการสำรองข้อมูล	ความถี่ในการสำรอง	สำรองในศูนย์ข้อมูล One Bangkok	สำรองบนระบบคลาวด์ภายนอก (Offsite)	ระยะเวลาเก็บรักษา (Retention)
1	ฐานข้อมูล Bonanza Investment	Full + Transaction Log	ทุกวัน (22:00 น.) / Log ทุกชั่วโมง	NAS Storage (RAID)	INET / True IDC Cloud Storage	รายวัน 30 วัน / รายเดือน 12 เดือน / ล้างปี 5-10 ปี
2	Active Directory & System State	System State Backup	สัปดาห์ละครั้ง (ทุกวันอาทิตย์)	NAS Storage	Cloud Storage	เก็บย้อนหลัง 12 สัปดาห์
3	File Server (เอกสารสำคัญ/สัญญา)	Incremental รายวัน / Full รายสัปดาห์	ทุกวันทำการ (23:00 น.)	NAS Storage	Cloud Storage	เก็บย้อนหลัง 1 ปี
4	FortiGate & Switch Config	Configuration Export	ทุกครั้งที่มีการแก้ไข + Change + ทุกสัปดาห์	Local IT Repository	Cloud Storage	ตลอดอายุการใช้งานอุปกรณ์

5. การบังคับใช้กลยุทธ์ 3-2-1 และการรักษาความปลอดภัย (3-2-1 Implementation & Security)

5.1 เสาหลัก 3-2-1 Backup Strategy

- 1. สำเนาข้อมูล 3 ชุด: ข้อมูลจริงบนเซิร์ฟเวอร์ + สำเนา Local Backup + สำเนา Cloud Offsite Backup
- 2. สื่อบันทึกข้อมูล 2 ประเภท: จัดเก็บใน Local SSD/HDD Server และบน Cloud Object/Block Storage
- 3. จัดเก็บนอกสถานที่ 1 ชุด (Offsite Copy): ส่งข้อมูลสำรองไปยังศูนย์ข้อมูลภายนอก (Enterprise Tier III Data Center ในประเทศไทย) ป้องกันกรณีเกิดเพลิงไหม้ น้ำท่วม หรืออาคาร One Bangkok ได้รับความเสียหาย

5.2 การป้องกันภัยคุกคาม Ransomware แบบ Immutable Backup

- ข้อมูลสำรองบนระบบคลาวด์ต้องเปิดใช้งานฟังก์ชัน **Object Lock (Immutable Storage / WORM)** ที่ห้ามแก้ไข ดัดแปลง หรือลบไฟล์ก่อนครบกำหนดอายุจัดเก็บ เพื่อป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสทำลายไฟล์สำรอง

5.3 การซักซ้อมทดสอบกู้คืนระบบ (Semi-Annual Restoration Drill)

- ฝ่าย IT ต้องจัดให้มีการทดสอบกู้คืนข้อมูลจริง (Restore Test) อย่างน้อยปีละ 2 ครั้ง (ทุก 6 เดือน)
- การทดสอบต้องกู้คืนฐานข้อมูลระบบ Bonanza ลงในเครื่องทดสอบ ตรวจสอบความถูกต้องของตารางพอร์ตการลงทุน (Integrity Check) และจับเวลาเปรียบเทียบกับเกณฑ์ RTO / RPO
- ต้องจัดทำ รายงานผลการซักซ้อมกู้คืนระบบ (Restore Drill Report) เสนอต่อคณะกรรมการกำกับดูแลด้าน IT และผู้บริหารลงนาม

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 61 / 107
--	--	---

6. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

- 1. GW-TEC-03: ข้อกำหนดการตั้งค่าระบบสำรองข้อมูลคลาวด์และการแจ้งเตือน (Offsite Cloud Backup & Notification Spec)
- 2. บันทึกรายงานสถานะการสำรองข้อมูลประจำวัน (Daily Backup Log & Email Notification Reports)
- 3. รายงานผลการซักซ้อมทดสอบกู้คืนระบบประจำปี (Semi-Annual Data Restoration Drill Report)
- 4. ทะเบียนประวัติไฟล์สำรองข้อมูลระยะยาว (Long-Term Archive Register)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev.): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 62 / 107
--	---	--

[GW-SOP-12] แผนรับมือเหตุการณ์ฉุกเฉินและกู้คืนระบบจากภัยพิบัติ (IT DRP)

รหัสเอกสาร	GW-SOP-12	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาสีลป์ ก้านจักร IT Specialist	นายโสธรา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุลชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

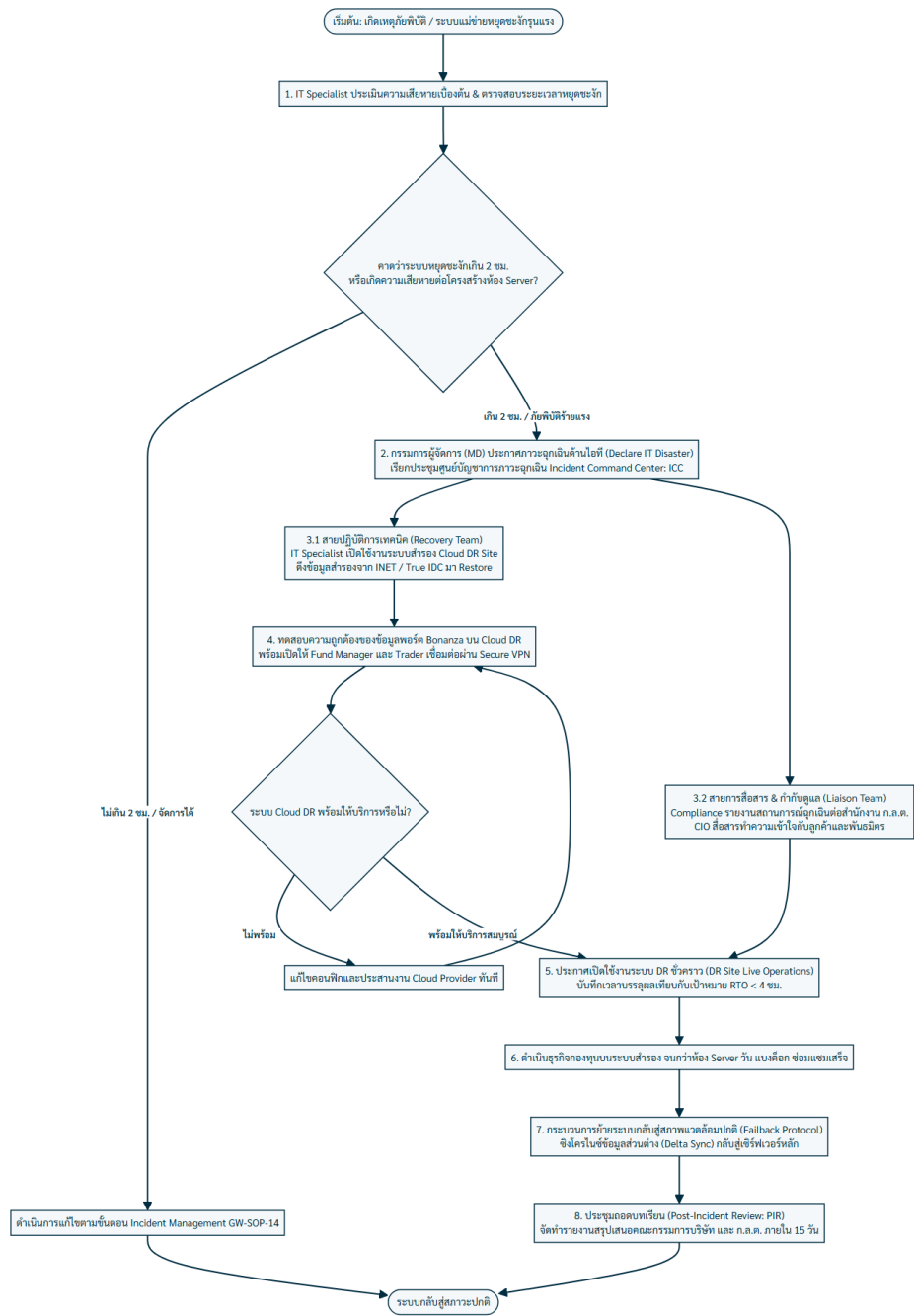
ระเบียบปฏิบัติงานฉบับนี้จัดทำขึ้นเพื่อกำหนดโครงสร้างการบัญชาการ ขั้นตอนการปฏิบัติการฉุกเฉิน และแผนกู้คืนระบบเทคโนโลยีสารสนเทศจากภัยพิบัติ (Disaster Recovery Plan: DRP) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- ตอบสนองต่อภาวะฉุกเฉิน ภัยพิบัติธรรมชาติ เหตุเพลิงไหม้ เหตุวินาศกรรม และภัยคุกคามทางไซเบอร์ร้ายแรงอย่างมีระบบ รวดเร็ว และปลอดภัย
- กู้คืนระบบงานหลักด้านการจัดการกองทุนส่วนบุคคล (ระบบ Bonanza Investment) ให้กลับมาดำเนินงานได้ตามเป้าหมายเวลาการฟื้นฟูระบบ (RTO < 4 ชั่วโมง) และจำกัดการสูญหายของข้อมูล (RPO < 24 ชั่วโมง)
- กำหนดสายการบังคับบัญชาฉุกเฉิน (Incident Command Structure) และการสื่อสารต่อผู้ลงทุนและหน่วยงานกำกับดูแล
- ปฏิบัติตามประกาศ ก.ล.ต. สช. 38/2565 และแนวปฏิบัติ นป. 6/2567
เรื่องการเตรียมความพร้อมด้านเทคโนโลยีสารสนเทศเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

2. ขอบเขตการบังคับใช้ (Scope)

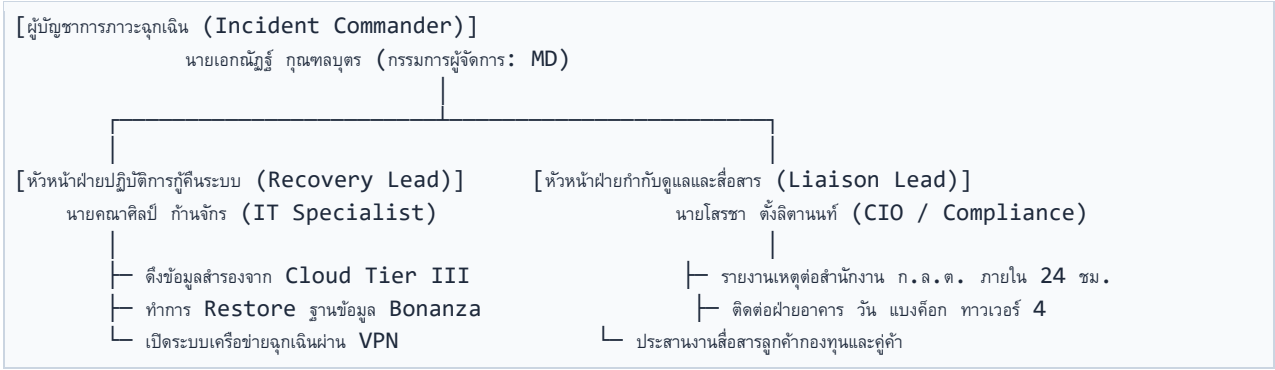
ครอบคลุมเหตุการณ์วิกฤตที่ส่งผลกระทบต่อห้องแม่ข่ายคอมพิวเตอร์ (Server Room 42U ชั้น 38 อาคาร วัน แบงค็อก ทาวเวอร์ 4), ระบบไฟฟ้าและปรับอากาศอาคาร, ระบบเครือข่ายอินเทอร์เน็ตสำนักงานใหญ่, และเซิร์ฟเวอร์ระบบ Bonanza Investment ทั้งหมด

3. ฟังก์กระบวนการบัญชาการและกู้คืนระบบจากภัยพิบัติ (Operational Process Flow)



รูปภาพ: ฟังก์กระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-12 แผนรับมือเหตุการณ์ฉุกเฉินและกู้คืนระบบจากภัยพิบัติ (IT DRP)

4. โครงสร้างศูนย์บัญชาการภาวะฉุกเฉิน (Incident Command Structure: ICS)



5. เกณฑ์เป้าหมายการกู้คืนระบบ (RTO & RPO Targets)

ระบบงาน (System Category)	ระดับความสำคัญ (Tier)	เป้าหมาย RTO (ระยะเวลาฟื้นฟูระบบ)	เป้าหมาย RPO (การสูญเสียข้อมูลสูงสุด)	แผนรองรับเมื่อเกิดภัยพิบัติ (DR Strategy)
ระบบจัดการกองทุน Bonanza (Core System)	Tier 1 (Mission-Critical)	< 4 ชั่วโมง	< 1 ชั่วโมง (Transaction Log) < 24 ชั่วโมง (Daily Snapshot)	Standby Cloud DR บน Tier III Data Center (INET / True IDC) กู้คืนผ่าน Script อัตโนมัติ
ระบบ Active Directory & Identity	Tier 1	< 2 ชั่วโมง	< 24 ชั่วโมง	Secondary AD Domain Controller บนคลาวด์ พร้อม Standby รองรับการยืนยันตัวตน
ระบบไฟร์วอลล์และเครือข่ายสำนักงาน	Tier 1	< 1 ชั่วโมง	0 นาที (Real-time Config)	อุปกรณ์สำรอง FortiGate Configuration Cloud Backup และท่อสำรอง Leased Line/4G Failover
ระบบ File Share และเอกสารทั่วไป	Tier 2 (Important)	< 8 ชั่วโมง	< 24 ชั่วโมง	ดึงข้อมูลสำรองจาก Offsite Cloud Backup

6. ขั้นตอนการปฏิบัติการกู้คืนระบบ (Step-by-Step Recovery Procedure)

ขั้นตอนที่ 1: การประเมินสถานการณ์และการประกาศภาวะฉุกเฉิน (Assessment & Declaration)

- เมื่อเซิร์ฟเวอร์หลักหยุดทำงาน หรือระบบไฟ/แอร์ห้อง Server One Bangkok ชัดข้อง IT Specialist เข้าตรวจสอบสถานะฮาร์ดแวร์และ UPS ทันที
- หากประเมินว่าระบบหลักไม่สามารถกู้คืนได้ภายใน 2 ชั่วโมง ให้รายงานต่อกรรมการผู้จัดการ (MD) ทันที

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 65 / 107
--	--	---

3. กรรมการผู้จัดการประกาศใช้ **แผนกู้คืนระบบจากภัยพิบัติ (Declare IT DRP)** อย่างเป็นทางการ และระดมทีม Incident Command

ขั้นตอนที่ 2: การเปิดใช้งานระบบสำรองบนคลาวด์ (Failover to Cloud DR)

- IT Specialist ล็อกอินเข้าสู่ระบบบริหารจัดการศูนย์ข้อมูลคลาวด์สำรอง (INET / True IDC) ผ่านช่องทางบริหารจัดการเฉพาะ (Out-of-Band Management)
- ดึง Snapshot ฐานข้อมูลและ Transaction Log ล่าสุดของระบบ Bonanza มาทำการ Mount และ Restore ลงใน Virtual Server สำรอง
- ตรวจสอบความถูกต้องของยอดคงเหลือและพอร์ตการลงทุน (Integrity Check)
- เปิดใช้งานเส้นทางเชื่อมต่อ Secure SSL-VPN ให้พนักงานกลุ่มผู้จัดการกองทุนและเทรดเดอร์เข้าใช้งานจากสถานที่ทำงานสำรอง (Alternative Site / WFH)

ขั้นตอนที่ 3: การสื่อสารและการรายงานตามกฎหมาย (Communication & Reporting)

- ฝ่าย Compliance จัดทำหนังสือแจ้งเหตุขัดข้องของระบบเทคโนโลยีสารสนเทศอย่างเป็นทางการต่อ **สำนักงาน ก.ล.ต. ภายใน 24 ชั่วโมง** นับจากเกิดเหตุ
- ฝ่ายการลงทุน (CIO) สื่อสารสถานะการดำเนินงานต่อผู้ลงทุนและสถาบันผู้รับฝากทรัพย์สิน (Custodian) เพื่อสร้างความเชื่อมั่น

ขั้นตอนที่ 4: การย้ายระบบกลับคืนสู่สภาวะปกติ (Failback Protocol)

- เมื่อห้องแม่ข่าย ณ อาคาร วัน แบงค็อก กลับสู่สภาพสมบูรณ์และผ่านการตรวจรับความปลอดภัย
- ดำเนินการนอกเวลาทำการ (หลัง 18:00 น. หรือวันหยุดสุดสัปดาห์): หยุดการทำธุรกรรมบน Cloud DR ชั่วคราว
- ซิงโครไนซ์ข้อมูลธุรกรรมใหม่ทั้งหมดที่เกิดขึ้นระหว่างใช้งาน DR กลับมายังเซิร์ฟเวอร์หลัก (Differential Synchronization)
- ทดสอบความถูกต้องของฐานข้อมูล Bonanza บนเซิร์ฟเวอร์หลัก และเปิดระบบให้บริการตามปกติ

7. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

- GW-TMP-15:** บันทึกการประกาศภาวะฉุกเฉินและรายงานสรุปการกู้คืนระบบ (IT DRP Activation & Incident Summary Report)
- แบบฟอร์มการสื่อสารภาวะฉุกเฉินต่อสำนักงาน ก.ล.ต. (SEC Incident Notification Form)
- รายงานบันทึกเวลาการกู้คืนระบบจริงเทียบกับ RTO/RPO (Actual Recovery Performance Log)
- รายงานการประชุมทบทวนและถอดบทเรียนหลังเหตุการณ์ (Post-Incident Review Meeting Minutes)

[GW-SOP-13] การบริหารจัดการผู้ให้บริการภายนอกด้านไอที (IT Outsourcing)

รหัสเอกสาร	GW-SOP-13	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุลชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

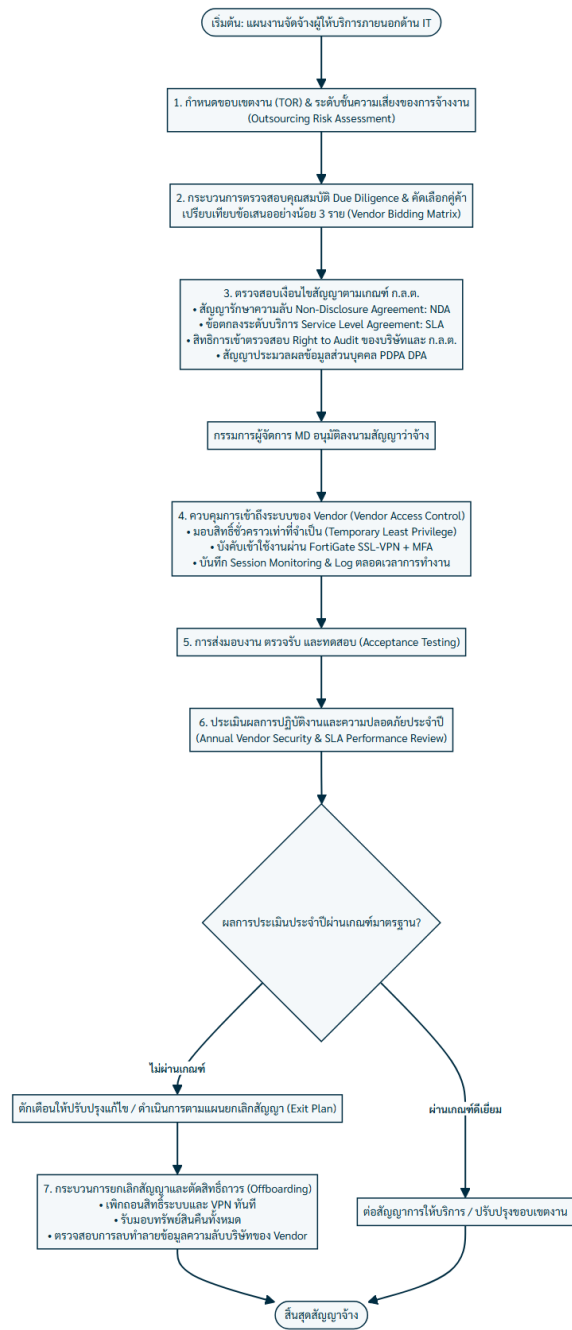
ระเบียบปฏิบัติงานฉบับนี้กำหนดกรอบการคัดเลือก ควบคุม กำกับดูแล และประเมินผลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcers / Vendors / Contractors) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- 1. ป้องกันความเสี่ยงจากการพึ่งพาผู้ให้บริการภายนอก (Vendor Concentration & Dependency Risk)
 - 2. มั่นใจว่าคู่ค้าภายนอกปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศของบริษัทและการคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด
 - 3. กำหนดให้มีสัญญาข้อตกลงระดับการให้บริการ (SLA) และเงื่อนไขสิทธิการเข้าตรวจสอบ (Right to Audit)
 - 4. สอดคล้องกับประกาศ ก.ล.ต. สธ. 38/2565 และประกาศแนวปฏิบัติ นป. 6/2567
- เรื่องการใช้บริการเทคโนโลยีสารสนเทศจากผู้รับดำเนินการภายนอก

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมคู่ค้าผู้ให้บริการด้าน IT ทุกประเภท ได้แก่: ผู้พัฒนาระบบและดูแลซอฟต์แวร์กองทุน Bonanza, ผู้ให้บริการศูนย์ข้อมูลและคลาวด์ (Cloud/Colocation เช่น INET / True IDC), ผู้รับเหมาติดตั้งระบบเครือข่ายและห้องแม่ข่าย (SI Vendor One Bangkok), ผู้ให้บริการวงจรรีโมต (ISP), และที่ปรึกษาด้านเทคโนโลยีสารสนเทศภายนอก

3. ฟังก์ชันการกำกับดูแลผู้ให้บริการภายนอก (Operational Process Flow)



รูปภาพ: ฟังก์ชันการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-13 การบริหารจัดการผู้ให้บริการภายนอกด้านไอที (IT Outsourcing)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 68 / 107
--	---	---

4. มาตรการควบคุมความปลอดภัยในการจ้างผู้รับดำเนินการภายนอก (Mandatory Controls)

4.1 ข้อกำหนดในสัญญาว่าจ้างภาคบังคับ (Mandatory Contractual Terms)

สัญญากับคู่ค้าไอทีทุกรายต้องระบุเงื่อนไขต่อไปนี้อย่างชัดเจน:

- การรักษาความลับ (Confidentiality & Non-Disclosure):** ห้ามนำข้อมูลลูกค้า พอร์ตการลงทุน หรือข้อมูลระบบไปเปิดเผยต่อบุคคลที่สาม ทั้งในระหว่างสัญญาและหลังสิ้นสุดสัญญา
- สิทธิการเข้าตรวจสอบ (Right to Audit):** ผู้ให้บริการต้องยินยอมให้บริษัท, ผู้ตรวจสอบอิสระ (เช่น ผู้ตรวจสอบอิสระภายนอก), และเจ้าหน้าที่สำนักงาน ก.ล.ต. เข้าตรวจสอบกระบวนการปฏิบัติงานและระบบสารสนเทศที่เกี่ยวข้องได้ตลอดเวลา
- การห้ามจ้างช่วงโดยไม่ได้รับอนุญาต (Sub-Contracting Restriction):** ห้ามส่งต่องานหรือว่าจ้างช่วง (Sub-contractor) ให้แก่บุคคลภายนอก เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจากบริษัท
- ข้อกำหนดแผนสำรองและการยกเลิกสัญญา (Exit Strategy):** ผู้ให้บริการต้องมีแผนส่งมอบงาน ข้อมูล และระบบกลับคืนแก่บริษัทอย่างราบรื่นโดยไม่คิดค่าบริการเกินสมควร

4.2 การควบคุมการเข้าถึงระบบของคู่ค้า (Vendor Access Security)

- ห้ามเปิดสิทธิ์ให้คู่ค้าภายนอกเข้าถึงระบบแบบถาวร (No Permanent Access)
- การเข้าทำงานจากระยะไกล (Remote Support) ต้องได้รับอนุมัติจาก IT Specialist เป็นลายลักษณ์อักษรล่วงหน้า
- ต้องเชื่อมต่อผ่าน FortiGate SSL-VPN พร้อมยืนยันตัวตน MFA และจำกัดให้เข้าถึงเฉพาะเครื่องเซิร์ฟเวอร์ที่เกี่ยวข้องเท่านั้น
- ฝ่าย IT ต้องบันทึกภาพ Session การทำงานและเก็บ Log ย้อนหลังเพื่อการตรวจสอบ

5. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

- GW-TMP-16:** ทะเบียนรายชื่อคู่ค้าและผู้ให้บริการภายนอกด้านไอที (IT Vendor & Outsourcer Register)
- GW-TMP-17:** แบบฟอร์มประเมินความเสี่ยงและผลการดำเนินงานคู่ค้าประจำปี (Annual Vendor Risk & SLA Evaluation Form)
- สัญญาว่าจ้างพร้อมข้อตกลงต่อท้ายสัญญา NDA, SLA และ PDPA Data Processing Agreement (DPA)
- บันทึกคำขอเปิดสิทธิ์และประวัติการเข้าใช้งานระบบของคู่ค้าภายนอก (Vendor Access Log)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev.): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 69 / 107
--	---	--

[GW-SOP-14] การจัดการเหตุการณ์ไม่พึงประสงค์และรายงานภัยไซเบอร์ (24h SEC)

(Cyber Incident Management & Regulatory Reporting Procedure)

รหัสเอกสาร	GW-SOP-14	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธชา ตั้งลิขิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณศลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดขั้นตอนการตรวจจับ ตอบสนอง ควบคุมความเสียหาย กู้คืนระบบ

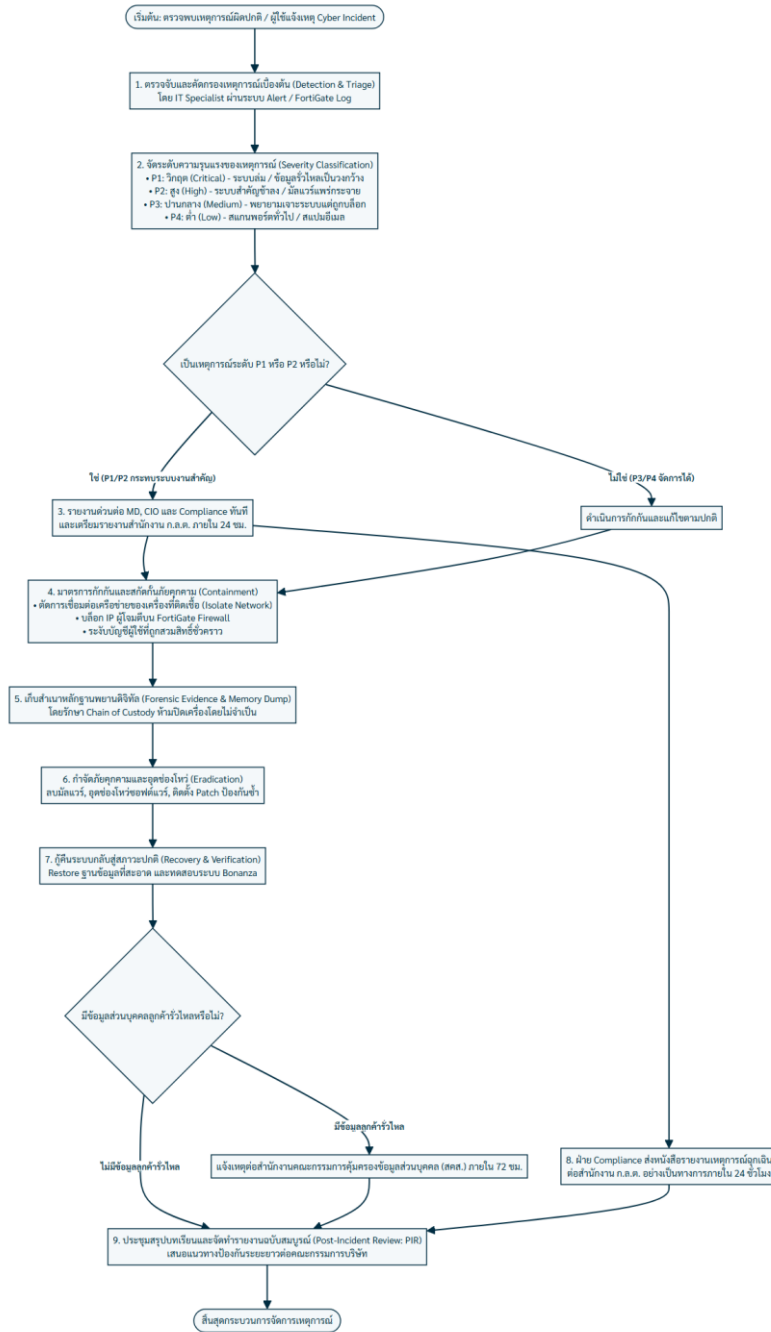
และรายงานเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Plan: CIRP) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- ระบุและควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ (เช่น Ransomware, การโจมตีระบบ, การเข้าถึงข้อมูลโดยไม่ชอบ) ได้อย่างทันท่วงที
- รักษาพยานหลักฐานทางดิจิทัล (Digital Forensics & Chain of Custody) ตามหลักกฎหมาย
- ปฏิบัติตามเกณฑ์บังคับของสำนักงาน ก.ล.ต. ตามประกาศที่ สธ. 38/2565 ในการรายงานเหตุการณ์ที่มีผลกระทบต่อระบบงานสำคัญภายใน 24 ชั่วโมง
- ปฏิบัติตามเกณฑ์การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ภายใน 72 ชั่วโมง

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมเหตุการณ์ผิดปกติและภัยคุกคามความมั่นคงปลอดภัยทั้งหมดที่เกิดขึ้นกับระบบเครือข่าย, ไฟร์วอลล์ FortiGate, เซิร์ฟเวอร์ห้องแม่ข่าย วัน แบงค็อก, ฐานข้อมูลและระบบ Bonanza Investment, อุปกรณ์คอมพิวเตอร์พนักงาน และข้อมูลส่วนบุคคลของลูกค้า

3. ผังกระบวนการจัดการเหตุการณ์ภัยคุกคามทางไซเบอร์ (Operational Process Flow)



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-14
การจัดการเหตุการณ์ไม่พึงประสงค์และรายงานภัยไซเบอร์ (24h SEC)

4. เมทริกซ์ระดับความรุนแรงของเหตุการณ์ (Incident Severity Matrix)

ระดับความรุนแรง (Severity)	คำจำกัดความและลักษณะเหตุการณ์	ผู้รับผิดชอบสั่งการ	กรอบเวลา (SLA)	ข้อกำหนดการรายงาน ก.ล.ต.
ระดับ 1: วิกฤต (Critical - P1)	• ระบบจัดการกองทุน Bonanza หยุดทำงานทั้งหมดในเวลาตลาดเปิด • การโจมตีด้วย Ransomware เข้ารหัสเซิร์ฟเวอร์หลัก • ข้อมูลบัญชี/พอร์ตการลงทุนของลูกค้ารั่วไหลสู่ภายนอก	กรรมการผู้จัดการ (MD) & คณะกรรมการ Incident Command	ตอบสนองทันที ภายใน 15 นาที	ต้องรายงาน ก.ล.ต. อย่างเป็นทางการภายใน 24 ชั่วโมง
ระดับ 2: สูง (High - P2)	• ระบบเครือข่ายหรือ Firewall ขัดข้อง มีเส้นทางสำรองรองรับ • มีการพยายามเจาะระบบจากภายนอกเข้าสู่เครือข่ายภายในสำเร็จบางส่วน • มัลแวร์แพร่กระจายบนเครื่องพนักงานมากกว่า 3 เครื่อง	IT Specialist & Compliance	ตอบสนองภายใน 30 นาที	รายงาน ก.ล.ต. หากประเมินว่าจะลุกลามสู่ระดับ P1
ระดับ 3: ปานกลาง (Medium - P3)	• ตรวจพบไวรัสบนเครื่องพนักงาน 1 เครื่องและถูก Antivirus กักกันไว้ได้ • การพยายามล่อลวงผิดพลาดซ้ำๆ จากภายนอกและระบบล็อกบัญชีอัตโนมัติ	IT Specialist	ตอบสนองภายใน 2 ชั่วโมง	บันทึกในรายงานสรุปประจำเดือน
ระดับ 4: ต่ำ (Low - P4)	• อีเมล Phishing ส่งเข้ามาแต่ระบบ Mail Filter บล็อกไว้ได้ • การสแกนพอร์ตเครือข่ายภายนอกที่ถูก FortiGate ปฏิเสธตามปกติ	IT Specialist	ตอบสนองภายใน 24 ชั่วโมง	บันทึกใน Log ประจำรอบ

 GRANDWAY บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 72 / 107
--	--	---

5. กระบวนการรายงานเหตุการณ์ต่อสำนักงาน ก.ล.ต. (Mandatory SEC Reporting Process)

ตามประกาศสำนักงาน ก.ล.ต. สธ. 38/2565 หากเกิดเหตุการณ์ระดับ P1 หรือเหตุที่ทำให้ระบบสำคัญหยุดชะงัก:

- การแจ้งเหตุเบื้องต้น (Initial Notification):** ฝ่าย Compliance ร่วมกับ IT Specialist ต้องประสานงานและแจ้งต่อเจ้าหน้าที่สำนักงาน ก.ล.ต. ที่กำกับดูแล ภายใน 24 ชั่วโมง ผ่านทางโทรศัพท์ อีเมล หรือระบบรับแจ้งเหตุของ ก.ล.ต.
- การส่งรายงานรายละเอียด (Detailed Incident Report):** จัดทำรายงานวิเคราะห์สาเหตุ ความเสียหาย แนวทางการแก้ไข และมาตรการป้องกันการเกิดซ้ำ ส่งมอบต่อสำนักงาน ก.ล.ต. ภายใน 15 วันทำการ นับแต่วันที่เหตุการณ์ยุติ

6. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

- GW-TMP-18:** แบบฟอร์มบันทึกและรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Incident & Breach Log Form)
- หนังสือแจ้งเหตุการณ์ขัดข้องของระบบสารสนเทศต่อสำนักงาน ก.ล.ต. (Official SEC Notification Letter)
- รายงานการตรวจสอบพยานหลักฐานทางดิจิทัล (Digital Forensic Examination Report)
- รายงานการประชุมทบทวนบทเรียนหลังเหตุการณ์ (Post-Incident Review Report)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 73 / 107
--	---	---

[GW-SOP-15] การควบคุมการเข้าถึงห้องแม่ข่ายทางกายภาพ (Server Room)

(Physical Server Room Access Control Procedure)

รหัสเอกสาร	GW-SOP-15	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิป ก้านจักร IT Specialist	นายโสธชา ตั้งลิदानนท์ Chief Investment Officer (CIO) / Compliance	นายเอกฉัตร ภูณชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของห้องแม่ข่ายคอมพิวเตอร์ (Server Room 42U) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด ณ ชั้น 38 อาคาร วัน แบงค็อก ทาวเวอร์ 4 (One Bangkok Tower 4) เพื่อ:

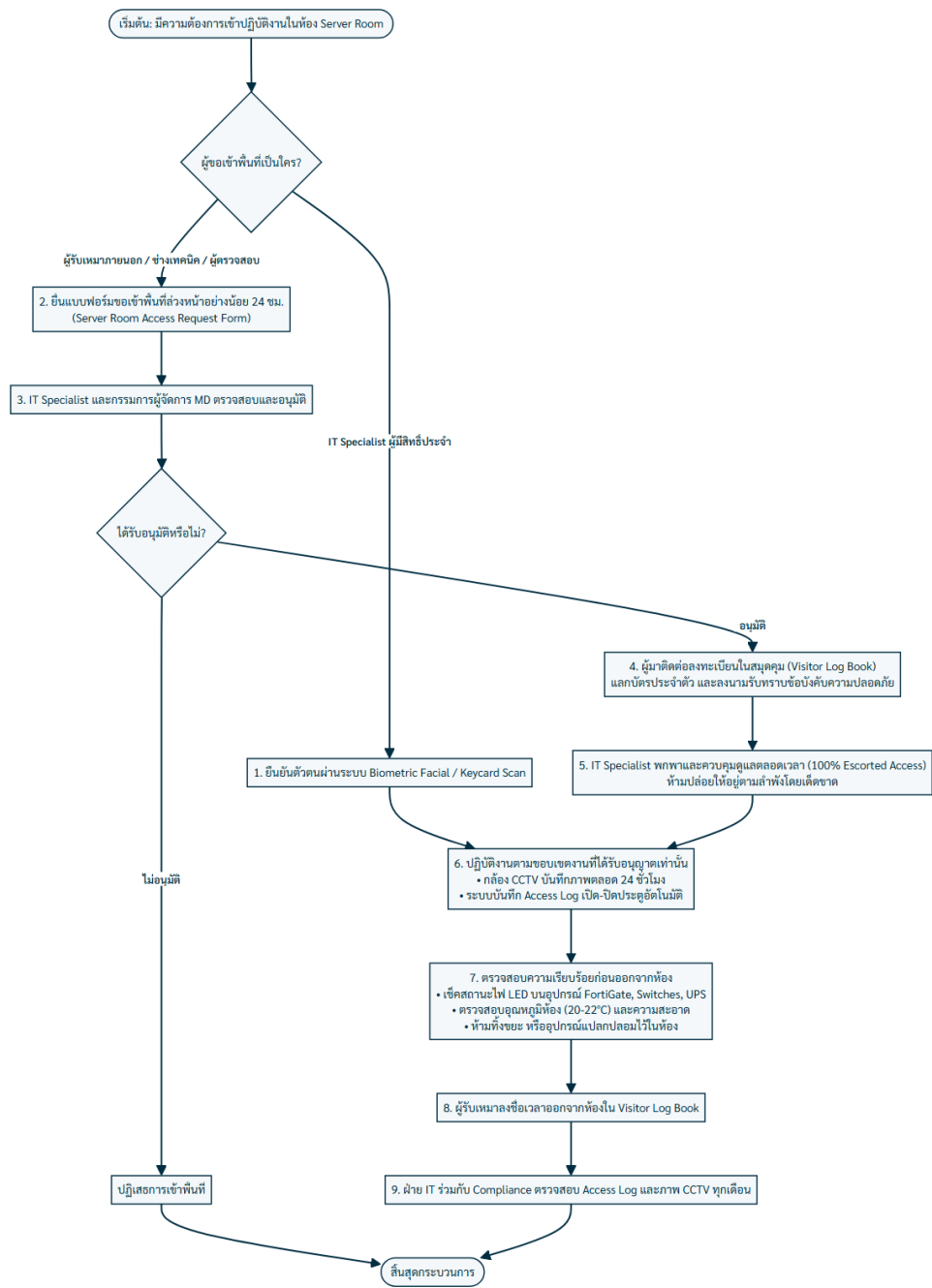
- ป้องกันการเข้าถึงอุปกรณ์แม่ข่าย ฮาร์ดแวร์ระบบกองทุน Bonanza, ไฟร์วอลล์ และตู้แร็ค 42U โดยบุคคลที่ไม่ได้รับอนุญาต
- ควบคุมและบันทึกประวัติการเข้า-ออกห้องแม่ข่ายของพนักงานและผู้รับเหมาภายนอก (Vendors / Engineers)
- รักษาสภาพแวดล้อมทางวิศวกรรม (อุณหภูมิ, ความชื้น, ระบบไฟฟ้า Dual Feeds, และระบบดับเพลิงสารสะอาด) ให้เป็นไปตามมาตรฐานสากล
- สอดคล้องกับมาตรฐาน ISO/IEC 27001 (Physical & Environmental Security) และประกาศสำนักงาน ก.ล.ต. สธ. 38/2565

2. ขอบเขตการบังคับใช้ (Scope)

ครอบคลุมพื้นที่ห้องแม่ข่ายคอมพิวเตอร์ (Server Room) ตู้แร็ค 42U ฐานเหล็ก Base Plinth 130x150 ซม.

ระบบปรับอากาศควบคุมอุณหภูมิ ระบบดับเพลิงอัตโนมัติ และระบบจ่ายไฟฟ้าสำรองทั้งหมด ณ สำนักงานใหญ่ วัน แบงค็อก

3. ผังกระบวนการควบคุมการเข้าพื้นที่ห้องแม่ข่าย (Operational Process Flow)



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-SOP-15 การควบคุมการเข้าถึงห้องแม่ข่ายทางกายภาพ (Server Room)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 75 / 107
--	--	---

4. มาตรการควบคุมทางกายภาพและวิศวกรรมอาคาร (Engineering & Physical Controls)

4.1 ระบบควบคุมการเปิด-ปิดประตู (Electronic Access Control)

- ประตูทางเข้าห้องแม่ข่ายต้องล็อกตลอดเวลาด้วยระบบกลอนแม่เหล็กไฟฟ้า (Magnetic Door Lock: EM-Lock)
- การผ่านเข้า-ออกต้องใช้การยืนยันตัวตนแบบชีวมิติ (Biometric Facial Recognition) หรือคีย์การ์ดความปลอดภัยสูงที่บันทึกข้อมูลรายบุคคล
- มีระบบกระจกแตกปลดล็อกฉุกเฉิน (Emergency Break-Glass Unit) ติดตั้งอยู่ภายในห้องเพื่อความปลอดภัยกรณีเกิดอัคคีภัย
- สัญญาณเตือนภัย (Door Ajar Alarm) จะดังขึ้นทันทีหากประตูถูกเปิดค้างไว้นานเกิน **60 วินาที**

4.2 ระบบโทรทัศน์วงจรปิด (CCTV Surveillance)

- ติดตั้งกล้องวงจรปิดความคมชัดสูงเลนส์มุมกว้าง (Wide-Angle CCTV Coverage) จำนวน 1 จุดภายในห้องแม่ข่าย ณ ตำแหน่งมุมสูงครอบคลุมพื้นที่ห้องทั้งหมดอย่างทั่วถึง ทั้งบริเวณหน้าตู้-หลังตู้แร็ค 42U และประตูทางเข้า-ออก โดยไม่มีจุดอับสายตา
- บันทึกภาพตลอด 24 ชั่วโมง 7 วัน และจัดเก็บภาพบันทึกย้อนหลังในระบบ NVR ไม่น้อยกว่า **90 วัน** ตามเกณฑ์ ก.ล.ด.

4.3 ระบบควบคุมสภาพแวดล้อม (Environmental Controls)

- **การควบคุมอุณหภูมิและความชื้น:** ติดตั้งระบบเครื่องปรับอากาศแบบ Inverter ที่รักษาอุณหภูมิระหว่าง **20°C – 22°C** และความชื้นสัมพัทธ์ **45% – 55%**
- **อุปกรณ์ดับเพลิงอัตโนมัติ:** รายการที่ตกลงกับผู้รับเหมาคือ SUNSAFETY ถังดับเพลิงอัตโนมัติชนิดดีเพดาน Clean Agent (NON CFC) 10 ปอนด์; การติดตั้งและการยอมรับของอาคารรอยืนยัน พร้อมระบบตรวจจับควันไฟล่วงหน้า (Early Warning Smoke Detectors)
- **ระบบจ่ายไฟฟ้าสำรอง (Power Redundancy):** เดินระบบสายไฟแยก 2 วงจรอิสระ (Dual Circuit Feeds: Circuit A & Circuit B) เข้าสู่ตู้แร็ค 42U ผ่าน True Online UPS และมีระบบสายดินที่ค่าความต้านทานต่ำกว่า 5 โอห์ม

4.4 วิศวกรรมการกระจายน้ำหนักตู้แร็ค (Floor Loading Capacity)

- ตู้แร็คเซิร์ฟเวอร์ขนาด 42U ต้องติดตั้งอยู่บน **ฐานเหล็กกระจายน้ำหนักสั่งทำพิเศษ (Base Plinth 130x150 ซม.)** ที่ยึดสมอเข้ากับพื้นคอนกรีตอาคาร เพื่อให้ค่าแรงกดกระจายตัวสม่ำเสมอไม่เกินเกณฑ์ความปลอดภัยของอาคาร วัน แบงค็อก ทาวเวอร์
- 4

5. กฎระเบียบความปลอดภัยภายในห้องแม่ข่าย (Server Room House Rules)

1. ห้ามนำอาหาร เครื่องดื่ม ขนม หรือของเหลวทุกชนิดเข้ามาในห้องแม่ข่ายโดยเด็ดขาด
2. ห้ามใช้ห้องแม่ข่ายเป็นพื้นที่เก็บของ จัดเก็บกล่องกระดาษ อุปกรณ์เก่า หรือสิ่งของติดไฟ
3. ห้ามเสียบปลั๊กเครื่องใช้ไฟฟ้าทั่วไป (เช่น เครื่องดูดฝุ่น พัดลม กาต้มน้ำ) เข้ากับเต้ารับไฟฟ้าของตู้แร็คหรือ UPS โดยเด็ดขาด
4. การเปิดตู้แร็ค 42U ด้านหน้าหรือด้านหลัง ต้องใช้กุญแจที่ควบคุมโดย IT Specialist และต้องล็อกกลับคืนทุกครั้งหลังเสร็จงาน

6. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

1. GW-TMP-19: แบบฟอร์มขออนุญาตเข้าพื้นที่ห้องแม่ข่ายคอมพิวเตอร์ (Server Room Access Request Form)

 GRANDWAY บจ. แกรนด์เวย์ แคปปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 76 / 107
---	---	---

2. GW-TMP-20: สมุดบันทึกประวัติการเข้า-ออกห้องแม่ข่ายคอมพิวเตอร์ (Server Room Visitor Log Book)
3. รายงานบันทึกเวลาการเปิด-ปิดประตูจากระบบ Access Control ประจำเดือน (Electronic Door Access Log Report)
4. รายงานผลการบำรุงรักษาระบบปรับอากาศ ระบบไฟฟ้า UPS และระบบดับเพลิงตามรอบ (Preventive Maintenance Report)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev.): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 77 / 107
--	--	--

[GW-BCP-02] แผนความต่อเนื่องทางธุรกิจและการประเมินผลกระทบ (BCP & BIA)

(Business Continuity Plan & Business Impact Analysis: BCP & BIA)

รหัสเอกสาร	GW-BCP-02	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายบริหารความเสี่ยงและฝ่ายไอที	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการทบทวน	ประจำปี (อย่างน้อยปีละ 1 ครั้ง)

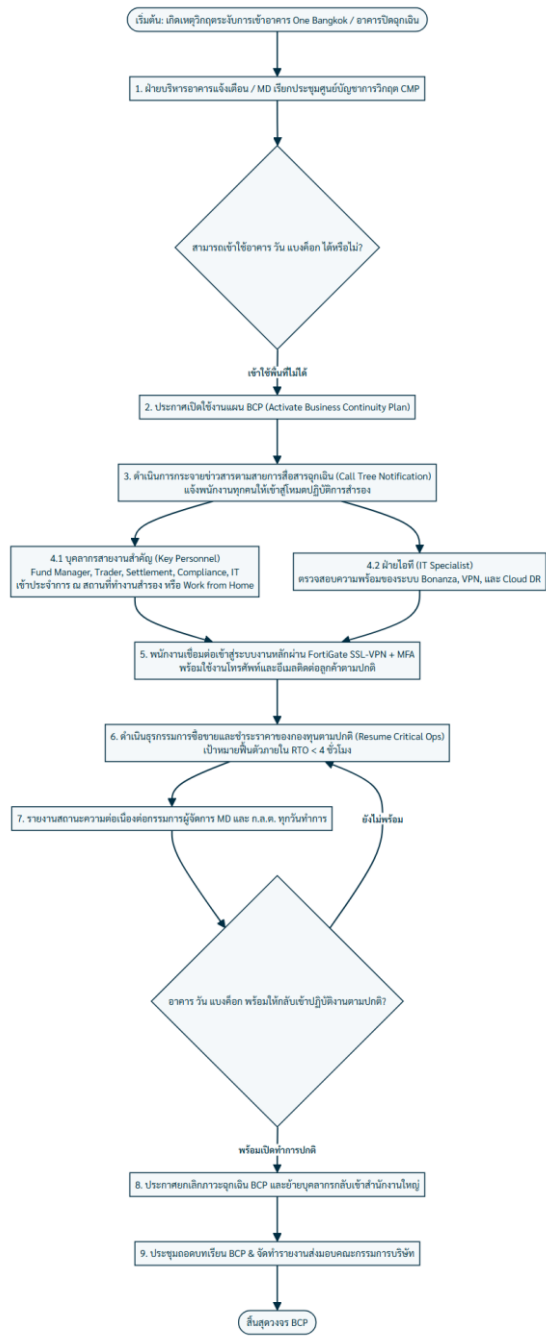
ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิป ก้านจักร IT Specialist	นายโสรชา ตั้งลิदानนท์ Chief Investment Officer (CIO) / Compliance	นายเอกฉัตร ภูณชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ระเบียบปฏิบัติงานฉบับนี้กำหนดขั้นตอนการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) และแผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อ:

- จัดลำดับความสำคัญของกระบวนการทางธุรกิจ ทรัพยากร และระบบไอทีที่จำเป็นต่อการบริหารจัดการกองทุนส่วนบุคคล
- กำหนดขั้นตอนปฏิบัติการสลับสถานที่ทำงาน (Workplace Relocation / Remote Working) และการกู้คืนกระบวนการทางธุรกิจ
- รองรับการปฏิบัติตามมาตรฐานสากล ISO 22301 และเกณฑ์การกำกับดูแลของสำนักงาน ก.ล.ต. ตามประกาศ สธ. 38/2565

2. ฟังก์กระบวนการบริหารความต่อเนื่องทางธุรกิจ (Operational Process Flow)



รูปภาพ: ฟังก์กระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-BCP-02 แผนความต่อเนื่องทางธุรกิจและการประเมินผลกระทบ (BCP & BIA)

3. ผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA Matrix)

กระบวนการทางธุรกิจ (Business Function)	แผนกรับผิดชอบ	ระดับความสำคัญ (Criticality)	MTPD สูงสุดที่ยอมรับได้	เป้าหมาย RTO	เป้าหมาย RPO	ทรัพยากรขั้นต่ำที่ต้องการ
1. การส่งคำสั่งซื้อขายหลักทรัพย์ (Trading)	Trading Desk	วิกฤตสูงสุด (Tier 1)	4 ชั่วโมง	< 2 ชั่วโมง	< 1 ชั่วโมง	โน้ตบุ๊กเข้ารหัส, VPN, อินเทอร์เน็ตความเร็วสูง, ระบบ Bonanza
2. การบริหารพอร์ตการลงทุน (Portfolio Mgmt)	Investment Team	วิกฤตสูงสุด (Tier 1)	4 ชั่วโมง	< 2 ชั่วโมง	< 1 ชั่วโมง	โน้ตบุ๊กเข้ารหัส, VPN, ข้อมูลราคาตลาด, ระบบ Bonanza
3. การชำระราคาและส่งมอบหลักทรัพย์ (Settlement)	Operations	วิกฤตสูง (Tier 1)	8 ชั่วโมง	< 4 ชั่วโมง	< 24 ชั่วโมง	ระบบเชื่อมต่อ Custodian Bank, ระบบ Bonanza, Token ธนาคาร
4. การควบคุมความเสี่ยงและกำกับดูแล (Compliance)	Compliance	สำคัญ (Tier 2)	8 ชั่วโมง	< 4 ชั่วโมง	< 24 ชั่วโมง	ระบบ Read-Only ตรวจสอบคำสั่งซื้อขาย, ช่องทางติดต่อ ก.ล.ต.
5. การดูแลโครงสร้างไอที (IT Infrastructure)	IT Department	สำคัญยิ่งยวด (Tier 1)	2 ชั่วโมง	< 1 ชั่วโมง	0 นาที	อุปกรณ์ Admin, การเข้าถึง Cloud DR, FortiGate VPN Management

4. แผนการสื่อสารในภาวะฉุกเฉิน (Emergency Call Tree)

- มีการจัดทำและอัปเดต ตารางรายชื่อและเบอร์ติดต่อฉุกเฉินของพนักงานทุกคน (Staff Emergency Contact List) ทุกไตรมาส
- เมื่อเกิดเหตุ กรรมการผู้จัดการ (MD) หรือผู้ได้รับมอบหมายจะส่งข้อความแจ้งเตือนผ่านช่องทาง SMS / โทรศัพท์ และกลุ่มสื่อสารฉุกเฉิน เพื่อให้พนักงานเริ่มปฏิบัติตามแผน BCP ทันที

5. แบบฟอร์มและหลักฐานเชิงประจักษ์ที่ต้องจัดเก็บ (Evidence & Forms)

- GW-TMP-21: แบบฟอร์มการประเมินผลกระทบทางธุรกิจประจำปี (Annual Business Impact Analysis Form)
- ตารางผังสายการติดต่อฉุกเฉินของพนักงาน (Emergency Call Tree Matrix)
- รายงานผลการซักซ้อมแผนความต่อเนื่องทางธุรกิจประจำปี (Annual BCP Simulation Exercise Report)
- รายงานสรุปสถานการณ์และบทเรียนหลังสิ้นสุดภาวะฉุกเฉิน (BCP Post-Incident Debriefing Report)

[GW-TEC-01] ผังแปลนและการจัดวางอุปกรณ์ห้องแม่ข่าย 42U วัน แบงค็อก

(Server Room 42U Layout & Engineering Specification)

รหัสเอกสาร	GW-TEC-01	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	สถานที่ติดตั้ง	ชั้น 38 อาคาร วัน แบงค็อก ทาวเวอร์ 4

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย กำนันจักร IT Specialist	นายโสธรา ตั้งลิขิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณชุลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. ข้อมูลภาพรวมโครงสร้างทางวิศวกรรม (Engineering Overview — Revision 5.0)

ห้องแม่ข่ายคอมพิวเตอร์ (Server Room) ของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด ตั้งอยู่ ณ ชั้น 38 อาคาร วัน แบงค็อก ทาวเวอร์ 4 (One Bangkok Tower 4) มีขนาดพื้นที่ประมาณ 2.50 x 3.20 เมตร (พื้นที่สุทธิประมาณ 6.26–8.00 ตร.ม.) ได้รับการออกแบบตามเกณฑ์วิศวกรรมอาคาร วัน แบงค็อก และมาตรฐาน Data Center สากล TIA-942:

- แผ่นเหล็กกระจายน้ำหนักบนพื้นยก (Overfloor Steel Spreader Plate):** ตู้แร็คขนาด 42U ติดตั้งบนแผ่นเหล็กโครงสร้าง SS400 ขนาด 1,300 x 1,500 มม.หนา 6 มม. (พื้นที่ 1.95 ตร.ม. มวลเหล็ก 91.85 กก.) วางบนระบบพื้นยก Raised Floor โดยตรงโดยไม่ต้องกรีดตัดพื้นยกเดิม รองใต้แผ่นด้วย แผ่น Neoprene Nominal 5 มม. เต็มพื้นที่ เพื่อซับแรงสั่นสะเทือนและกระจายน้ำหนักลงสู่ระบบคาน Pedestal/Stringer สู่พื้นคอนกรีตอาคาร (Concrete Slab) อย่างสมบูรณ์ ค่าเฉลี่ยมวลรวมปลอดภัยกว่าเกณฑ์จำกัดน้ำหนักของอาคาร วัน แบงค็อก (500 กก./ตร.ม.)
- การจัดวางตู้แร็คและระยะยื่น (Rack Placement & Margins):** ตู้แร็คขนาด 800 x 1,100 มม. ตั้งอยู่กึ่งกลางแผ่นเหล็ก โดยมีปีกแผ่นเหล็กยื่นด้านข้างข้างละ 250 มม. และด้านหน้า-หลังด้านละ 200 มม. แนวตู้หัน หน้าตู้ขึ้นด้านบน (Front faces UP toward room entrance) ใกล้ทางเข้าห้อง และ หลังตู้หันลงด้านล่าง (Rear faces DOWN)
- การแบ่งโซนระดับพื้นห้อง (Floor Zoning & Door Clearance):**



บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป

Grandway Capital Group Ltd.

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)

คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก

Master IT Operations & Cyber Security Suite

รหัสเอกสาร: GW-IT-MANUAL-2026

ฉบับที่ (Rev): 2.0

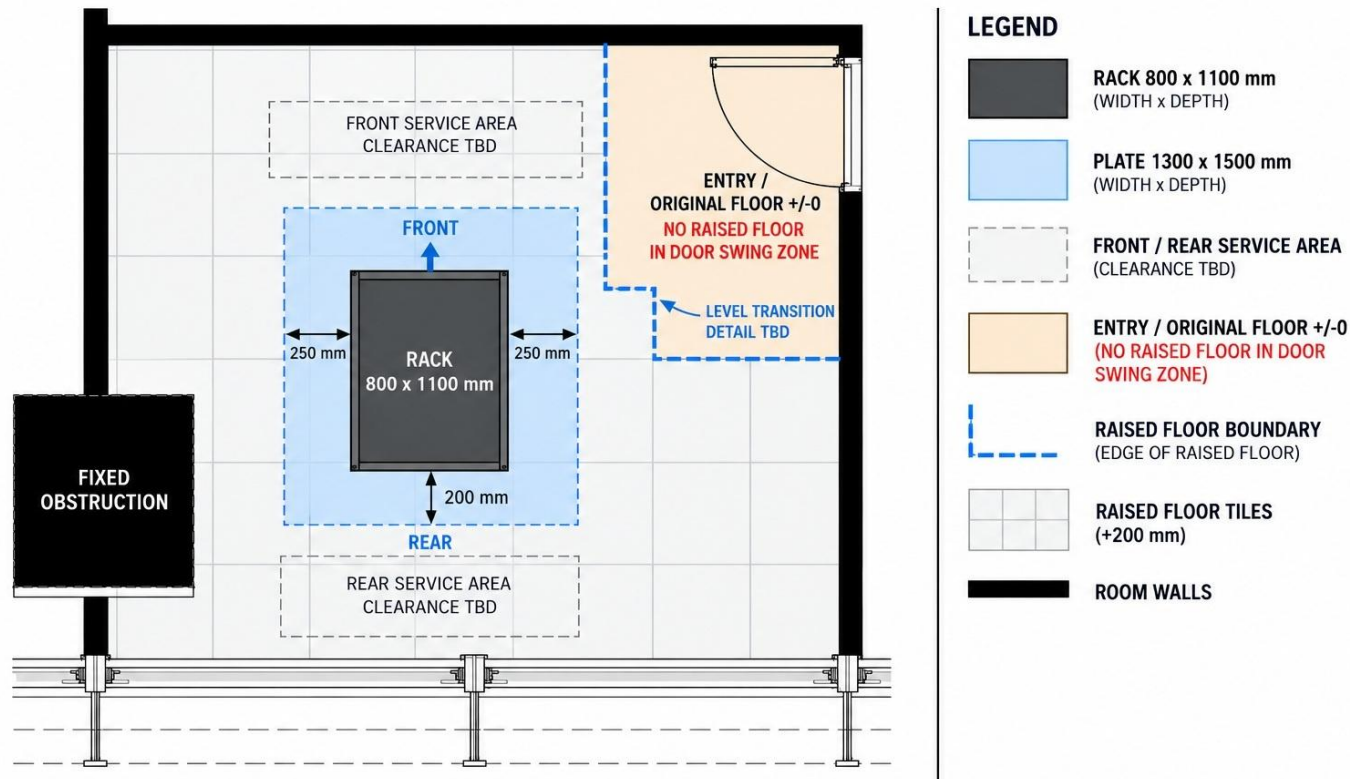
วันที่มีผล: 01/11/2569

ชั้นความลับ: Confidential

หน้าที่: 81 / 107

- **โซนพื้นยก (+200 มม.):** พื้นที่ส่วนใหญ่ในห้องติดตั้งพื้นยก Calcium Sulphate สูง +200 มม. เป็นฐานรองรับแผ่นเหล็ก ตู้แร็ค 42U และช่องเดินสายสัญญาณ Cat6A / รางสายไฟ Dual Feeds
- **โซนวางเปิดประตู (\$\pm 0\$):** มุมขวามือบริเวณทางเข้าประตูห้องแม่ข่าย คงระดับพื้นคอนกรีตเดิม \$\pm 0\$ (ไม่ติดตั้งพื้นยก) เพื่อให้บานประตูเปิดสวิงเข้าห้องได้เต็มวงโดยไม่ติดขัดแผ่นเหล็กและตู้แร็คตั้งอยู่บนโซนพื้นยกทั้งหมด ไม่รบกวนเปิดประตู
- **สถาปัตยกรรมระบบประมวลผล (Cloud-First Workload):** ระบบแกนหลักของกองทุน (Production Workload) ทั้งหมด 4 VMs (GW-DC01, GW-APP01, GW-DB01, GW-FS01) ทำงานอยู่บน True IDC Cloud Tier III ภายใต้โครงสร้างคลัสเตอร์ความพร้อมสูง จึงไม่มีเครื่อง Physical HCI หนักๆ วางในห้อง 42U นี้ ช่วยลดภาระน้ำหนักและภาระความร้อนได้อย่างมีประสิทธิภาพ
- **ระบบปรับอากาศ:** ติดตั้งเครื่องปรับอากาศแบบ Inverter ควบคุมอุณหภูมิที่ **20°C - 22°C** ความชื้น 45–55% RH ตลอด 24 ชม.
- **อุปกรณ์ดับเพลิงอัตโนมัติ:** SUNSAFETY ถังดับเพลิงอัตโนมัติติดเพดาน Clean Agent (NON CFC) 10 ปอนด์ ไม่ทำลายอุปกรณ์อิเล็กทรอนิกส์

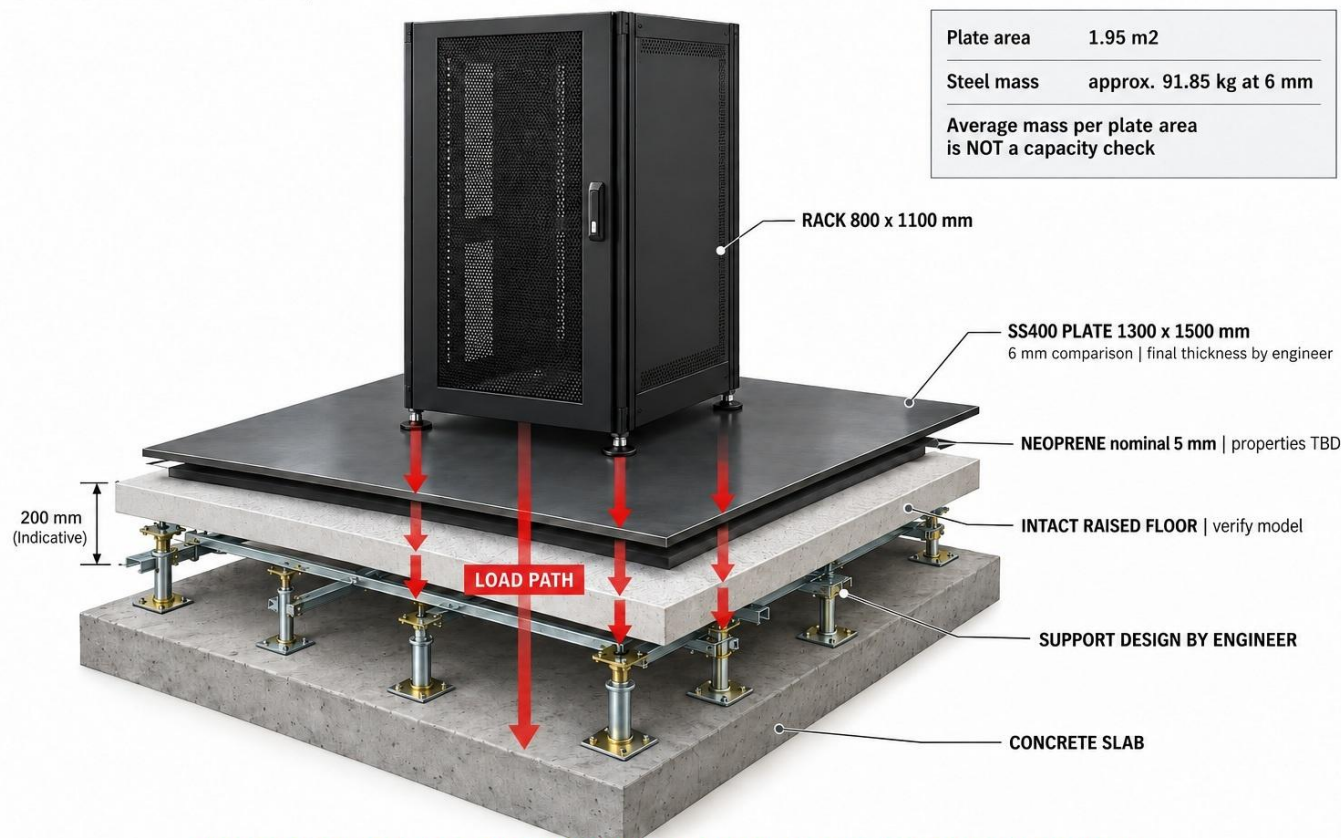
GW ONE BANGKOK | RACK ORIENTATION



CONCEPT PLAN | NOT TO SCALE | ENGINEER AND BUILDING REVIEW REQUIRED

รูปภาพ: ผังจัดวางตู้แร็ค 42U ระยะเปิดประตูตู้ และระยะวงสวิงประตูห้องแม่ข่าย (Rack Layout & Door Swing Clearance) ชั้น 38 อาคาร วัน แบงค็อก

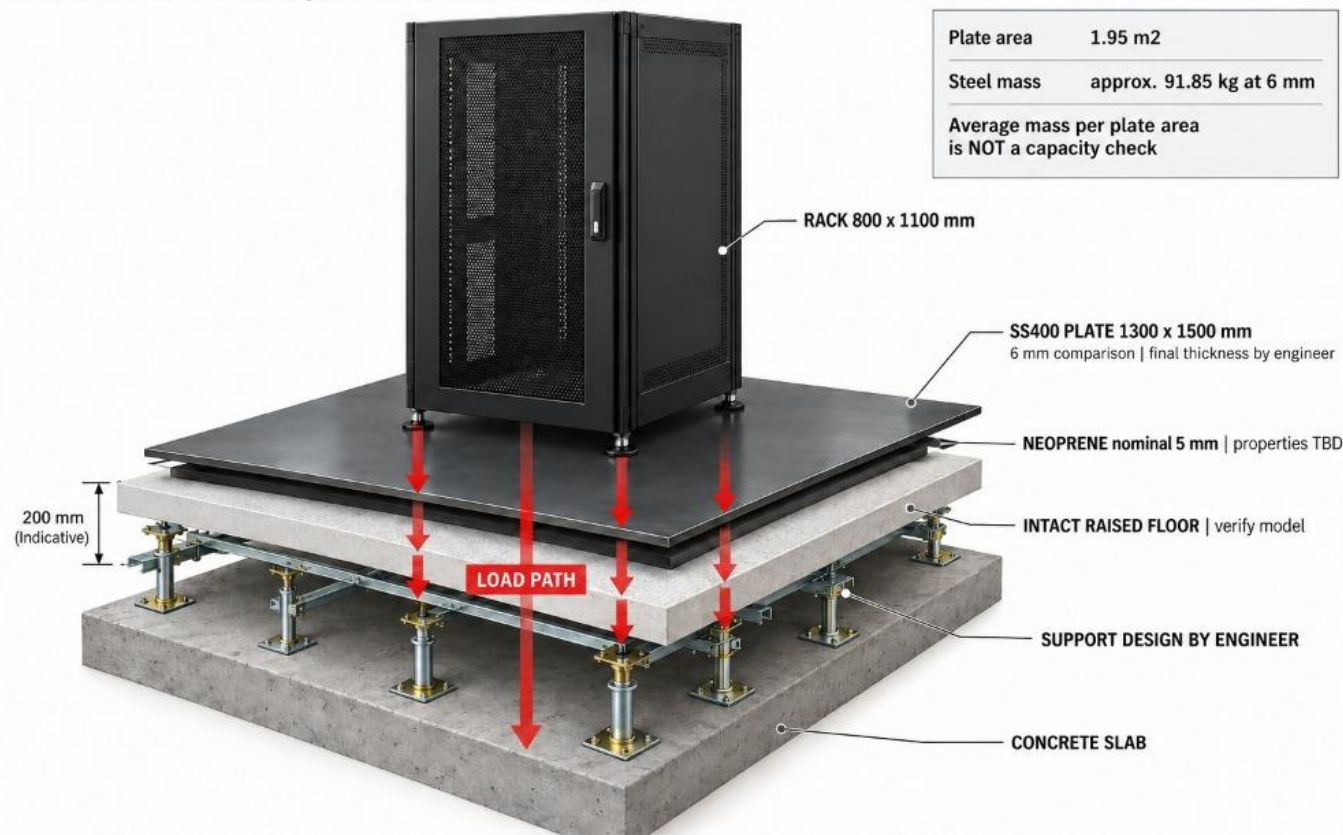
GW ONE BANGKOK | OVERFLOOR LOAD PATH



PROPOSED METHOD | NOT FOR FABRICATION | ENGINEER AND BUILDING APPROVAL REQUIRED

รูปภาพ: แบบแปลนวิศวกรรมแผ่นเหล็กกระจายน้ำหนักตู้แร็คบนพื้นยก (Overfloor Steel Spreader Plate 1.30 x 1.50 m, SS400 หนา 6 มม. พร้อม Neoprene 5 มม.)

GW ONE BANGKOK | OVERFLOOR LOAD PATH



PROPOSED METHOD | NOT FOR FABRICATION | ENGINEER AND BUILDING APPROVAL REQUIRED

รูปภาพ: แบบจำลอง 3 มิติวิศวกรรมการถ่ายเทน้ำหนักลงจุดเส้าพื้นยก (Overfloor Load Path 3D Engineering Model) — จุดถ่ายแรง 9 จุดเส้าพื้นยก

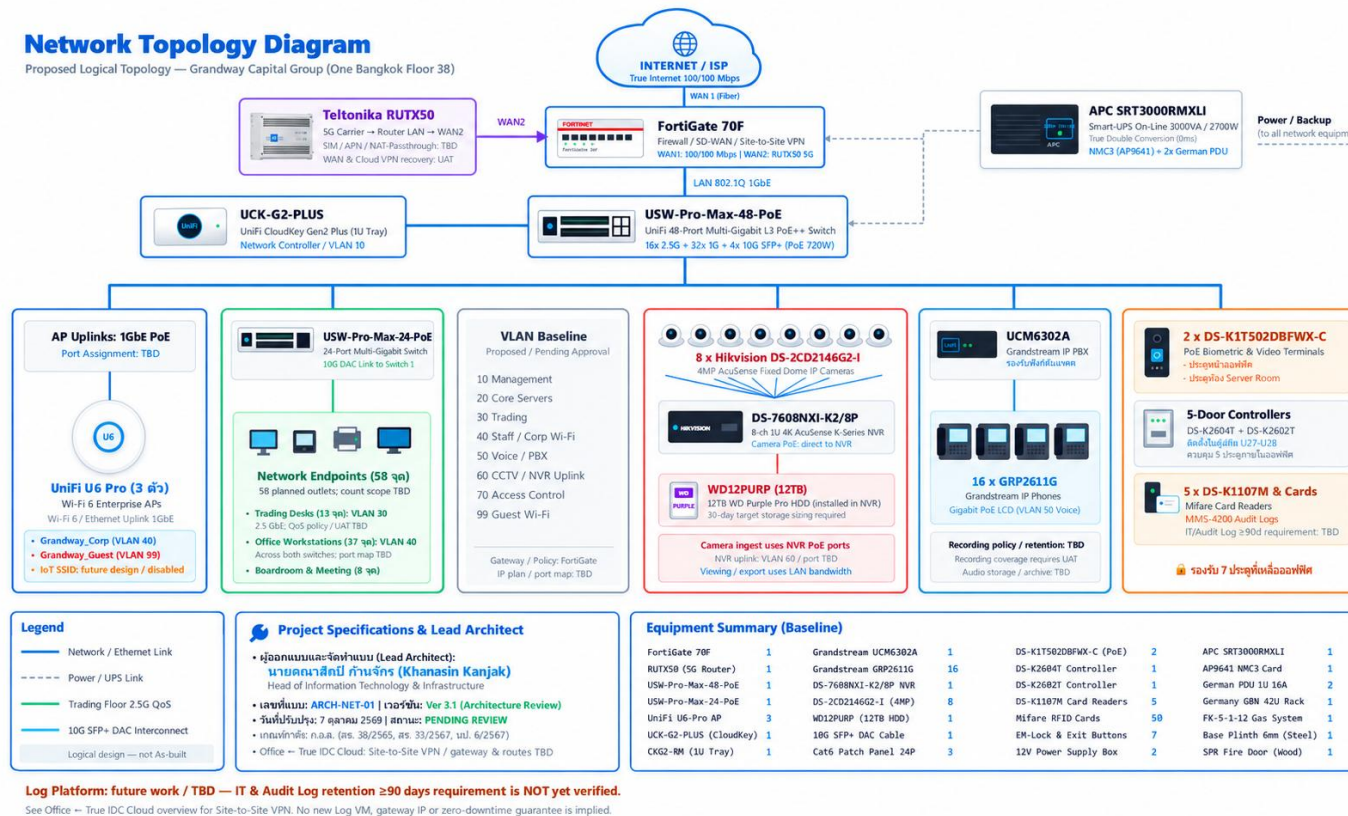


บจ. แกรนด์เวย์ แคปปิตอล กรุ๊ป
Grandway Capital Group Ltd.

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)
คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก
Master IT Operations & Cyber Security Suite

รหัสเอกสาร: GW-IT-MANUAL-2026
ฉบับที่ (Rev): 2.0
วันที่มีผล: 01/11/2569
ชั้นความลับ: Confidential
หน้าที่: 85 / 107

2. แผนผังจัดวางอุปกรณ์ภายในตู้แร็ค 42U (Rack Elevation Layout: U42 - U01)



รูปภาพ: แผนผังโครงสร้างเครือข่ายความมั่นคงปลอดภัยและสถาปัตยกรรมระบบสารสนเทศ (Grandway Enterprise Network Architecture Topology Diagram Rev 3.1) — ตู้แร็ค 42U One Bangkok



บจ. แกรนด์เวย์ แคปปิตอล กรุ๊ป
Grandway Capital Group Ltd.

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)

คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก

Master IT Operations & Cyber Security Suite

รหัสเอกสาร: GW-IT-MANUAL-2026

ฉบับที่ (Rev): 2.0

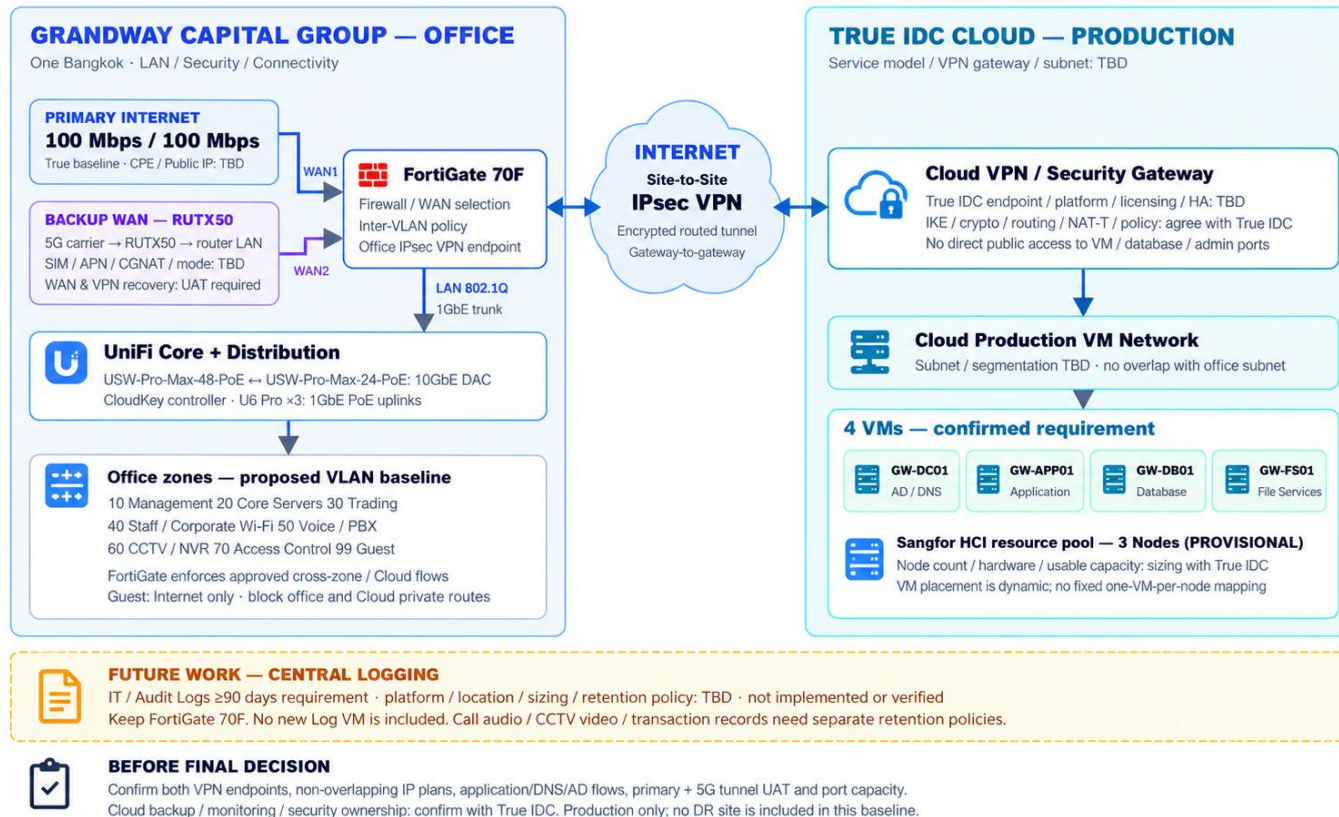
วันที่มีผล: 01/11/2569

ชั้นความลับ: Confidential

หน้าที่: 86 / 107

GW | OFFICE ↔ TRUE IDC CLOUD

Production connectivity overview · Revision 3.1 · 07 Oct 2026 · Architecture Review / Pending Decision



รูปภาพ: สถาปัตยกรรมเครือข่ายไฮบริดคลาวด์เชื่อมโยงสำนักงานใหญ่และศูนย์ข้อมูลภายนอก (Office-to-Cloud Hybrid Infrastructure Architecture) — One Bangkok ↔ True IDC Tier III Cloud

U42 - U41 : Fiber Optic Patch Panel (FTTH/ISP Leased)



บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป

Grandway Capital Group Ltd.

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)

คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก

Master IT Operations & Cyber Security Suite

รหัสเอกสาร: GW-IT-MANUAL-2026

ฉบับที่ (Rev): 2.0

วันที่มีผล: 01/11/2569

ชั้นความลับ: Confidential

หน้าที่: 87 / 107

U40 - U39 : Cat6A Modular Patch Panel 24 Port (VLANs)
U38 : Cable Management Horizontal 1U
U37 : FortiGate 70F Next-Gen Firewall (WAN1/WAN2)
U36 : Teltonika RUTX50 5G Router (WAN2 Backup)
U35 - U34 : UniFi Pro Max 48 PoE Enterprise Switch
U33 : Cable Management Horizontal 1U
U32 - U31 : UniFi Pro Max 24 PoE Enterprise Switch
U30 - U25 : 10GbE SFP+ DAC Inter-Switch Link & Mgmt
U24 - U21 : Network Attached Storage (NAS Backup RAID)
U20 - U17 : CCTV NVR System (PoE Ingest & Storage)
U16 - U11 : Blanking Panels (Optimal Airflow Control)
U10 - U07 : APC/Eaton True Online UPS 3kVA/5kVA
U06 - U01 : Extended Battery Module (EBM Battery Pack)

ด้านข้างตู้ : Dual Vertical Metered PDU (Feeds A & B)

ฐานตู้แร็ค : Overfloor SS400 Plate 1300x1500mm + Pad

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 88 / 107
--	--	---

3. ผังโครงข่ายไฟฟ้าและความมั่นคงปลอดภัยทางกายภาพ (MEP & Power Redundancy)

1. วงจรไฟฟ้าคู่ (Dual Circuit Power Feeds):

- Circuit A (Main Feed): จ่ายไฟจากแผงสวิตช์บอร์ดฉุกเฉินอาคาร (Emergency Generator Backup) → ผ่าน True Online UPS → PDU A
- Circuit B (Bypass/Secondary Feed): จ่ายไฟจากแผงอาคารอิสระ → PDU B

2. ระบบสายดิน (Grounding & Bonding): ติดตั้ง Signal Reference Ground Bar ภายในห้องแม่ข่าย เชื่อมต่อด้วยสายทองแดงเปลือยเข้ากับเสาโครงสร้างอาคาร โดยมีค่าความต้านทานดิน < 5 โอห์ม

3. ระบบกล้อง CCTV และ Access Control:

- ติดตั้งกล้องวงจรปิดความคมชัดสูงเลนส์มุมกว้าง (Wide-Angle CCTV) จำนวน 1 จุดภายในห้องแม่ข่าย ณ ตำแหน่งมุมสูง ครอบคลุมพื้นที่ห้องทั้งหมด หน้าตู้และหลังตู้แร็ค 42U และประตูเข้า-ออกตลอด 24 ชม. บันทึกเข้า NVR ย้อนหลังไม่น้อยกว่า 90 วัน
- ประตูล็อกด้วยกลอนแม่เหล็กไฟฟ้า (EM-Lock 600 lbs) ปลดล็อกด้วยสแกนไบโอหน้า (Biometric Facial) และมีปุ่มกดออกฉุกเฉิน Break-Glass

[GW-TEC-02] ตารางมาตรฐานนโยบายความปลอดภัย Active Directory (GPO Matrix)

(Active Directory Group Policy Objects: GPO Baseline Matrix)

รหัสเอกสาร	GW-TEC-02	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	ระบบเป้าหมาย	Domain Controller & Windows Endpoints

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณชุลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

เอกสารฉบับนี้กำหนดค่ามาตรฐานความมั่นคงปลอดภัย (Security Baseline Configuration) สำหรับการบังคับใช้นโยบายผ่าน Active Directory Group Policy Objects (GPO) บนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์พนักงานทั้งหมด เพื่อให้สอดคล้องกับมาตรฐาน CIS Benchmarks และข้อกำหนดของสำนักงาน ก.ล.ต. ตามประกาศ สธ. 38/2565

2. ตารางมาตรฐานการกำหนดค่า GPO (Master GPO Baseline Settings)

หมวดหมู่ (Category)	การตั้งค่านโยบาย (Policy Setting)	ค่ามาตรฐานที่กำหนด (Grandway Baseline)	เหตุผลความมั่นคงปลอดภัย
---------------------	-----------------------------------	--	-------------------------

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.		ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite		รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 90 / 107
Password Policy	ความยาวรหัสผ่านขั้นต่ำ (Minimum password length)	12 ตัวอักษร	ป้องกันการโจมตีแบบ Brute-Force	
	ความซับซ้อนของรหัสผ่าน (Password complexity)	Enabled (ต้องมีตัวพิมพ์ใหญ่, เล็ก, ตัวเลข, สัญลักษณ์)	เพิ่มความยากในการคาดเดารหัสผ่าน	
	อายุการใช้งานรหัสผ่านสูงสุด (Max password age)	90 วัน	บังคับเปลี่ยนรหัสผ่านตามรอบ ก.ล.ต.	
	จดจำรหัสผ่านย้อนหลัง (Enforce password history)	10 ครั้งล่าสุด	ป้องกันการใช้รหัสผ่านเดิมซ้ำ	
Account Lockout	จำนวนครั้งล็อกอินผิดสูงสุด (Lockout threshold)	5 ครั้ง	ระงับบัญชีเมื่อตรวจพบการเดารหัสผ่าน	
	ระยะเวลาล็อกบัญชี (Lockout duration)	30 นาที (หรือจนกว่า IT ปลดล็อก)	ชะลอการโจมตีอัตโนมัติ	
	ตัวนับรีเซ็ตความผิดพลาด (Reset lockout counter)	30 นาที	รีเซ็ตประวัติความผิดพลาด	
Interactive Logon	เวลาพักหน้าจออัตโนมัติ (Screen Lock Timeout)	5 นาที (300 วินาที)	ป้องกันผู้อื่นสวมสิทธิ์เมื่อไม่อยู่ที่โต๊ะ	
	ซ่อนชื่อผู้ใช้งานล่าสุด (Don't display last signed-in)	Enabled	ป้องกันการล่วงรู้ Username	
Device & USB Control	ข้อความแจ้งเตือนข้อตกลง (Legal Notice / AUP Banner)	Enabled (ระบุข้อห้ามการใช้ระบบโดยมิชอบ)	ข้อกำหนดทางกฎหมาย พ.ร.บ.คอมพิวเตอร์	
	ปิดกั้นการเขียนข้อมูลลง USB (Block USB Write Access)	Enabled (Read-Only / Disabled)	ป้องกันข้อมูลลูกค้าและพอร์ตรั่วไหลออกนอกองค์กร	
	ปิดการทำงานของฟังก์ชัน AutoPlay/Autorun	Enabled for all drives	ป้องกันการแพร่กระจายของไวรัสผ่าน USB	
User Rights & Admin	ตัดสิทธิ์ Local Administrator บนเครื่องผู้ใช้	Enabled (User อยู่ในสิทธิ์ Standard User)	ป้องกันพนักงานติดตั้งซอฟต์แวร์เถื่อน	
	ปิดใช้งานบัญชี Guest Account (Guest Status)	Disabled	ปิดช่องโหว่การเข้าใช้โดยไม่ระบุตัวตน	
Windows Audit Policy	ปิดโปรโตคอล NTLMv1 และบังคับใช้ NTLMv2/Kerberos	Send NTLMv2 response only / Refuse LM & NTLM	ป้องกันการดักจับกุญแจรหัสผ่านบนเครือข่าย	
	Audit Account Logon Events	Success & Failure	บันทึกประวัติการเข้าสู่ระบบเพื่อสอบสวน Log	
	Audit Privilege Use & Policy Change	Success & Failure	บันทึกการใช้สิทธิ์แอดมินและการแก้ไข GPO	
Endpoint Protection	บังคับเปิดใช้งาน Windows Defender / EDR Agent	Enabled (Real-Time Protection On)	ป้องกันมัลแวร์และ Ransomware ตลอดเวลา	
	บังคับอัปเดต Security Signatures รายวัน	Enabled (Update every 4 hours)	อัปเดตฐานข้อมูลไวรัสล่าสุด	

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 91 / 107
--	---	---

[GW-TEC-03] ข้อกำหนดระบบสำรองข้อมูลคลาวด์และการแจ้งเตือนอัตโนมัติ

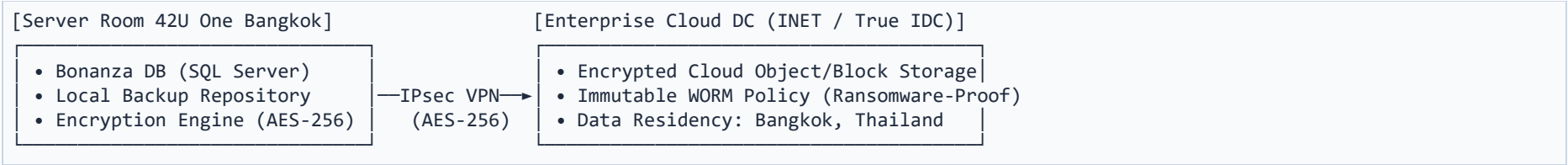
(Offsite Cloud Backup & Automated Alert Specification)

รหัสเอกสาร	GW-TEC-03	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	ระบบปลายทาง	Enterprise Cloud Tier III (INET / True IDC)

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณฑลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. สถาปัตยกรรมระบบสำรองข้อมูลภายนอก (Offsite Cloud Backup Architecture)

เพื่อรองรับกลยุทธ์ 3-2-1 และแผนความต่อเนื่องทางธุรกิจ ข้อมูลระบบจัดการกองทุน Bonanza และระบบโครงสร้างพื้นฐานจะถูกสำรองและส่งสำเนาไปยังศูนย์ข้อมูลคลาวด์มาตรฐานสากล Tier III ในประเทศไทย (รองรับเกณฑ์มาตรฐานทางเทคนิคของทั้ง INET Cloud และ True IDC) ผ่านอุโมงค์สัญญาณเครือข่ายเข้ารหัส FortiGate Site-to-Site IPsec VPN Tunnel:



2. ข้อกำหนดการแจ้งเตือนสถานะการสำรองข้อมูล (Automated Notification Matrix)

สถานะการสำรองข้อมูล	เงื่อนไขการตรวจจับ (Trigger Condition)	ช่องทางแจ้งเตือน (Channel)	ผู้รับการแจ้งเตือน (Recipient)	การดำเนินการตอบสนอง (Action Required)
● สถานะสำเร็จ (Success)	งาน Backup รายงานสำเร็จ 100% ข้อมูลครบถ้วนตาม Checksum	Email Daily Summary Report	IT Specialist	บันทึกประวัติลงใน Daily Backup Log ตามปกติ
● สถานะเตือน (Warning / Retry)	ส่งไฟล์ขึ้นคลาวด์ช้ากว่าปกติ หรือไฟล์ชั่วคราวบางส่วนติดล็อก	Email Alert + SMS/App Alert	IT Specialist	ระบบ Re-run อัตโนมัติใน 2 ชม. / ตรวจสอบแบนด์วิดท์
● สถานะล้มเหลววิกฤต (Critical Failure)	- งาน Backup ไม่ทำงานตามรอบ (Missed Job) - ข้อมูลเสียหาย / ติดต่อ Cloud Storage ไม่ได้ - มีความผิดพลาดเกิน 2 ครั้งติดต่อกัน	High-Priority Alert (Email, โทรศัพท์, ข้อความด่วน)	IT Specialist, CIO, และ MD	เข้าแก้ไขภายใน 1 ชั่วโมง / หากแก้ไขไม่ได้ใน 4 ชม. ให้รายงานผู้บริหารเพื่อเปิดแผนฉุกเฉิน

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 93 / 107
---	--	--

3. ตัวอย่างรูปแบบรายงานแจ้งเตือนทางอีเมล (Specimen Notification Email)

From: backup-alert@grandway.co.th
To: khanasin.k@grandway.co.th, it-alerts@grandway.co.th
Subject: [SUCCESS] Grandway Daily Cloud Backup - Bonanza DB & Core System (05-Oct-2026)

```
=====
GRANDWAY CAPITAL GROUP LIMITED - IT BACKUP OPERATIONS REPORT
=====
Backup Job Name   : JOB-DAILY-OFFSITE-BONANZA-PROD
Source Server     : GW-SRV-BONANZA01 (One Bangkok Server Room)
Target Location   : Offsite Cloud Tier III Storage (Vault: GW-OFFSITE-VAULT-01)
Encryption Status: AES-256 (GCM Mode) Encrypted & Verified
Status            : SUCCESS (100% Completed)
-----
Execution Start   : 05/10/2026 22:00:02
Execution End     : 05/10/2026 22:42:15 (Duration: 42 mins 13 secs)
Total Data Size   : 142.8 GB
Transferred Size  : 18.4 GB (Deduplicated & Compressed)
Integrity Hash    : SHA256: 8f4e2b1c9a7d3e5f... (MATCHED)
Next Scheduled    : 06/10/2026 22:00:00
=====
This is an automated system notification from Grandway ISMS Infrastructure.
```

[GW-TEC-04] เมทริกซ์สิทธิการใช้งานระบบงานหลักกองทุน (Bonanza RBAC Matrix)

(Master User Access Matrix: Bonanza Core System RBAC)

รหัสเอกสาร	GW-TEC-04	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	ระบบเป้าหมาย	ระบบจัดการกองทุนส่วนบุคคล Bonanza Investment

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งลิขิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณชุลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์และการแบ่งแยกหน้าที่ (SoD Principles)

ตารางเมทริกซ์นี้กำหนดสิทธิ์การเข้าถึงและการทำธุรกรรมในระบบจัดการกองทุนส่วนบุคคลหลัก (Bonanza Investment Core System) โดยยึดหลักการแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties: SoD) และระบบสองคนตรวจทาน (Maker-Checker Dual Control) เพื่อป้องกันความขัดแย้งทางผลประโยชน์ตามเกณฑ์ ก.ล.ต. สธ. 38/2565

2. ตารางเมทริกซ์สิทธิตามโมดูลระบบ Bonanza Investment (Core Module Access Matrix)

โมดูลระบบ Bonanza (Module Name)	Fund Manager	Trader	Settlement / Back Office	Compliance	IT	Managing
---------------------------------	--------------	--------	--------------------------	------------	----	----------

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.		ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite			รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 95 / 107	
	(ผู้จัดการกองทุน)	(เจ้าหน้าที่ส่งคำสั่ง)		Officer	Specialist (ผู้ดูแลระบบ)	Director (MD)
1. Customer & Portfolio Profile เปิดพอร์ต/บันทึกนโยบายลงทุน	Create / Edit (Maker)	Read-Only	Read-Only	Read-Only	No Access	Final Approval (Checker)
2. Investment Limit Monitoring ตรวจสอบเพดานความเสี่ยงกองทุน	Read-Only	Read-Only	Read-Only	Configure / Override	No Access	Read-Only
3. Order Creation (ส่งคำสั่งลงทุน) สร้างคำสั่งซื้อขายหลักทรัพย์	Create / Submit (Maker)	No Access	No Access	Read-Only	No Access	Approval (กรณีพิเศษ)
4. Order Execution (เคาะคำสั่งซื้อขาย) ส่งคำสั่งเข้าตลาดหลักทรัพย์	No Access	Execute Only (Checker/Trader)	No Access	Read-Only	No Access	No Access
5. Post-Trade Clearing & Settlement กระทบยอดและยืนยันการชำระราคา	No Access	No Access	Execute & Confirm (Full Settlement)	Read-Only	No Access	Read-Only
6. NAV Calculation & Fee Billing คำนวณมูลค่าสินทรัพย์สุทธิและค่าธรรมเนียม	Read-Only	No Access	Calculate & Post	Read-Only	No Access	Approval
7. System Audit Trail & Logs ตรวจสอบประวัติการทำธุรกรรม	Read-Only (พอร์ตนตนเอง)	No Access	No Access	Full Audit View	System Level Log	Full Audit View
8. User & System Configuration ตั้งค่าพารามิเตอร์ระบบและผู้ใช้	No Access	No Access	No Access	Read-Only (สิทธิ์)	Configure User / System (ห้ามดูข้อมูลพอร์ต)	Approval

(คำอธิบายสิทธิ์: Create = สร้างรายการ, Edit = แก้ไขรายการ, Execute = ดำเนินการธุรกรรม, Read-Only = ดูได้อย่างเดียว, No Access = ไม่มีสิทธิ์เข้าถึง)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 96 / 107
--	---	---

[GW-TEC-05] ข้อกำหนดรูปแบบ Audit Trail และการบันทึกประวัติธุรกรรมระบบกองทุน

(Bonanza Activity Log & Audit Trail Technical Specification)

รหัสเอกสาร	GW-TEC-05	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	ระบบเป้าหมาย	ระบบ Bonanza Investment Core Database

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสธรา ตั้งลิขานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณชุลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

เอกสารฉบับนี้กำหนดโครงสร้างข้อมูล รูปแบบฟิลด์ และมาตรฐานการจัดเก็บบันทึกประวัติการทำธุรกรรม (Audit Trail / Activity Log) บนระบบจัดการกองทุนส่วนบุคคล Bonanza Investment เพื่อให้มีร่องรอยการตรวจสอบที่สมบูรณ์ ป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation) และสอดคล้องกับข้อกำหนดของสำนักงาน ก.ล.ต. ตามประกาศ สธ. 38/2565

2. โครงสร้างฟิลด์ข้อมูลการบันทึก Log (Mandatory Log Schema)

ลำดับ	ชื่อฟิลด์ (Field)	ประเภทข้อมูล (Data Type)	ตัวอย่างข้อมูล (Example Value)	คำอธิบายรายละเอียด
-------	-------------------	--------------------------	--------------------------------	--------------------

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.		ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite			รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 97 / 107
	Name)				
1	`EventID`	UUID / String	`a8f5b120-7e3a-4d29-91fb-6e42b26090c1`	รหัสอ้างอิงเฉพาะของแต่ละเหตุการณ์ (Unique Event Identifier)	
2	`Timestamp`	ISO 8601 (UTC+7)	`2026-10-05T14:30:15.124+07:00`	วันและเวลาที่เกิดเหตุการณ์ ละเอียดถึงระดับมิลลิวินาที	
3	`UserID`	String	`soracha.t`	บัญชีผู้ใช้งานที่กระทำการรายการ (User Identity)	
4	`UserRole`	String	`FundManager`	บทบาทหน้าที่ของพนักงานขณะทำการรายการ	
5	`ClientIP`	IPv4 / IPv6	`192.168.20.105`	หมายเลข IP ต้นทางของเครื่องคอมพิวเตอร์	
6	`ActionType`	Enum	`ORDER_CREATE`, `PORTFOLIO_EDIT`	ประเภทการกระทำ เช่น สร้างคำสั่ง, อนุมัติ, แก้ไขข้อมูล	
7	`TargetEntity`	String	`Portfolio:GW-PF-0089`	วัตถุหรือระบบที่ถูกกระทำ	
8	`OldValue`	JSON / Text	`{"Allocation_Cash": 25.0}`	ค่าข้อมูลก่อนการแก้ไข (สำหรับรายการประเภท UPDATE/DELETE)	
9	`NewValue`	JSON / Text	`{"Allocation_Cash": 10.0}`	ค่าข้อมูลใหม่หลังการแก้ไข	
10	`Status`	Enum	`SUCCESS` / `FAILED` / `REJECTED`	สถานะผลลัพธ์ของการกระทำ	
11	`SessionID`	String	`SESS-987214-XYZ`	รหัสเซสชันการเชื่อมต่อของผู้ใช้	
12	`HashSignature`	SHA-256 Hash	`e3b0c44298fc1c149afb4c8996fb92427ae41e...`	ค่าแฮชคำนวณจากฟิลด์ทั้งหมดเพื่อป้องกันการดัดแปลงย้อนหลัง	

3. ตัวอย่างการบันทึก Log ในรูปแบบ JSON (Specimen Audit Log Entry)

```
{
  "EventID": "a8f5b120-7e3a-4d29-91fb-6e42b26090c1",
  "Timestamp": "2026-10-05T14:30:15.124+07:00",
  "UserID": "soracha.t",
  "UserRole": "FundManager",
  "ClientIP": "192.168.20.105",
  "MACAddress": "00:1A:2B:3C:4D:5E",
```

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 98 / 107
<pre>"ActionType": "ORDER_CREATE", "TargetEntity": "Order:ORD-20261005-0042", "Details": { "PortfolioID": "GW-PF-0089", "Symbol": "PTT.BK", "Side": "BUY", "Quantity": 50000, "LimitPrice": 34.50, "OrderValue": 1725000.00 }, "Status": "SUCCESS", "SessionID": "SESS-987214-XYZ", "HashSignature": "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855" }</pre>		

4. มาตรการเก็บรักษาและอายุการจัดเก็บ (Log Retention Rules)

- 1. การเก็บรักษาด้านการซื้อขายและธุรกรรมพอร์ต (Trading & Portfolio Records): ต้องจัดเก็บไว้ในระบบ ไม่น้อยกว่า 5 - 10 ปี ตามพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์
- 2. การป้องกันการแก้ไข (Tamper-Proofing): ข้อมูล Audit Trail ถูกเขียนลงในฐานข้อมูลแบบ Append-Only และถูกสำรองไปยัง WORM Storage บนระบบคลาวด์ทุกวันทำการ

[GW-TEC-06] ทะเบียนคุมทรัพย์สินอุปกรณ์เทคโนโลยีสารสนเทศหลัก (Asset Register)

(Master IT Hardware Asset Register)

รหัสเอกสาร	GW-TEC-06	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	รอบการตรวจสอบ	ตรวจนับทางกายภาพปีละ 1 ครั้ง

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาธิปไตย ก้านจักร IT Specialist	นายโสรชา ตั้งลิขิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณชลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569

1. วัตถุประสงค์ (Objective)

ทะเบียนคุมทรัพย์สินสารสนเทศฉบับนี้ใช้สำหรับบันทึกและติดตามอุปกรณ์ฮาร์ดแวร์ อุปกรณ์เครือข่าย เซิร์ฟเวอร์ และคอมพิวเตอร์พนักงานทั้งหมดของ บริษัท แกรนด์เวย์ แคปิตอล กรุ๊ป จำกัด เพื่อการควบคุมวงจรชีวิตทรัพย์สินและรองรับการตรวจสอบของสำนักงาน ก.ล.ต. ตามประกาศ สธ. 38/2565

2. ตารางทะเบียนคุมทรัพย์สินสารสนเทศหลัก (Master Hardware Inventory Table)

รหัสทรัพย์สิน	หมวดหมู่	รายการอุปกรณ์ / รุ่น (Model)	Serial Number	Hostname / IP Address	ผู้ถือครอง / แผนก	สถานที่ติดตั้ง	สถานะการเข้าถึง	สถานะอุปกรณ์
---------------	----------	------------------------------	---------------	-----------------------	-------------------	----------------	-----------------	--------------

(Asset Tag)								
GW-HW-SRV-001	Server	Dell PowerEdge R650 (Bonanza DB)	7X9K2M3	`srv-bonanza-db01` 192.168.30.10	ฝ่ายไอที / กองทุน	Server Room (U29-32)	TDE / BitLocker	ใช้งานปกติ (Active)
GW-HW-SRV-002	Server	Dell PowerEdge R650 (AD & Apps)	8Y1L3N4	`srv-ad-dc01` 192.168.10.10	ฝ่ายไอที	Server Room (U25-28)	BitLocker	ใช้งานปกติ (Active)
GW-HW-FW-001	Firewall	FortiGate 70F (Primary)	FGT70FTK21000451	`gw-fw-pri01` 192.168.10.1	ฝ่ายไอที	Server Room (U37)	Hardware Crypto	ใช้งานปกติ (Active)
GW-HW-FW-002	Firewall	FortiGate 70F (HA Standby)	FGT70FTK21000452	`gw-fw-sec01` 192.168.10.2	ฝ่ายไอที	Server Room (U36)	Hardware Crypto	พร้อมสำรอง (Standby)
GW-HW-SW-001	Switch	UniFi Enterprise 48-PoE Switch	UBNT48P-99214	`gw-sw-core01` 192.168.10.3	ฝ่ายไอที	Server Room (U34-35)	SSH Key Auth	ใช้งานปกติ (Active)
GW-HW-NAS-001	Storage	Synology RackStation NAS 12-Bay	SYN-RS1221-881	`gw-nas-bkup01` 192.168.10.20	ฝ่ายไอที	Server Room (U21-24)	AES-256 Volume	ใช้งานปกติ (Active)
GW-HW-UPS-001	Power	APC Smart-UPS Online 3kVA	APC3K-TH2026-01	NMC IP: 192.168.10.50	ฝ่ายไอที	Server Room (U07-10)	N/A	ใช้งานปกติ (Active)
GW-HW-NB-001	Laptop	Lenovo ThinkPad X1 Carbon Gen 11	PF4A9812	`gw-nb-akanit` DHCP (VLAN 20)	นายเอกณัฐ (MD)	ผู้บริหาร / พกพา	BitLocker (AES-256)	ใช้งานปกติ (Active)
GW-HW-NB-002	Laptop	Lenovo ThinkPad X1 Carbon Gen 11	PF4A9813	`gw-nb-soracha` DHCP (VLAN 20)	น.ส.โสธรา (CIO)	กองทุน / พกพา	BitLocker (AES-256)	ใช้งานปกติ (Active)
GW-HW-NB-003	Laptop	Lenovo ThinkPad P1 Gen 6	PF4B1104	`gw-nb-khanasin` DHCP (VLAN 10/20)	นายคณาธิลป์ (IT)	ฝ่ายไอที / พกพา	BitLocker (AES-256)	ใช้งานปกติ (Active)

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.		ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite					รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 101 / 107	
GW-HW-NB-004	Laptop	Lenovo ThinkPad T14 Gen 4	PF4C2215	`gw-nb-trader01` DHCP (VLAN 20)	Trading Desk (Trader)	สำนักงาน One Bangkok	BitLocker (AES- 256)	ใช้งานปกติ (Active)
GW-HW-NB-005	Laptop	Lenovo ThinkPad T14 Gen 4	PF4C2216	`gw-nb-settle01` DHCP (VLAN 20)	Settlement Officer	สำนักงาน One Bangkok	BitLocker (AES- 256)	ใช้งานปกติ (Active)

3. รอบการตรวจสอบและการปรับปรุงข้อมูล (Maintenance & Audit Routine)

- 1. การอัปเดตข้อมูลแบบเรียลไทม์: เมื่อมีการจัดซื้อ ยืมคืน โอนย้าย หรือส่งซ่อมอุปกรณ์ IT Specialist ต้องบันทึกสถานะในทะเบียนคุมภายใน 24 ชั่วโมง
- 2. การตรวจนับประจำปี (Annual Physical Stock Verification): ฝ่าย IT ร่วมกับฝ่ายบัญชีตรวจนับทรัพย์สินจริงเทียบกับทะเบียนคุมทุกไตรมาสที่ 4 ของปี

 บจ. แกรนด์เวย์ แคปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก Master IT Operations & Cyber Security Suite	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 102 / 107
--	---	--

[GW-TEC-07] ผังโครงสร้างเครือข่ายความมั่นคงปลอดภัยและการแยก VLAN (8 VLANs)

(Enterprise Network Architecture & VLAN Segmentation Specification)

รหัสเอกสาร	GW-TEC-07	ฉบับที่ (Rev.)	2.0
หน่วยงานรับผิดชอบ	ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)	วันที่มีผลบังคับใช้	1 พฤศจิกายน 2569
ระดับชั้นความลับ	ลับเฉพาะภายใน (Confidential)	สถานที่ติดตั้ง	สำนักงานใหญ่ ชั้น 38 อาคาร วัน แบงค็อก

ผู้จัดทำ (Prepared By)	ผู้สอบทาน (Reviewed By)	ผู้อนุมัติ (Approved By)
นายคณาสีลป์ ก้านจักร IT Specialist	นายโสธรา ตั้งจิตานนท์ Chief Investment Officer (CIO) / Compliance	นายเอกณัฐ กุณขลบุตร กรรมการผู้จัดการ (Managing Director)
วันที่: / / 2569	วันที่: / / 2569	วันที่: / / 2569



บจ. แกรนด์เวย์ แคปปิตอล กรุ๊ป
Grandway Capital Group Ltd.

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)
คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก
Master IT Operations & Cyber Security Suite

รหัสเอกสาร: GW-IT-MANUAL-2026

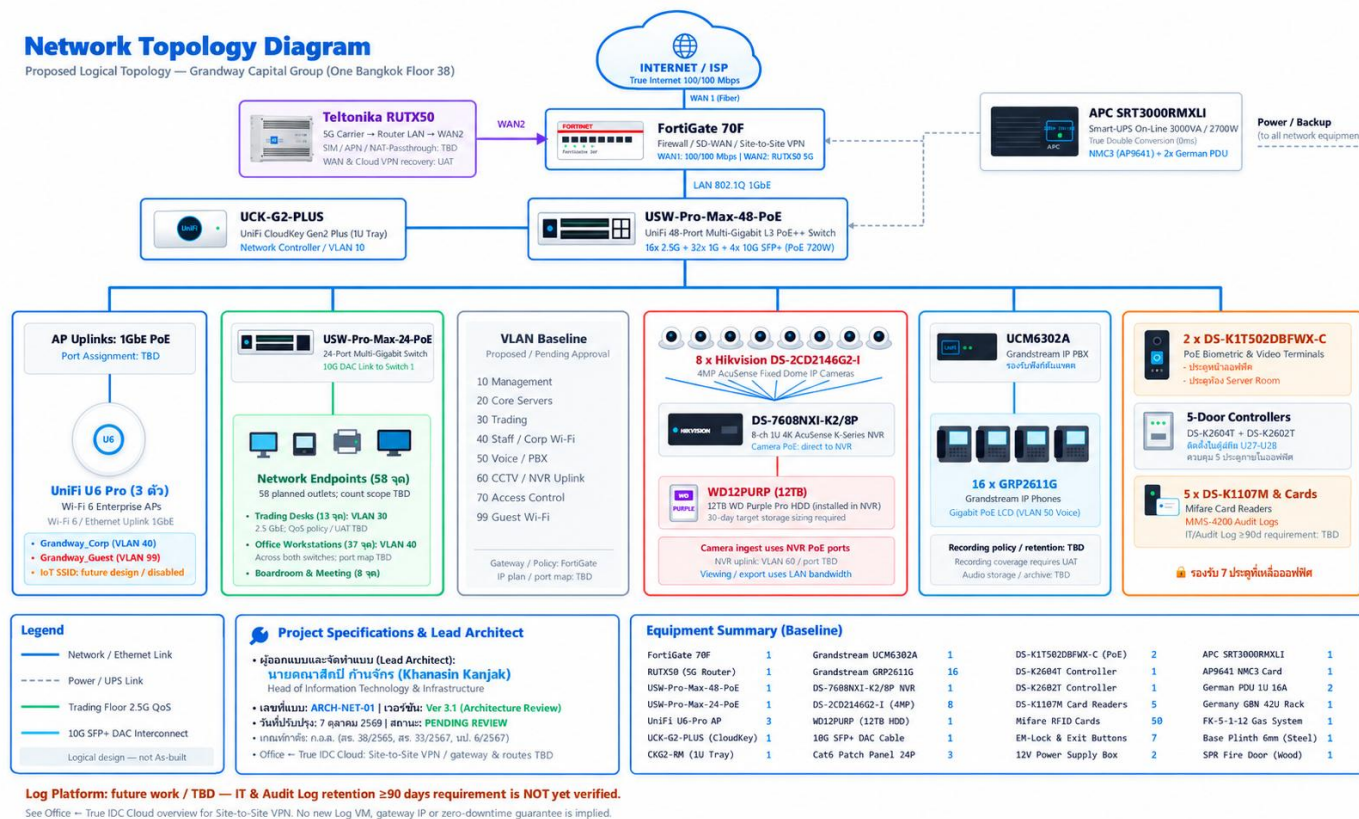
ฉบับที่ (Rev): 2.0

วันที่มีผล: 01/11/2569

ชั้นความลับ: Confidential

หน้าที่: 103 / 107

1. แผนผังโครงสร้างสถาปัตยกรรมเครือข่ายองค์กร (Network Topology Diagram — Revision 3.1)



รูปภาพ: แผนผังโครงสร้างสถาปัตยกรรมเครือข่ายองค์กร (Grandway Enterprise Network Topology Revision 3.1) — แยก 8 VLANs และ FortiGate Next-Gen Firewall



บจ. แกรนด์เวย์ แคปปิตอล กรุ๊ป
Grandway Capital Group Ltd.

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)

คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก

Master IT Operations & Cyber Security Suite

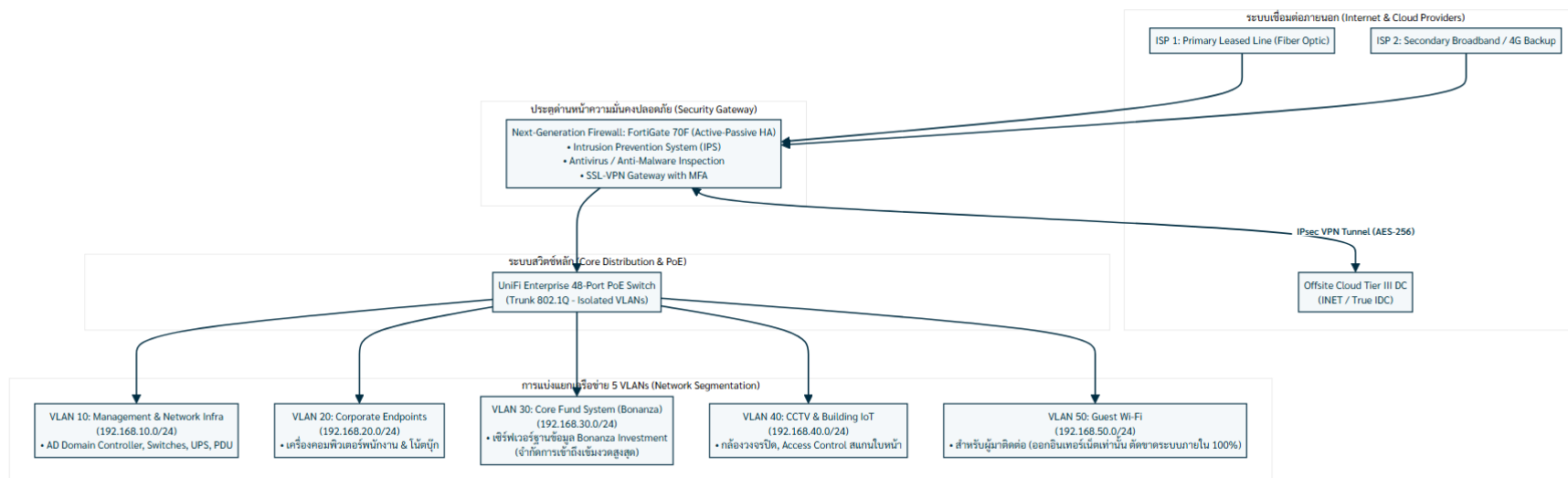
รหัสเอกสาร: GW-IT-MANUAL-2026

ฉบับที่ (Rev): 2.0

วันที่มีผล: 01/11/2569

ชั้นความลับ: Confidential

หน้าที่: 104 / 107



รูปภาพ: ผังกระบวนการปฏิบัติงานเชิงระบบ (Operational Workflow Flowchart) — GW-TEC-07 ผังโครงสร้างเครือข่ายความมั่นคงปลอดภัยและการแยก VLAN (8 VLANs)

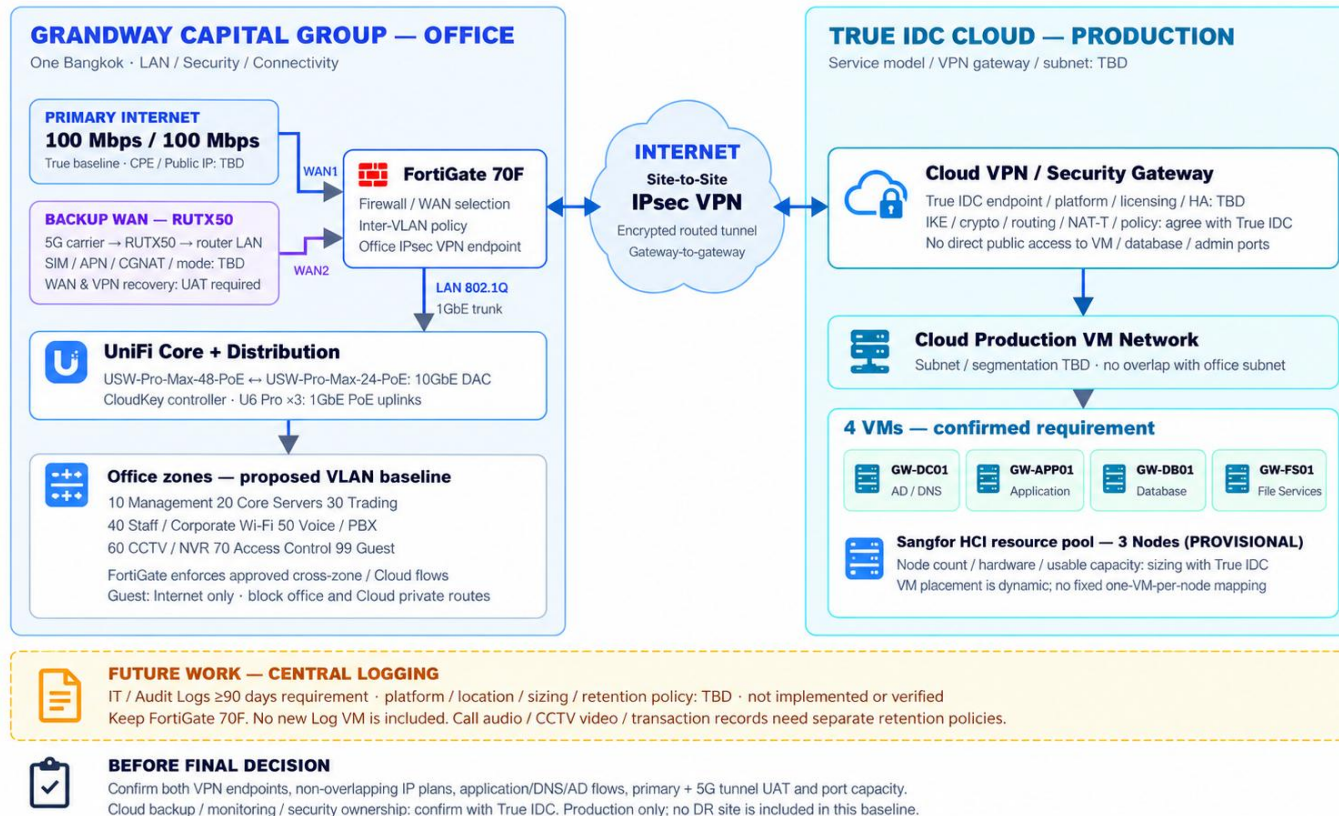
2. ตารางการแบ่งแยกเครือข่ายและการควบคุมเส้นทางข้อมูล (8-VLAN & Routing Matrix)

รหัส VLAN	ชื่อเครือข่าย (VLAN Name)	ช่วงไอพีแอดเดรส (IP Subnet)	นโยบายการควบคุมและสิทธิ์การเชื่อมต่อ (Firewall Policy Rules)
VLAN 10	Management & Infra	`10.10.10.0/24`	- เข้าถึงได้เฉพาะผู้ดูแลระบบไอที (IT Admin) ผ่านเครื่องที่กำหนดและผ่าน MFA - ห้าม VLAN อื่นเข้าถึงโดยตรง ยกเว้นพอร์ตบริการจำเป็น (DNS, NTP)
VLAN 20	Server Zone	`10.10.20.0/24`	- โซนเซิร์ฟเวอร์ภายในสำนักงาน (สำรองไว้ / Local NAS Backup) - ไม่อนุญาตให้ออก Internet โดยตรง เชื่อมโยง Cloud ผ่าน IPsec VPN
VLAN 30	Trading Zone	`10.10.30.0/24`	- โซนธุรกรรมกองทุน (Restricted Trading Zone) ตามเกณฑ์ ก.ล.ด. - ควบคุมสิทธิ์เข้มงวด บันทึก Audit Log ครบถ้วน ได้รับ Bandwidth สูงสุด
VLAN 40	Corporate Staff	`10.10.40.0/24`	- สำหรับเครื่องพนักงานบริษัทที่ Join Domain Entra ID / Active Directory - มี Web Filtering ป้องกันมัลแวร์ และบล็อกเว็บไซต์เสี่ยง
VLAN 50	Voice / IP-PBX	`10.10.50.0/24`	ระบบโทรศัพท์ไอพีและการบันทึกเสียงสนทนาการส่งข้อมูลหลักทรัพย์สิน
VLAN 60	CCTV Video	`10.10.60.0/24`	- ส่งสัญญาณภาพตรงเข้า NVR PoE บันทึกภาพย้อนหลังตามนโยบาย - ตัดขาดจากเน็ตเวิร์กพนักงาน การดูย้อนหลังทำผ่าน NVR Software เฉพาะ
VLAN 70	Access Control	`10.10.70.0/24`	ระบบควบคุมประตูสแกนใบหน้าและบัตรผ่านเข้าห้อง Server และสำนักงาน
VLAN 99	Guest Wi-Fi	`10.10.99.0/24`	สำหรับผู้มาติดต่อ (ออกอินเทอร์เน็ตเท่านั้น ตัดขาดจาก VLAN อื่น 100%)

3. สถาปัตยกรรมการเชื่อมต่อ True IDC Cloud และการเข้าถึงระยะไกล (Hybrid Cloud & VPN)

GW | OFFICE ↔ TRUE IDC CLOUD

Production connectivity overview · Revision 3.1 · 07 Oct 2026 · Architecture Review / Pending Decision



รูปภาพ: สถาปัตยกรรมไฮบริดคลาวด์เชื่อมโยงระบบกองทุน (Hybrid Cloud Architecture: One Bangkok ↔ True IDC Tier III Cloud)

1. การเชื่อมต่อสำนักงาน ↔ True IDC Cloud (Site-to-Site IPsec VPN):

 GRANDWAY บจ. แกรนด์เวย์ แคปปิตอล กรุ๊ป Grandway Capital Group Ltd.	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) คู่มือระเบียบปฏิบัติการเทคโนโลยีสารสนเทศเล่มหลัก <i>Master IT Operations & Cyber Security Suite</i>	รหัสเอกสาร: GW-IT-MANUAL-2026 ฉบับที่ (Rev): 2.0 วันที่มีผล: 01/11/2569 ชั้นความลับ: Confidential หน้าที่: 107 / 107
--	--	---

- เชื่อมโยงอุโมงค์นิรภัย IPsec VPN เข้ารหัส AES-256 ระหว่าง FortiGate 70F สำนักงานใหญ่ ชั้น 38 One Bangkok กับ Cloud Gateway ของ True IDC
- รองรับการเข้าถึงระบบงานแกนหลัก (4 VMs: GW-DC01, GW-APP01, GW-DB01, GW-FS01) อย่างไรก็ดี

2. การเข้าถึงระยะไกลสำหรับผู้บริหารและพนักงาน (Secure SSL-VPN):

- การเข้าทำงานจากภายนอก (WFH / Travel) ต้องเชื่อมต่อผ่าน **FortiGate SSL-VPN**
- บังคับใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (**Multi-Factor Authentication: MFA**) ด้วย TOTP / Push Notification บนมือถือ
- กำหนดสิทธิ์การเข้าถึงตามหลัก Least Privilege เข้าถึงได้เฉพาะระบบที่ได้รับมอบหมายเท่านั้น