ตารางแสดงรายละเอียดการจัดเก็บหลักฐาน

ประเภทหลักฐานที่ต้องจัดเก็บ	รายละเอียดขั้นต่ำ	ระยะเวลาจัดเก็บขั้นต่ำ
หลักฐานการเข้าถึงพื้นที่หวงห้าม (physical access log)	บุคคลที่เข้าถึง / วันเวลาที่ผ่านเข้าออก / ความพยายามในการเข้าถึง (ถ้ามี)	ไม่น้อยกว่า 3 เดือน
หลักฐานการเข้าถึงระบบปฏิบัติการฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์ (authentication log)	บัญชีผู้ใช้งาน / วันและเวลาที่เข้าใช้งาน / ความพยายามในการเข้าใช้งาน	ไม่น้อยกว่า 3 เดือน
หลักฐานการเข้าถึงและใช้งานระบบสารสนเทศ (application log) ของบุคคลที่สามารถเข้าถึงข้อมูล	บัญชีผู้ใช้งาน / หมายเลขประจำเครื่องที่ใช้งาน (IP address) / วันและเวลาที่เข้าใช้งาน --- กรณีที่เป็นระบบสารสนเทศเพื่อการซื้อขายหลักทรัพย์ (trading system) ให้เพิ่มรายละเอียดชื่อย่อหลักทรัพย์ (securities symbol) / หมายเลขบริษัทสมาชิก (broker No. 4 หลัก : xxxx) / เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET order ID) / เลขที่บัญชีซื้อขายหลักทรัพย์ (account ID) / วันและเวลาในการส่งคำสั่งซื้อขายหลักทรัพย์ (yyyy/mm/dd - hh:mm:ss:sss) / หมายเลข Public และ Local IP address ต้นทาง (source) / หมายเลข IP address ปลายทาง (destination) / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) / terminal type (ถ้ามี) เช่น iPad, iPhone เป็นต้น --- ทั้งนี้ ผู้ประกอบธุรกิจต้องสามารถระบุตัวตนผู้ใช้งานและ local IP address ในช่วงเวลาที่ใช้งานได้ (เฉพาะการใช้งานผ่านอุปกรณ์ของบริษัท)	ไม่น้อยกว่า 1 ปี สำหรับผู้ประกอบธุรกิจนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์ซึ่งมิได้จำกัดเฉพาะหลักทรัพย์อันเป็นตราสารแห่งหนี้หรือหน่วยลงทุน และตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า ไม่น้อยกว่า 6 เดือน สำหรับผู้ประกอบธุรกิจประเภทอื่น
หลักฐานการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจ (internet access log) (“a	บัญชีผู้ใช้งาน / หมายเลขประจำเครื่องที่ใช้งาน (IP address) / หมายเลขอินเทอร์เน็ตของผู้ประกอบธุรกิจ (organization IP address) / วันเวลาที่มีการใช้งาน / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) --- ทั้งนี้ ผู้ประกอบธุรกิจต้องสามารถระบุตัวตนผู้ใช้งานและ IP address ในช่วงเวลาที่ใช้งานได้	
หลักฐานการใช้งานแฟ้มข้อมูล (audit log)*	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / บันทึกการเรียกดูและการแก้ไขข้อมูล	ไม่น้อยกว่า 6 เดือน
หลักฐานการบริหาร (event log) ระบบปฏิบัติการ และ network firewall	วันและเวลาที่เกิดเหตุการณ์ / เหตุการณ์ที่เกิดขึ้นกับ OS (event services) เช่น สถานะการให้บริการของ service / เหตุการณ์ที่เกิดขึ้นกับ network firewall เช่น การปรับปรุงหรือแก้ไข firewall rules	ระยะเวลาตามที่จำเป็นและเพียงพอสำหรับการตรวจสอบซึ่งสอดคล้องกับความเสี่ยงที่ผู้ประกอบธุรกิจได้ประเมินไว้
หลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ของ network firewall (network firewall log)	วันและเวลา / IP address ต้นทาง (source) และปลายทาง (destination) / firewall action / port ที่ใช้ติดต่อ	
หลักฐานการจัดการบริหารข้อมูล (database log)	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน	
หลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging)**	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / ข้อมูลการติดต่อตลอดระยะเวลาการสนทนา	ไม่น้อยกว่า 6 เดือน

ผู้ประกอบธุรกิจทุกประเภท

** จัดเก็บเฉพาะบุคคลที่สามารถเข้าถึงข้อมูลภายใน (“access person”) ของผู้ประกอบธุรกิจนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์ ซึ่งมิได้จำกัดเฉพาะหลักทรัพย์อันเป็นตราสารแห่งหนี้ หรือหน่วยลงทุน ตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า และผู้ประกอบธุรกิจจัดการกองทุนรวมหรือกองทุนส่วนบุคคล เท่านั้น

*** นิยามว่าด้วย access person ให้เป็นไปตามประกาศแนวปฏิบัติว่าด้วยการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า