

เลขที่.....



## สัญญาการรักษาความลับระบบสารสนเทศ

สัญญาฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา และหลักปฏิบัติสากล ที่เกี่ยวข้องกับการรักษาความลับของข้อมูลต่าง ๆ ที่อยู่ในความครอบครองหรือควบคุมดูแลของสำนักงานคณะกรรมการอาหารและยา

ตามสัญญาฉบับนี้ ข้าพเจ้าขอรับรองว่าจะเก็บรักษาเอกสารและข้อมูลต่าง ๆ ของสำนักงานคณะกรรมการอาหารและยา ที่ไม่สามารถเผยแพร่แก่บุคคลอื่นได้ ไว้เป็นความลับ โดยข้าพเจ้ารับรองว่าจะดำเนินการตามข้อกำหนดดังต่อไปนี้

### 1. ข้อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

#### 1.1 การใช้งานรหัสผ่าน

- (1) ต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) โดยมีบัญชีชื่อผู้ใช้งานของตนเอง และห้ามใช้ร่วมกับผู้อื่น รวมทั้ง ห้ามเผยแพร่ แจกจ่าย หรือให้ผู้อื่นล่วงรู้รหัสผ่าน
- (2) ต้องกำหนดรหัสผ่านให้ประกอบด้วยตัวอักษรไม่น้อยกว่า 8 ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)
- (3) ไม่กำหนดรหัสผ่านของบัญชีผู้ใช้ของตนเองจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว
- (4) ไม่ใช้รหัสผ่านของบัญชีผู้ใช้ของตนเองในการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- (5) ไม่ใช้ฟังก์ชันหรือโปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านแบบอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- (6) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- (7) เปลี่ยนรหัสผ่านในทุก 90 วัน หรือ ทุกครั้งได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

1.2 การนำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ ต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 และต้องใช้วิธีการเข้ารหัสที่เป็นมาตรฐานสากล

1.3 การกระทำใด ๆ ที่เกิดจากการใช้บัญชีผู้ใช้งานของตนเอง ที่มีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าจะกระทำนั้น จะเกิดจากตนเองหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบของเจ้าของบัญชีผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

1.4 ต้องพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ระบบคอมพิวเตอร์หรือระบบสารสนเทศของสำนักงาน หากเกิดปัญหาในการพิสูจน์ตัวตนนั้น ไม่ว่าจะจากการล็อกของรหัสผ่าน หรือจากความผิดพลาดใด ๆ ก็ตาม ต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

(1) ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนเข้าถึงระบบปฏิบัติการของคอมพิวเตอร์ทุกประเภท

(2) ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนการใช้งานระบบคอมพิวเตอร์อื่นในเครือข่าย

(3) ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนการใช้งานอินเทอร์เน็ต และต้องบันทึกข้อมูลซึ่งสามารถระบุตัวตนของผู้ใช้งานได้

(4) ต้องล็อกหน้าจอทุกครั้ง เมื่อผู้ใช้งานไม่อยู่ที่คอมพิวเตอร์ และ ต้องพิสูจน์ตัวตนทุกครั้งก่อนกลับมาใช้งานระบบสารสนเทศต่อ

(5) ต้องตั้งเวลาพักหน้าจอ (Screen Saver) ให้กับคอมพิวเตอร์ทุกเครื่อง โดยเริ่มพักหน้าจอหลังจากที่ผู้ใช้หยุดการใช้งานเป็นเวลา 10 นาที

1.5 ต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าจะข้อมูลนั้นจะเป็นของสำนักงาน หรือเป็นของบุคคลภายนอก

1.6 ต้องไม่เผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูง

1.7 ต้องร่วมกันดูแลรักษาและรับผิดชอบต่อข้อมูลของสำนักงาน และข้อมูลของบุคคลภายนอกหากเกิดการสูญหาย หรือ นำไปใช้ในทางที่ผิด หรือเผยแพร่โดยไม่ได้รับอนุญาต หากเกิดความเสียหายจากกรณีดังกล่าว ต้องมีส่วนร่วมรับผิดชอบต่อความเสียหายนั้นด้วย

1.8 ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ

1.9 มีสิทธิเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลของตนเองตามสมควร ยกเว้นในกรณีที่สำนักงานต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับสำนักงาน ซึ่งสำนักงานอาจแต่งตั้งผู้ทำหน้าที่ตรวจสอบ เพื่อตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

1.10 ห้ามใช้งานโปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายที่กำหนดให้คอมพิวเตอร์ในเครือข่ายแต่ละเครื่อง มีแฟ้มข้อมูลเก็บไว้ในตัวเอง ซึ่งผู้ใช้สามารถใช้แฟ้มข้อมูลจากคอมพิวเตอร์ แทนการใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือ โปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับการอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

1.11 ห้ามใช้งานโปรแกรมออนไลน์เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

1.12 ห้ามใช้สินทรัพย์ของสำนักงาน เผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรมความมั่นคงของประเทศ กฎหมาย หรือ กระทบต่อภารกิจของสำนักงาน

1.13 ห้ามใช้สินทรัพย์ของสำนักงาน เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของสำนักงาน

1.14 ไม่ใช่สินทรัพย์ของสำนักงาน เพื่อประโยชน์ทางการค้า

1.15 ไม่กระทำการใด ๆ เพื่อดักข้อมูล ไม่ว่าจะข้อมูล ข้อความ ภาพ เสียง หรือสิ่งอื่นใดในระบบเครือข่ายของสำนักงาน ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

1.16 ไม่รบกวน ทำลาย หรือทำให้ระบบสารสนเทศของสำนักงานต้องหยุดชะงัก

1.17 ห้ามใช้ระบบสารสนเทศของสำนักงาน เพื่อการควบคุมคอมพิวเตอร์ หรือ ระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

1.18 ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานระบบคอมพิวเตอร์หรือระบบสารสนเทศหรือดักจับรหัสผ่านของผู้อื่น ไม่ว่าจะเข้าไปเพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากร หรือเพื่อการอื่นใดก็ตาม

1.19 ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบคอมพิวเตอร์ หรือระบบเครือข่าย หรือระบบสารสนเทศของสำนักงาน โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

1.20 การควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear desk and clear screen policy) ผู้ใช้งานต้องควบคุมเอกสาร ข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บหรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

## 2. ข้อกำหนดด้านการบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and Intellectual Property and Preventing Malware)

2.1 ซอฟต์แวร์ที่สำนักงานอนุญาตให้ใช้งาน หรือที่สำนักงานมีลิขสิทธิ์ ให้ขอใช้งานได้ตามหน้าที่และความจำเป็น โดยห้ามติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิด

2.2 ซอฟต์แวร์ที่สำนักงานจัดเตรียมไว้ให้ถือเป็นสิ่งจำเป็น ห้ามติดตั้ง ถอดถอนเปลี่ยนแปลงแก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ยกเว้นได้รับการอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ หรือผู้ที่มีสิทธิในลิขสิทธิ์

2.3 ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti Virus) ตามที่สำนักงานประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องที่ใช้เพื่อการศึกษาหรือทดสอบที่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

2.4 ต้องตรวจสอบข้อมูล เพิ่มข้อมูล ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น เพื่อตรวจจับไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

2.5 ต้องปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น

2.6 ต้องระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ จะต้องแจ้งเหตุแก่ผู้ดูแลระบบ

2.7 เมื่อพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

2.8 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซิงข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของสำนักงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

2.9 ห้ามเผยแพร่ไวรัสคอมพิวเตอร์ โปรแกรมไม่ประสงค์ดี หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อสินทรัพย์ของสำนักงาน

2.10 ห้ามพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ในลักษณะหนึ่งลักษณะใดดังต่อไปนี้

(1) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยของระบบคอมพิวเตอร์ระบบเครือข่ายและระบบสารสนเทศ รวมทั้งการกระทำในลักษณะที่เป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลของบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

(2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(3) พัฒนาโปรแกรมใด ๆ ที่จะทำซ้ำตัวโปรแกรม หรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(5) สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ที่นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย

3. ข้อกำหนดด้านการควบคุมการใช้อินเทอร์เน็ต (Internet)

3.1 ต้องตรวจจับไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตทุกครั้ง

3.2 ห้ามใช้ระบบอินเทอร์เน็ต (Internet) ของสำนักงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับสำนักงาน

3.3 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

3.4 ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งาน จากระบบอินเทอร์เน็ต (Internet) และการปรับปรุงโปรแกรมต่าง ๆ ให้เป็นปัจจุบัน (Update) ต้องไม่ละเมิดลิขสิทธิ์

3.5 ห้ามเปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ผ่านกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) หรือ เครือข่ายสังคมออนไลน์ (Social Media)

3.6 ต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่ว ุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน หรือทำลายความสัมพันธ์กับบุคลากรของหน่วยงานภายนอก ผ่านกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) หรือ เครือข่ายสังคมออนไลน์ (Social Media)

3.7 ห้ามนำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก รวมทั้งต้องไม่เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

3.8 ต้องออกจากระบบอินเทอร์เน็ต (Internet) และปิดเว็บเบราว์เซอร์หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

3.9 ต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

#### 4. ระยะเวลาสัญญา

สัญญาฉบับนี้มีผลใช้บังคับตั้งแต่วันที่ลงนามเป็นต้นไป และมีกำหนดระยะเวลา 2 ปี นับแต่วันที่ ลงนามในสัญญานี้ เมื่อสัญญานี้ได้สิ้นสุดลงไม่ว่ากรณีใด ๆ ให้ข้อผูกพันในการเก็บความลับตามสัญญาฉบับนี้ยังคงมีผลใช้บังคับอยู่ตลอดไป

#### 5. ความรับผิด

ข้าพเจ้าทราบและตระหนักดีว่า การกระทำใด ๆ บนระบบสารสนเทศของสำนักงานคณะกรรมการอาหารและยาที่ขัดกับข้อกำหนดในสัญญาฉบับนี้ และข้อกำหนดตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา ถือเป็นความผิดต่อแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา และจะต้องได้รับผิดทางวินัยตามระเบียบราชการ และข้าพเจ้าทราบว่า จะต้องรับผิดชอบในทางแพ่งหรือต้องรับโทษทางอาญาตามบทบัญญัติของกฎหมายที่เกี่ยวข้องด้วย หากพบว่า การกระทำดังกล่าวเป็นความผิดตามกฎหมายนั้น

ลงชื่อ.....ผู้ให้สัญญา

(.....)

วันที่.....

ลงชื่อ.....พยาน

(.....)

วันที่.....

ลงชื่อ.....พยาน

(.....)

วันที่.....