นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานการทะเบียน จุฬาลงกรณ์มหาวิทยาลัย

ปรับปรุงล่าสุด: 8 ตุลาคม 2568

วัตถุประสงค์และขอบเขต

สำนักงานการทะเบียน จุฬาลงกรณ์มหาวิทยาลัย (สนท.) กำหนดนโยบายและแนวปฏิบัติฉบับนี้ขึ้นเพื่อเป็นแนวทางในการรักษาและบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้สารสนเทศมีความปลอดภัย มีความถูกต้องครบถ้วน สามารถรักษาความลับของข้อมูล มีความพร้อมในการให้บริการและพร้อมใช้งาน เพื่อป้องกันภัยคุกคามทางไซเบอร์ ลดความเสี่ยงจากช่องโหว่และผู้บุกรุกหรือเหตุละเมิด และเพื่อส่งเสริมให้มีการติดตาม เฝ้าระวัง และเตรียมพร้อมในการตอบสนองต่อภัยคุกคามทางไซเบอร์และการกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ

องค์ประกอบ

1. นโยบายความมั่นคงปลอดภัยด้านกายภาพ
2. นโยบายการรักษาความปลอดภัยของเครือข่าย
3. นโยบายการบริหารจัดการการเข้าถึงและควบคุมการใช้งานสารสนเทศ
4. นโยบายการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ไอทีของหน่วยงาน
5. นโยบายการดำเนินงานต่อเนื่องและแผนรองรับเหตุการณ์ฉุกเฉิน
6. นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคคล
7. นโยบายการตรวจสอบและประเมินความเสี่ยง
8. ภาคผนวก ก ลำดับชั้นความสำคัญของข้อมูลสารสนเทศด้านงานทะเบียน
9. ภาคผนวก ข การควบคุมการเข้าถึงฐานข้อมูลและการกำหนดสิทธิของผู้ใช้งานภายในสำนักงานการทะเบียน
10. ภาคผนวก ค การควบคุมการเข้าถึงและการกำหนดสิทธิของผู้ใช้งานภายนอกสำนักงานการทะเบียน

นิยาม

“สำนักงาน”	หมายถึง	สำนักงานการทะเบียน จุฬาลงกรณ์มหาวิทยาลัย
“ฝ่าย”	หมายถึง	สังกัดย่อยภายในสำนักงานการทะเบียน จุฬาลงกรณ์มหาวิทยาลัย อันประกอบด้วย ฝ่ายทะเบียนนิสิต ฝ่ายทะเบียนการศึกษา ฝ่ายบริหาร และฝ่ายเทคโนโลยีสารสนเทศ
“ฝ่ายเทคโนโลยีสารสนเทศ”	หมายถึง	ฝ่ายเทคโนโลยีสารสนเทศ สำนักงานการทะเบียน จุฬาลงกรณ์มหาวิทยาลัย ซึ่งให้บริการด้านเทคโนโลยีสารสนเทศ ดูแลฐานข้อมูลของสำนักงานการทะเบียน และบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายสารสนเทศภายในสำนักงานการทะเบียน
“ผู้อำนวยการ”	หมายถึง	ผู้อำนวยการสำนักงานการทะเบียน
“ผู้อำนวยการฝ่าย”	หมายถึง	ผู้อำนวยการฝ่าย สำนักงานการทะเบียน

“เจ้าหน้าที่”	หมายถึง	ข้าราชการ พนักงานมหาวิทยาลัย พนักงานวิสามัญ พนักงานจ้างเหมาบริการ ที่ปรึกษา ผู้เชี่ยวชาญ หรือบุคลากรอื่นใดของสำนักงานการทะเบียน
“ผู้ดูแลระบบ”	หมายถึง	เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลระบบคอมพิวเตอร์ หรือระบบฐานข้อมูล หรือระบบงานต่าง ๆ ภายในสำนักงานการทะเบียน
“หน่วยงานภายใน”	หมายถึง	ส่วนงานหรือหน่วยงานภายในจุฬาลงกรณ์มหาวิทยาลัย ซึ่งสนท. อนุญาตให้มีสิทธิในการเข้าถึงและใช้ข้อมูลของสนท. หรือเข้าใช้ระบบของสนท. ซึ่งจะได้รับสิทธิในการเข้าถึงและใช้ข้อมูลหรือเข้าใช้ระบบตามอำนาจหรือตามกรณีที่ได้รับอนุญาต
“หน่วยงานภายนอก”	หมายถึง	หน่วยงานของรัฐ องค์กร หรือบริษัทเอกชน ซึ่งสนท. อนุญาตให้มีสิทธิในการเข้าถึงและใช้ข้อมูลของสนท. หรือเข้าถึงระบบหรือสินทรัพย์ต่าง ๆ ของสนท. ซึ่งจะได้รับสิทธิในการเข้าถึงและใช้ข้อมูลหรือเข้าใช้ระบบตามกรณีที่ได้รับอนุญาต หรือตามข้อตกลงใด ๆ ที่ได้มีการลงนามร่วมกันไว้
“บุคลากรจุฬาฯ”	หมายถึง	ข้าราชการ พนักงานมหาวิทยาลัย พนักงานวิสามัญ พนักงานจ้างเหมาบริการ ที่ปรึกษา ผู้เชี่ยวชาญ หรือบุคลากรอื่นใดของหน่วยงานภายในจุฬาลงกรณ์มหาวิทยาลัย
“บุคคลภายนอก”	หมายถึง	บุคคลที่ไม่ใช่เจ้าหน้าที่ของสำนักงานการทะเบียน
“มหาวิทยาลัย”	หมายถึง	จุฬาลงกรณ์มหาวิทยาลัย
“นิสิต”	หมายถึง	นิสิตจุฬาลงกรณ์มหาวิทยาลัย และหมายรวมถึง บัณฑิตผู้สำเร็จการศึกษาจากจุฬาลงกรณ์มหาวิทยาลัย ผู้ศึกษาบางรายวิชา ผู้เรียนในโครงการการเรียนรู้ตลอดชีวิต (Lifelong Learning) และผู้ที่เคยศึกษาในจุฬาลงกรณ์มหาวิทยาลัยแต่ไม่สำเร็จการศึกษา
“สิทธิของผู้ใช้งาน”	หมายถึง	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสนท.
“ข้อมูลส่วนบุคคล”	หมายถึง	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อมตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
“เอกสาร”	หมายถึง	เอกสารข้อมูลที่อยู่ในรูปแบบกระดาษ

นโยบายความมั่นคงปลอดภัยด้านกายภาพ

นโยบายความมั่นคงปลอดภัยด้านกายภาพ กำหนดขึ้นเพื่อให้มีมาตรการและแนวทางในการควบคุมการเข้า-ออกอาคารและพื้นที่สำนักงาน การเข้า-ออกพื้นที่จำกัดการเข้าถึง การติดตั้งและใช้งานห้องควบคุมระบบ การจัดทำบัญชีทรัพย์สินและการควบคุมทรัพย์สิน ตลอดจนการเก็บรักษาและบำรุงรักษาอุปกรณ์คอมพิวเตอร์ เพื่อให้ข้อมูลสารสนเทศและสินทรัพย์สารสนเทศมีความปลอดภัยจากการสูญหาย การถูกขโมย การเกิดความเสียหาย การก่อกวน การถูกเปิดเผยโดยไม่ได้รับอนุญาต การกระทำโดยประมาท อุบัติเหตุ หรืออุบัติภัยทางธรรมชาติ เป็นต้น

คำจำกัดความ

“พื้นที่สำนักงาน”	หมายถึง	พื้นที่ส่วนปฏิบัติงานของผู้บริหารและเจ้าหน้าที่ของสนท. อันหมายรวมถึง พื้นที่ปฏิบัติงานทั่วไป และพื้นที่จำกัดการเข้าถึง
“พื้นที่ให้บริการ”	หมายถึง	พื้นที่ส่วนที่รองรับการให้บริการนิสิตและบุคคลภายนอก
“พื้นที่จำกัดการเข้าถึง”	หมายถึง	พื้นที่ที่เป็นห้องควบคุมระบบ ทั้งที่อยู่ภายในเขตพื้นที่ของมหาวิทยาลัยและนอกพื้นที่ของมหาวิทยาลัย

1. การควบคุมการเข้า-ออกอาคารและพื้นที่สำนักงาน

1.1 ผู้อำนวยการ หรือผู้อำนวยการฝ่ายที่รับผิดชอบ หรือผู้ที่ได้รับมอบหมาย ต้องกำกับดูแลระบบควบคุมการเข้า-ออกอาคาร และระบบควบคุมการเข้า-ออกพื้นที่สำนักงาน ให้อยู่ในสภาพที่ใช้การได้ปกติ เมื่อพบว่าระบบควบคุมการเข้า-ออกอาคาร หรือระบบควบคุมการเข้า-ออกพื้นที่สำนักงานไม่สามารถใช้การได้ปกติ ต้องแจ้งให้ผู้รับผิดชอบของมหาวิทยาลัยรับทราบและแก้ไขโดยทันที

1.2 ผู้อำนวยการ หรือผู้อำนวยการฝ่ายที่รับผิดชอบ หรือผู้ที่ได้รับมอบหมาย ต้องติดตั้งระบบกล้อง CCTV เพื่อรักษาความปลอดภัยบริเวณทางเข้า-ออกอาคาร และความปลอดภัยภายในสำนักงาน และกำกับดูแลให้อยู่ในสภาพที่ใช้การได้ปกติ

1.3 นิสิตและบุคคลภายนอกที่มาติดต่อสำนักงานการทะเบียน จะต้องอยู่ในพื้นที่ให้บริการเท่านั้น ไม่อนุญาตให้เข้ายังในพื้นที่สำนักงานทุกกรณี ยกเว้นกรณีที่มีการนัดหมายไว้เป็นการล่วงหน้า

1.4 นิสิตและบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงพื้นที่สำนักงาน จะต้องอยู่หรือปฏิบัติงานในพื้นที่ที่ได้รับอนุญาตหรือพื้นที่ที่กำหนดไว้เพื่อปฏิบัติงานเท่านั้น

1.5 ในกรณีที่มีความจำเป็นเร่งด่วน หรือเหตุการณ์ฉุกเฉินที่อาจเป็นผลให้เกิดความเสียหายต่อชีวิตหรือทรัพย์สิน บุคคลภายนอกสามารถเข้า-ออกอาคารและพื้นที่สำนักงานได้ เมื่อได้รับอนุญาตจากผู้อำนวยการ

2. การควบคุมการเข้า-ออกพื้นที่จำกัดการเข้าถึง

2.1 ห้ามบุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้น เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

2.2 กรณีมีบุคลากรจุฬาฯ หรือบุคคลภายนอกที่จำเป็นต้องเข้าไปปฏิบัติงานในพื้นที่จำกัดการเข้าถึง บุคคลผู้นั้นจะต้องได้รับอนุญาตจากผู้อำนวยการ หรือรองผู้อำนวยการที่ได้รับมอบหมายให้ดูแลด้านเทคโนโลยีสารสนเทศ หรือผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ และต้องมีเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ เข้าไปร่วมสังเกตการณ์ปฏิบัติงาน และประสานงานด้วยทุกครั้ง

2.3 ในกรณีที่มีความจำเป็นเร่งด่วน หรือเหตุการณ์ฉุกเฉินที่อาจเป็นผลให้เกิดความเสียหายต่อชีวิตหรือทรัพย์สิน บุคคลภายนอกสามารถเข้า-ออกอาคารและพื้นที่จำกัดการเข้าถึงได้ เมื่อได้รับอนุญาตจากผู้บริหารสูงสุด

3. การติดตั้งและใช้งานห้องควบคุมระบบ

3.1 ติดตั้งระบบควบคุมการเข้า-ออกห้อง

3.2 ติดตั้งระบบและอุปกรณ์ป้องกันอัคคีภัย

3.3 ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง

3.4 ติดตั้งระบบปรับอากาศและควบคุมอุณหภูมิ

3.5 การเดินสายไฟ สายสื่อสาร และสายเคเบิล ให้เป็นไปตามมาตรฐานความปลอดภัย

3.6 ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่างๆ

4. การจัดทำบัญชีทรัพย์สินและการควบคุมทรัพย์สิน

4.1 จัดทำบัญชีทรัพย์สินสำหรับครุภัณฑ์อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย และซอฟต์แวร์ที่มีค่าลิขสิทธิ์ โดยต้องบันทึกว่าอุปกรณ์ดังกล่าวใช้งานที่ฝ่ายใด หรือใช้งานที่เจ้าหน้าที่คนใด

4.2 ตรวจสอบและปรับปรุงข้อมูลในบัญชีทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง การเคลื่อนย้าย การเปลี่ยนผู้ครอบครอง การยืม การโอน หรือการจำหน่ายออกจากทะเบียนครุภัณฑ์ของสำนักงานการทะเบียน

4.3 เจ้าหน้าที่ที่ต้องการยืมอุปกรณ์คอมพิวเตอร์เพื่อนำไปปฏิบัติงานนอกสำนักงาน แต่ยังอยู่ภายในพื้นที่ของมหาวิทยาลัย ต้องแจ้งให้ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ และเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศผู้ดูแลครุภัณฑ์ทราบ

4.4 เจ้าหน้าที่ที่ต้องการยืมอุปกรณ์คอมพิวเตอร์เพื่อนำไปปฏิบัติงานนอกมหาวิทยาลัย หรือเพื่อปฏิบัติงานที่บ้าน ต้องทำเรื่องขอยืมเป็นลายลักษณ์อักษรและได้รับอนุมัติจากผู้อำนวยการ โดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศผู้ดูแลครุภัณฑ์เป็นผู้บันทึกข้อมูลการยืมอุปกรณ์ของสำนักงานออกไปใช้งานนอกมหาวิทยาลัย และบันทึกข้อมูลการส่งคืนเพื่อเป็นหลักฐาน

4.5 เมื่อมีการจำหน่ายอุปกรณ์ครุภัณฑ์คอมพิวเตอร์หรืออุปกรณ์เครือข่าย ต้องทำลายข้อมูลและซอฟต์แวร์ลิขสิทธิ์ในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ก่อนการจำหน่าย โดยข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

5. การบำรุงรักษาอุปกรณ์

5.1 วางแผนการบำรุงรักษาอุปกรณ์หรือระบบ ตามรอบระยะเวลาและ/หรือความสำคัญของอุปกรณ์หรือระบบ

5.2 บันทึกประวัติการบำรุงรักษาและซ่อมบำรุงอุปกรณ์หรือระบบทุกครั้ง

5.3 กรณีจัดจ้างบุคคลภายนอกหรือผู้ให้บริการภายนอกเพื่อบำรุงรักษาและซ่อมบำรุงอุปกรณ์ กำหนดระยะเวลาและขอบเขตบำรุงรักษาจะต้องเป็นไปตามสัญญาการจ้าง

5.4 การเข้าบำรุงรักษาและซ่อมบำรุงอุปกรณ์โดยบุคคลภายนอกหรือผู้ให้บริการภายนอก จะต้องมีการควบคุมดูแลการปฏิบัติงานโดยเจ้าหน้าที่ กรณีที่ต้องเข้าบำรุงรักษาและซ่อมบำรุงอุปกรณ์ในพื้นที่จำกัดการเข้าถึง เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ หรือผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ จะต้องควบคุมดูแลอยู่ในพื้นที่ด้วย

<u>นโยบายการรักษาความปลอดภัยของเครือข่าย</u>

นโยบายการรักษาความปลอดภัยของเครือข่าย กำหนดขึ้นเพื่อให้มีการป้องกันการบุกรุกจากบุคคลที่ไม่พึงประสงค์ ควบคุมการเชื่อมต่อจากภายนอกและการเชื่อมต่อจากภายใน และเพื่อให้มีรายงานที่ตรวจสอบการดำเนินกิจกรรมของผู้ที่เข้าใช้งานระบบ หรือตรวจจับการเชื่อมต่อที่ผิดปกติ

1. **การใช้งานระบบไฟร์วอลล์ (Firewall Policy)**
   - 1.1 กำหนดให้มีการใช้ระบบไฟร์วอลล์เพื่อป้องกันการบุกรุกจากบุคคลภายนอกและควบคุมการเชื่อมต่อ
   - 1.2 กำหนดนโยบาย (Policy) หรือตั้งค่า (Configure) ระบบไฟร์วอลล์เพื่อกรองข้อมูลในขณะที่มีการเชื่อมต่อเครือข่ายอินเทอร์เน็ต เช่น การป้องกันมัลแวร์ การป้องกันไวรัสคอมพิวเตอร์ การป้องกันผู้บุกรุก การป้องกันชุดคำสั่งประสงค์ร้าย
   - 1.3 ผู้ดูแลระบบต้องตรวจสอบว่าระบบไฟร์วอลล์เปิดใช้งานอยู่ตลอดเวลาและมีสถานะปกติ
   - 1.4 ผู้ดูแลระบบต้องกำหนดและควบคุมการใช้งานระบบไฟร์วอลล์ และระมัดระวังไม่ให้มีผู้เกี่ยวข้องเข้ามาแก้ไขเปลี่ยนแปลงนโยบายหรือการตั้งค่าที่กำหนดไว้แล้วได้
2. **การระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log System)**
   - 2.1 กำหนดให้มีการใช้ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อใช้เฝ้าระวังและติดตามเหตุการณ์ที่อาจเป็นความเสี่ยงต่อระบบเครือข่าย และเก็บสถิติจำนวนผู้เข้าใช้งานและปริมาณการใช้งาน เพื่อจะได้บริหารจัดการเครือข่ายให้มีเสถียรภาพ
   - 2.2 ผู้ดูแลระบบต้องตรวจสอบว่าระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เปิดใช้งานอยู่ตลอดเวลาและมีสถานะปกติ และต้องมีการบำรุงรักษาระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้อยู่ในสภาพที่พร้อมใช้งาน
   - 2.3 เมื่อตรวจสอบรายงานข้อมูลจราจรทางคอมพิวเตอร์และพบเหตุการณ์ที่มีความเสี่ยงสูงและอาจกระทบต่อเครือข่าย ต้องสืบหาสาเหตุและหาทางป้องกันแก้ไข

<u>นโยบายการบริหารจัดการการเข้าถึงและควบคุมการใช้งานสารสนเทศ</u>

นโยบายการบริหารจัดการการเข้าถึงและควบคุมการใช้งานสารสนเทศ กำหนดขึ้นเพื่อให้ข้อมูลส่วนบุคคลของนิสิต และข้อมูลอื่น ๆ ที่สำคัญต่อสำนักงานได้รับการจำแนกชั้นความลับตามระดับความสำคัญ เพื่อให้เจ้าหน้าที่ของสำนักงานการทะเบียนและบุคลากรจุฬาฯ รับทราบถึงมาตรการการจำกัดการเข้าถึงข้อมูล และใช้งานข้อมูลแต่ละชั้นความลับได้อย่างถูกต้องเหมาะสม โดยเป็นไปตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของนิสิต จุฬาลงกรณ์มหาวิทยาลัย

1. การกำหนดลำดับความสำคัญของข้อมูล

1.1 สำนักงานการทะเบียน จัดแบ่งประเภทของข้อมูล ดังนี้

1.1.1 <u>ข้อมูลสารสนเทศด้านงานทะเบียน</u> หมายถึง ข้อมูลที่สำนักงานการทะเบียนใช้เพื่อการดำเนินงานด้านทะเบียนทั้งหมดของมหาวิทยาลัย ตามภาระหน้าที่รับผิดชอบที่ระบุไว้ในข้อบังคับจุฬาลงกรณ์มหาวิทยาลัย ว่าด้วยการบริหารสำนักงานการทะเบียน พ.ศ. 2556 ข้อ 7 แบ่งออกเป็น

1.1.1.1 ข้อมูลที่เป็นข้อมูลส่วนบุคคลของนิสิต เช่น เลขประจำตัวนิสิต ชื่อ-นามสกุลของนิสิต ข้อมูลการศึกษาของนิสิตรายบุคคล เป็นต้น (รายละเอียดตาม หมวด ข. ในนโยบายคุ้มครองข้อมูลส่วนบุคคลของนิสิต จุฬาลงกรณ์มหาวิทยาลัย)

1.1.1.2 ข้อมูลที่เป็นข้อมูลจำนวนและสถิติ เช่น จำนวนนิสิตลงทะเบียน จำนวนนิสิตพ้นสถานภาพฯ ในแต่ละภาคการศึกษา สถิติผู้สำเร็จการศึกษา เป็นต้น

1.1.1.3 ข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคลของนิสิต เช่น ข้อมูลหลักสูตร ข้อมูลรายวิชา ข้อมูลอาคาร ข้อมูลรหัสคณะ รหัสภาควิชา รหัสสาขา เป็นต้น

1.1.2 <u>ข้อมูลสารสนเทศด้านการบริหาร</u> หมายถึง ข้อมูลที่สำนักงานการทะเบียนใช้เพื่อการดำเนินงานด้านบริหารทั่วไป ซึ่งไม่เกี่ยวข้องกับงานทะเบียน เช่น ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและการบัญชี ข้อมูลยุทธศาสตร์ ข้อมูลสารบรรณ ข้อมูลพัสดุครุภัณฑ์ เป็นต้น

1.2 สำนักงานการทะเบียน จัดลำดับชั้นความสำคัญของข้อมูล ดังนี้

1.2.1 การจัดลำดับชั้นความสำคัญของข้อมูลสารสนเทศด้านงานทะเบียน เป็นไปตาม **ภาคผนวก ก**

1.2.2 การจัดลำดับชั้นความสำคัญของข้อมูลสารสนเทศด้านการบริหาร ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ดังนี้

1.2.2.1 ลับที่สุด

1.2.2.2 ลับมาก

1.2.2.3 ลับ

1.2.2.4 ข้อมูลใช้ภายในสำนักงาน

1.2.2.5 ข้อมูลสาธารณะ

2. การใช้งานข้อมูล

2.1 เจ้าหน้าที่ต้องใช้ข้อมูลตามกฎระเบียบ นโยบาย และแนวปฏิบัติของสำนักงาน

2.2 เจ้าหน้าที่ต้องใช้ข้อมูลเท่าที่จำเป็นและเกี่ยวข้องกับภารกิจการดำเนินงานเท่านั้น

2.3 การสร้าง นำเข้า บันทึก หรือแก้ไขข้อมูล ต้องทำตามแนวปฏิบัติของสำนักงาน หรือโดยได้รับอนุมัติจากผู้อำนวยการสำนักงานการทะเบียน หรือตามคำสั่งของมหาวิทยาลัย หรือคำสั่งอื่นใดที่โดยชอบด้วยกฎหมาย แล้วแต่กรณี

2.4 เจ้าหน้าที่ต้องตระหนักและระมัดระวังเป็นพิเศษในการใช้งานข้อมูลประเภทลับ และข้อมูลส่วนบุคคล เพื่อไม่ให้ข้อมูลถูกเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาต

2.5 เจ้าหน้าที่ต้องตระหนักถึงการรักษาข้อมูลลับและข้อมูลส่วนบุคคลที่อยู่ในเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ จะต้องมีการปกป้องข้อมูลด้วยการเข้ารหัส หรือการควบคุมการเข้าใช้งานเครื่องคอมพิวเตอร์ด้วยระบบปฏิบัติการ

2.6 เจ้าหน้าที่ควรเก็บรักษาเอกสารลับ หรือเอกสารที่มีข้อมูลส่วนบุคคล หรือสื่อบันทึกข้อมูลที่มีข้อมูลลับหรือข้อมูลส่วนบุคคล ให้มีความปลอดภัย โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อไม่อยู่ที่โต๊ะทำงาน

2.7 เจ้าหน้าที่ควรเก็บเอกสารลับ หรือเอกสารที่มีข้อมูลส่วนบุคคล ออกจากอุปกรณ์ต่าง ๆ เสมอ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร

2.8 ข้อมูลใดที่เป็นข้อมูลลับ หรืออาจส่งผลต่อความมั่นคงปลอดภัยของระบบ ต้องได้รับการเข้ารหัส

2.9 เมื่อจำเป็นต้องทำลายเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูล ให้ดำเนินการดังนี้

2.9.1 เอกสาร: ตัดด้วยเครื่องทำลายเอกสาร

2.9.2 ไฟล์ข้อมูลบนแฟลชไดร์ฟ ฮาร์ดดิสก์ ฮาร์ดดิสก์พกพา: ลบทิ้งถาวร

2.9.3 ไฟล์ข้อมูลบนคลาวด์: ลบทิ้งถาวร

3. การเปิดเผยข้อมูล

3.1 เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับและข้อมูลส่วนบุคคลของนิสิตกับผู้อื่น ทุกกรณี

3.2 เมื่อให้บริการหรือตอบข้อซักถามใด ๆ เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับและข้อมูลส่วนบุคคลของนิสิต ผ่านทางโทรศัพท์ ไลน์ หรือเฟซบุ๊ก หรือช่องทางอื่นใดที่ไม่สามารถระบุยืนยันตัวตนของผู้ขอรับบริการหรือผู้ติดต่อสอบถามได้

3.3 เมื่อให้บริการหรือตอบข้อซักถามใด ๆ ที่มีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลของนิสิต เจ้าหน้าที่สามารถเปิดเผยข้อมูลส่วนบุคคลของนิสิตได้ ในกรณีต่อไปนี้

3.3.1 เมื่อนิสิตเป็นผู้ติดต่อร้องขอด้วยตัวเองที่สำนักงาน ทั้งนี้ต้องยืนยันตัวตนด้วยบัตรประจำตัวประชาชน บัตรประจำตัวนิสิต หรือหนังสือเดินทาง หรือด้วยวิธีอื่นใดที่สำนักงานการทะเบียนกำหนด

3.3.2 เมื่อนิสิตเป็นผู้ติดต่อร้องขอผ่านช่องทางอีเมล

3.3.2.1 นิสิตต้องนิสิตต้องใช้อีเมล @student.chula.ac.th หรือ @alumni.chula.ac.th เท่านั้น

3.3.2.2 หากนิสิตใช้อีเมลอื่นๆ ที่ไม่ใช่อีเมลในโดเมน chula.ac.th นิสิตต้องยืนยันตัวตนโดยการแนบบัตรประจำตัวประชาชน บัตรประจำตัวนิสิต หรือหนังสือเดินทาง หรือด้วยวิธีอื่นใดที่สำนักงานการทะเบียนกำหนด

3.3.3 เมื่อบุคคลที่สามได้รับมอบอำนาจให้ดำเนินการแทน เฉพาะในกรณีต่อไปนี้

3.3.3.1 เมื่อบุคคลที่สามดำเนินการขอและรับเอกสารสำคัญทางการศึกษาแทนนิสิต โดยมีหนังสือมอบฉันทะและสำเนาบัตรประจำตัวประชาชน บัตรประจำตัวนิสิต หรือหนังสือเดินทาง ของนิสิตเจ้าของเอกสารสำคัญทางการศึกษา

3.3.3.2 เมื่อบุคคลที่สามผู้ดำเนินการขอและรับเอกสารสำคัญทางการศึกษาแทนนิสิต เป็นบิดาและมารดาของนิสิต โดยบิดาหรือมารดาผู้ดำเนินการแทนต้องยืนยันตัวตนตามวิธีที่สำนักงานการทะเบียนกำหนด และข้อมูลของบิดาหรือมารดาผู้ดำเนินการแทนต้องตรงกับข้อมูลที่นิสิตระบุไว้ในระเบียนประวัติ

3.3.4 เมื่อบุคลากรจุฬาฯ ที่มีภารกิจหน้าที่เกี่ยวข้องด้านทะเบียนนิสิตร้องขอข้อมูลส่วนบุคคลของนิสิตเพื่อใช้ในการปฏิบัติงาน ให้ติดต่อร้องขอและเปิดเผยข้อมูลเป็นลายลักษณ์อักษร หรือผ่านช่องทางอีเมล @chula.ac.th กรณีเร่งด่วนอนุโลมให้เปิดเผยข้อมูลทางโทรศัพท์ได้ แต่บุคลากรจุฬาฯ ผู้ติดต่อร้องขอข้อมูลนั้นต้องส่งอีเมลตามมาเพื่อเป็นหลักฐานการขอข้อมูล

3.4 แนวทางการเปิดเผยข้อมูลส่วนบุคคลของนิสิต หรือการให้บริการข้อมูลที่มีข้อมูลส่วนบุคคลของนิสิต ต้องเป็นไปตาม หมวด จ. การใช้งานข้อมูลส่วนบุคคลร่วมกันกับส่วนงาน/หน่วยงานภายนอก และ หมวด ฉ. การส่งหรือโอนข้อมูลไปยังต่างประเทศ ในนโยบายคุ้มครองข้อมูลส่วนบุคคลของนิสิต จุฬาลงกรณ์มหาวิทยาลัย

3.5 การให้บริการข้อมูลที่มีข้อมูลส่วนบุคคลของนิสิต ต้องมีการเข้ารหัสไฟล์เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง หรือมีการรักษาความปลอดภัยของข้อมูล

3.6 การให้บริการข้อมูลที่มีข้อมูลส่วนบุคคลของนิสิต ให้แก่ส่วนงานหรือหน่วยงานของมหาวิทยาลัย จะต้องส่งถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของส่วนงานหรือหน่วยงาน ตามที่คำสั่งหรือประกาศแต่งตั้ง เท่านั้น

4. การควบคุมการเข้าถึงสารสนเทศ

4.1 แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศที่เป็นเอกสาร

4.1.1 สถานที่ตั้งหรือสถานที่เก็บรักษาเอกสารที่เป็นข้อมูลลับ หรือเป็นข้อมูลส่วนบุคคลของนิสิต ต้องมีการควบคุมการเข้าถึง โดยมีระบบการควบคุมการเข้า-ออก พื้นที่สำนักงาน

4.1.2 ผู้อำนวยการฝ่ายต้องกำหนดให้มีกระบวนการควบคุมการเข้าถึงเอกสาร เพื่อรักษาเอกสารที่เป็นข้อมูลลับ หรือเป็นข้อมูลส่วนบุคคลของนิสิต ให้มีความปลอดภัย ไม่ให้ข้อมูลถูกเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันความเสียหายที่อาจเกิดขึ้นจากอุบัติเหตุหรือภัยธรรมชาติ

4.1.3 ในกรณีที่ได้รับอนุมัติให้เปิดเผยข้อมูลลับหรือข้อมูลส่วนบุคคล หรือเปิดเผยข้อมูลส่วนบุคคลของนิสิตได้ตามข้อ 3.3 เจ้าหน้าที่ต้องระมัดระวังในกระบวนการส่งเอกสารที่เป็นข้อมูลลับ หรือเอกสารที่เป็นข้อมูลส่วนบุคคลของนิสิต ไม่ให้มีผู้ที่ไม่เกี่ยวข้องเข้าถึงข้อมูลเอกสารนั้นได้ โดยอาจปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

4.2 แนวปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

4.2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศ ต้องมีการควบคุมการเข้าออกที่รัดกุม

4.2.2 สำนักงานการทะเบียน จะให้สิทธิเจ้าหน้าที่และบุคลากรจุฬาฯ ในการเข้าใช้งานระบบเฉพาะในส่วนที่จำเป็นตามหน้าที่ความรับผิดชอบเท่านั้น

4.2.3 เจ้าหน้าที่และบุคลากรจุฬาฯ ที่ต้องการได้สิทธิเข้าระบบเทคโนโลยีสารสนเทศของสำนักงานการทะเบียน ต้องได้รับอนุญาตจากผู้บังคับบัญชาของตน และได้รับอนุมัติสิทธิจากผู้อำนวยการสำนักงานการทะเบียน

4.2.4 ผู้ดูแลระบบเป็นผู้กำหนดสิทธิการเข้าถึงข้อมูลให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของเจ้าหน้าที่และบุคลากรจุฬาฯ ผู้ปฏิบัติงาน ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ เพื่อเปลี่ยนแปลงหรือยกเลิกสิทธิให้เป็นไปอย่างถูกต้องและเป็นปัจจุบัน

4.2.5 ผู้ดูแลระบบมีหน้าที่ต้องตรวจสอบการอนุญาตและการอนุมัติให้สิทธิเข้าใช้งานระบบ โดยต้องมีบันทึกเอกสารขอสิทธิเข้าใช้งานระบบต่าง ๆ ที่ลงนามอนุญาตโดยผู้บังคับบัญชาของผู้ขอสิทธิใช้เข้างาน และลงนามอนุมัติโดยผู้อำนวยการสำนักงานการทะเบียน และต้องจัดเก็บเอกสารเหล่านั้นไว้เป็นหลักฐาน

4.2.6 ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้ โดยเป็นไปตามแนวปฏิบัติของผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ หรือโดยได้รับอนุมัติจากผู้อำนวยการสำนักงานการทะเบียน

4.2.7 ผู้ดูแลระบบต้องบันทึกประวัติการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบหากเกิดปัญหา

4.3 การควบคุมการเข้าถึงฐานข้อมูลและการกำหนดสิทธิของผู้ใช้งานภายในสำนักงานการทะเบียน **เป็นไปตาม ภาคผนวก ข**

4.4 การควบคุมการเข้าถึงและการกำหนดสิทธิของผู้ใช้งานภายนอกสำนักงานการทะเบียน **เป็นไปตาม ภาคผนวก ค**

5. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

5.1 การบริหารจัดการสิทธิผู้ใช้งาน (User Management)

5.1.1 สำนักงานการทะเบียน กำหนดสิทธิของนิสิตในการเข้าใช้งานระบบลงทะเบียนแรกเข้า (Adm Reg) และระบบลงทะเบียนเรียน (Reg Chula) ตามข้อมูลบัญชีและข้อมูลรหัสผ่าน CUNET ที่สร้างและกำหนดโดยสำนักบริหารเทคโนโลยีสารสนเทศ โดยสิทธิในการเข้าใช้งานระบบจะเป็นไปตามสถานภาพการเป็นนิสิต

5.1.2 ผู้ดูแลระบบกำหนดสิทธิของเจ้าหน้าที่สำนักงานการทะเบียน ตามฝ่ายที่สังกัด หน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน หากมีความจำเป็นต้องใช้ระบบงานใดเพิ่มเติมภายหลังการกำหนดสิทธิให้ครั้งแรก หรือมีการเปลี่ยนสังกัด หรือหน้าที่ความรับผิดชอบ ต้องทำเรื่องผ่านผู้อำนวยการฝ่ายที่สังกัด โดยผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเป็นผู้อนุมัติ

5.1.3 ผู้ดูแลระบบกำหนดสิทธิของบุคลากรจุฬาฯ ตามรายละเอียดในภาคผนวก ค โดยบุคลากรจุฬาฯ ต้องส่ง “แบบฟอร์มคำร้องขอสิทธิ์เพื่อใช้ระบบงานของสำนักงานการทะเบียน” ทั้งนี้ต้องได้รับมอบหมายจากผู้บังคับบัญชาของตน และได้รับอนุมัติโดยผู้อำนวยการสำนักงานการทะเบียน

5.1.4 ผู้ดูแลระบบกำหนดสิทธิของผู้บริหารมหาวิทยาลัยโดยตำแหน่ง ตามรายละเอียดใน ภาคผนวก ค

5.1.5 ผู้ดูแลระบบต้องตรวจสอบบัญชีรายชื่อผู้ใช้งาน เพื่อไม่ให้มีการสร้างบัญชีหรือให้สิทธิซ้ำซ้อน

5.1.6 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิการใช้งานระบบที่ตรงกับหน้าที่ความรับผิดชอบ

5.1.7 ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่เหมาะสม โดยต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างน้อยปีละ 1 ครั้ง

5.1.8 สำนักงานการทะเบียนกำหนดยกเลิกสิทธิการเข้าใช้งานระบบของผู้ใช้งานโดยไม่แจ้งให้ทราบล่วงหน้า ในกรณีต่อไปนี้

5.1.8.1 ผู้ใช้งานไม่เข้าใช้งานในระบบเป็นระยะเวลาติดต่อกัน 6 เดือน

5.1.8.2 ผู้ใช้งานสิ้นสุดสถานภาพการเป็นบุคลากรของมหาวิทยาลัย หรือสิ้นสุดการจ้างโดยสำนักงานการทะเบียน

5.1.8.3 ผู้ใช้งานมีการย้ายสังกัด หรือปรับเปลี่ยนหน้าที่ความรับผิดชอบ ซึ่งกระทบต่อขอบเขตข้อมูลที่เข้าถึงได้ด้วยสิทธิการใช้งานที่มีอยู่แต่เดิม

5.1.8.4 ผู้ใช้งานสิ้นสุดวาระตำแหน่งผู้บริหาร

5.1.8.5 ผู้ใช้งานที่เป็นนิสิต สิ้นสุดสถานภาพการเป็นนิสิต และสำนักบริหารเทคโนโลยีสารสนเทศได้ลบข้อมูลบัญชีผู้ใช้งาน CUNET แล้ว

5.2 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (Password Management)

5.2.1 ผู้ดูแลระบบ กำหนดรหัสผ่านชั่วคราวในครั้งแรกให้แก่ผู้ใช้งาน แล้วส่งมอบให้ผู้ใช้งานทางอีเมล @chula.ac.th ของผู้ใช้งาน

5.2.2 ผู้ใช้งานที่ได้รับรหัสผ่านชั่วคราวครั้งแรก ควรเปลี่ยนรหัสผ่านใหม่ทันที และรหัสผ่านใหม่ควรเป็นไปตามรูปแบบตามที่สำนักงานการทะเบียนกำหนด

5.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

5.3.1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยต้องรักษารหัสผ่านให้เป็นความลับอย่างเคร่งครัด ไม่จดหรือบันทึกรหัสผ่านไว้ในที่ที่บุคคลอื่นสังเกตเห็นง่าย และต้องเปลี่ยนรหัสผ่านทุก 180 วัน หรือเมื่อมีการแจ้งเตือนการรั่วไหลอันเป็นเหตุให้ต้องเปลี่ยนรหัสผ่าน

5.3.2 ผู้ใช้งานที่ได้รับสิทธิแล้วต้องระมัดระวังไม่ให้ผู้อื่นใช้บัญชีและรหัสผ่านของตนในการเข้าระบบ หากเกิดปัญหาจากการอนุญาต หรือปล่อยปละละเลยให้ผู้อื่นใช้งานบัญชีของตนเองได้ เช่น การเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การมีผู้ไม่หวังดีเข้ามาดำเนินการในระบบแทนจนเกิดความเสียหายต่อตัวเจ้าของบัญชีหรือผู้อื่น เจ้าของบัญชีผู้ได้รับสิทธินั้นจะต้องเป็นผู้รับผิดชอบเพียงผู้เดียว

5.3.3 ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีเมื่อเลิกใช้งาน และต้องกำหนดรหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์เมื่อไม่ถูกใช้งานหรือไม่ได้ดูแลชั่วคราว

5.3.4 ผู้ใช้งานต้องไม่ใช้สิทธิการเข้าถึงระบบของตนในการเข้าถึงข้อมูลใด ๆ ที่ไม่เกี่ยวข้องกับหน้าที่การปฏิบัติงาน หรือโดยไม่มีเหตุผลอันสมควร

5.3.5 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้ข้อมูลที่ได้รับสิทธิเข้าถึง และปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของนิสิต จุฬาลงกรณ์มหาวิทยาลัย กับ พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5.3.6 ผู้ใช้งานห้ามทำกระทำการใดๆ อันจะสร้างภาระหรือส่งผลเสียหายต่อระบบเทคโนโลยีสารสนเทศหรือฐานข้อมูล หรือลักลอบรับรู้บัญชีและรหัสผ่านของผู้อื่น หรือกระทำความผิดใดๆ ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560

6. การบริหารจัดการบันทึกและตรวจสอบการเข้าถึง

6.1 ระบบเทคโนโลยีสารสนเทศของสำนักงานการทะเบียน ต้องมีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ เช่น บันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการเข้าออกระบบ บันทึกการปฏิบัติงานในระบบของผู้ใช้งาน บันทึกการบุกรุก และบันทึกข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

6.2 บันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ จะต้องเก็บไว้อย่างน้อย 3 เดือน โดยมีรายละเอียดดังนี้

6.2.1 ข้อมูลบัญชีชื่อผู้ใช้งาน

6.2.2 ข้อมูลวัน/เวลาที่เข้าถึงระบบ

6.2.3 ข้อมูลวัน/เวลาที่ออกจากระบบ

6.2.4 ข้อมูลกิจกรรมและการปฏิบัติงานในระบบ

6.2.5 ข้อมูลก่อนการเปลี่ยนแปลง และข้อมูลหลังการเปลี่ยนแปลง (ถ้ามี)

6.2.6 ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง

6.2.7 ข้อมูลการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ

6.2.8 ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

6.2.9 ข้อมูลการเปลี่ยนการกำหนดค่า (Configuration) ของระบบ

6.2.10 ข้อมูลโพรโทคอล (Protocol) เครือข่ายที่ใช้

6.2.11 ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

6.3 ต้องจำกัดสิทธิการเข้าถึงบันทึกข้อมูลเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

7. การป้องกันการเข้าถึงระบบที่ไม่ได้รับอนุญาต (User Authentication)

7.1 ผู้ใช้งานระบบสารสนเทศต้องพิสูจน์ตัวตนก่อนเข้าใช้งานระบบ โดยแสดงตัวตน (Identify) ด้วยชื่อบัญชีผู้ใช้งาน (Username) และพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบหลักฐานว่าเป็นผู้ใช้งานตัวจริง

7.2 วิธีการพิสูจน์ยืนยันตัวตน ได้แก่ การใช้รหัสผ่าน (Password) หรือวิธีอื่นใดที่สำนักงานการทะเบียนจะใช้งานในอนาคต

7.3 การเข้าสู่ระบบสารสนเทศจากระยะไกล (Remote Access) จะกระทำได้เมื่อมีความจำเป็นและเมื่อได้รับอนุญาตจากผู้บริหารสูงสุดเท่านั้น และต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน

นโยบายการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ไอทีของหน่วยงาน

นโยบายการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ของหน่วยงาน กำหนดขึ้นเพื่อให้เจ้าหน้าที่ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ไอทีอันเป็นทรัพย์สินของสำนักงานเก็บรักษาทรัพย์สินอุปกรณ์ไอทีให้อยู่ในสภาพที่ใช้งานได้ และตระหนักถึงข้อควรระมัดระวังในการใช้งาน เพื่อป้องกันไม่ให้เกิดความเสี่ยงต่อภัยคุกคามที่จะส่งผลต่อระบบเทคโนโลยีสารสนเทศของสำนักงาน

1. การใช้งานเครื่องคอมพิวเตอร์และการเข้าถึงระบบภายในสำนักงาน

1.1 ผู้ดูแลระบบต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของสำนักงาน และกำหนดชื่อบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งาน เพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

1.2 ผู้ใช้งานต้องระบุบัญชีชื่อผู้ใช้งานและรหัสผ่านเพื่อยืนยันตัวตนเข้าใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศของสำนักงาน

1.3 คอมพิวเตอร์ของสำนักงานต้องมีการติดตั้งโปรแกรมหรือซอฟต์แวร์สำหรับตรวจจับมัลแวร์ ไวรัสคอมพิวเตอร์ หรือชุดคำสั่งประสงค์ร้ายที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ และต้องอัปเดตให้เป็นเวอร์ชั่นล่าสุดเสมอ

1.4 การติดตั้งโปรแกรมหรือซอฟต์แวร์ใด ๆ ต้องติดตั้งโดยผู้ดูแลระบบเท่านั้น หากมีความจำเป็นต้องติดตั้งโปรแกรมหรือซอฟต์แวร์อื่นเพื่อใช้ในการทำงาน ต้องขออนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

1.5 ไม่ติดตั้งโปรแกรมหรือซอฟต์แวร์ใด ๆ ที่ไม่เกี่ยวข้องกับการทำงาน หรือละเมิดลิขสิทธิ์

1.6 ผู้ใช้งานควรอัปเดตระบบปฏิบัติการ เว็บเบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ เมื่อมีการแจ้งเตือนให้อัปเดต

1.7 ผู้ใช้งานควรสแกนไวรัสคอมพิวเตอร์และมัลแวร์เป็นประจำ

1.8 ผู้ใช้งานควรระมัดระวังในการดาวน์โหลดโปรแกรมหรือไฟล์ต่าง ๆ จากอินเทอร์เน็ต

1.9 ผู้ใช้งานต้องรายงานผู้ดูแลระบบทันทีเมื่อพบเหตุการณ์น่าสงสัยหรือเหตุการณ์ผิดปกติกับเครื่องคอมพิวเตอร์ที่ใช้งาน หรือระบบสารสนเทศใด ๆ ของสำนักงาน

1.10 ผู้ใช้งานต้องไม่ใช้คอมพิวเตอร์ของสำนักงานเพื่อการกระทำที่ผิดกฎหมาย หรือกระทำความผิดใด ๆ ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560

2. การใช้งานเครื่องคอมพิวเตอร์และการเข้าถึงระบบจากภายนอกสำนักงาน

2.1 การยืมเครื่องคอมพิวเตอร์ของสำนักงานเพื่อปฏิบัติงานนอกสถานที่ตั้ง

2.1.1 การยืมเครื่องคอมพิวเตอร์ของสำนักงานเพื่อปฏิบัติงานนอกสถานที่ตั้ง ให้ปฏิบัติตาม ข้อ 4.3 และข้อ 4.4 ของนโยบายความมั่นคงปลอดภัยด้านกายภาพ

2.1.2 เจ้าหน้าที่มีหน้าที่ต้องดูแลรักษาเครื่องคอมพิวเตอร์ไม่ให้เกิดความเสียหายทั้งด้านฮาร์ดแวร์และระบบปฏิบัติการ และไม่ให้เครื่องคอมพิวเตอร์สูญหาย โดยปฏิบัติในแนวทางเดียวกันกับการใช้งานเครื่องคอมพิวเตอร์และการเข้าถึงระบบภายในสำนักงาน

2.1.3 เมื่อหมดความจำเป็นในการยืมเครื่องคอมพิวเตอร์เพื่อปฏิบัติงานนอกสถานที่ตั้ง ต้องคืนเครื่องคอมพิวเตอร์คืนที่เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศผู้ดูแลครุภัณฑ์

2.2 การปฏิบัติงานจากระยะไกล (Remote Access)

2.2.1 การเข้าสู่ระบบสารสนเทศจากระยะไกล (Remote Access) เพื่อเข้าสู่เครื่องคอมพิวเตอร์และระบบสารสนเทศของสำนักงาน จะกระทำได้เมื่อมีความจำเป็นและเมื่อได้รับอนุมัติจากผู้อำนวยการเท่านั้น

2.2.2 วิธีการเข้าถึงระบบสารสนเทศของสำนักงานจากระยะไกล ต้องได้รับอนุมัติจากผู้อำนวยการก่อน

2.2.3 ผู้ปฏิบัติงานจากระยะไกลต้องแสดงตัวตนและพิสูจน์ยืนยันตัวตนก่อนการเข้าใช้งาน และต้องมีการลงบันทึกเข้าใช้งาน

2.2.4 ผู้ดูแลระบบต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยที่เพิ่มขึ้นอย่างเคร่งครัด ต้องควบคุมช่องทางที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวัง หากมีเหตุการณ์ปกติต้องระงับการให้บริการทันที

2.2.5 เมื่อครบกำหนดระยะเวลาขออนุญาต หรือเมื่อสิ้นความจำเป็นในการปฏิบัติงานจากระยะไกลแล้ว ให้ยกเลิกสิทธิการเข้าถึงระบบจากการปฏิบัติงานจากระยะไกล

2.3 การใช้สื่อบันทึกข้อมูล

2.3.1 เจ้าหน้าที่ต้องใช้แฟลชไดรฟ์ (Flash Drive) ที่สำนักงานจัดซื้อให้กับเครื่องคอมพิวเตอร์ของสำนักงานเป็นการเฉพาะเท่านั้น ไม่อนุญาตให้นำแฟลชไดรฟ์ไปใช้เป็นการส่วนตัว หรือใช้กับเครื่องคอมพิวเตอร์อื่นที่ไม่ใช่เครื่องที่สำนักงานกำหนดไว้

2.3.2 ห้ามใช้แฟลชไดรฟ์อื่นที่ไม่ใช่แฟลชไดรฟ์ที่สำนักงานจัดซื้อให้กับเครื่องคอมพิวเตอร์ของสำนักงาน

นโยบายการดำเนินงานต่อเนื่องและแผนรองรับเหตุการณ์ฉุกเฉิน

นโยบายการดำเนินงานต่อเนื่องและแผนรองรับเหตุการณ์ฉุกเฉิน กำหนดขึ้นเพื่อให้มั่นใจว่าเมื่อเกิดเหตุขัดข้องหรือภัยพิบัติ ระบบสารสนเทศและชุดข้อมูลสำคัญของสำนักงานจะยังพร้อมใช้งานโดยไม่มีการหยุดชะงัก และสามารถกู้กลับคืนมาได้กรณีเกิดความเสียหาย

1. การสำรองและกู้คืนข้อมูล

1.1 จัดทำบัญชีฐานข้อมูลและระบบสารสนเทศของสำนักงานที่มีความสำคัญ

1.2 จัดให้มีการสำรองข้อมูลและระบบสารสนเทศของสำนักงานให้อยู่ในสภาพพร้อมใช้งาน โดยจัดเรียงลำดับตามความสำคัญและผลกระทบที่จะเกิดขึ้นต่อสำนักงานหากเกิดความเสียหายหรือสูญเสีย

1.3 กำหนดขั้นตอนการปฏิบัติการสำรองและกู้คืนข้อมูล

1.4 กำหนดช่วงเวลาสำรองข้อมูลสำคัญตามระยะเวลาที่เหมาะสมต่อความสำคัญของข้อมูล เช่น ข้อมูลที่มีความสำคัญมาก สำรองข้อมูลทุกวัน เป็นต้น

1.5 ผู้ดูแลระบบที่ได้รับมอบหมายให้สำรองข้อมูล ต้องทำบันทึกรายละเอียดในการสำรองข้อมูลทุกครั้ง โดยแสดงชื่อระบบหรือชื่อฐานข้อมูลที่สำรอง วัน เดือน ปี และเวลาในการสำรองข้อมูล

1.6 การสำรองข้อมูลที่มีความสำคัญ ต้องให้มีการเข้ารหัส (Encryption) เพื่อไม่ให้มีการเปิดเผยข้อมูลสำรอง

1.7 ต้องมีการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

1.8 จัดให้มี Data Recovery Site เพื่อให้ฐานข้อมูลพร้อมใช้งานเสมอ แม้เกิดความเสียหายหรือเหตุขัดข้องที่ Data Center เพื่อความต่อเนื่องของการใช้งาน

1.9 กรณีเกิดความเสียหายต่อระบบสารสนเทศ เครือข่าย หรือฐานข้อมูล จนต้องทำการกู้คืน ให้ผู้ดูแลระบบดำเนินการแก้ไขโดยใช้ชุดข้อมูลที่ทันสมัยที่สุดที่ได้สำรองไว้เพื่อกู้คืนระบบให้กลับมาใช้งานได้ปกติ พร้อมทั้งบันทึกการดำเนินการแก้ไข ผลการแก้ไข และสรุปการปฏิบัติงานให้แก่ผู้บังคับบัญชาหรือผู้บริหารสูงสุด

1.10 เมื่อเกิดความเสียหายที่กระทบต่อการใช้งานระบบ ต้องแจ้งให้ผู้ใช้งานทราบ และรายงานความคืบหน้าจนกว่าจะดำเนินการแก้ไขเสร็จสิ้น

2. นโยบายการดำเนินงานต่อเนื่องและรับเหตุการณ์ฉุกเฉิน

2.1 กำหนดหน้าที่และออกคำสั่งมอบหมายการปฏิบัติหน้าที่แทนกัน เพื่อรองรับกรณีผู้มีอำนาจสั่งการในด้านต่างๆ ไม่สามารถปฏิบัติหน้าที่ได้

2.2 จัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน เพื่อให้การดำเนินงานในสภาวะฉุกเฉินเป็นไปอย่างต่อเนื่อง ซึ่งอาจแตกต่างกันตามสถานการณ์ เช่น

2.2.1 ภัยพิบัติทางธรรมชาติ ได้แก่ แผ่นดินไหว อัคคีภัย อุทกภัย วาตภัย

2.2.2 โรคระบาด

2.2.3 การโจมตีทางไซเบอร์ ที่ทำให้ระบบหรือฐานข้อมูลเสียหาย

2.2.4 อุปกรณ์เครือข่ายชำรุด ได้รับความเสียหาย หรือทำงานผิดปกติ

2.2.5 เหตุการณ์ก่อการร้าย การก่อความไม่สงบ

2.2.6 เหตุการณ์ชุมนุมทางการเมือง

2.2.7 เหตุสุดวิสัยอื่น ๆ ที่ทำให้ผู้อำนวยการ รองผู้อำนวยการและ/หรือผู้อำนวยการฝ่ายที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทนกัน หรือผู้ดูแลระบบ ไม่สามารถปฏิบัติหน้าที่ได้

2.3 แผนรองรับเหตุการณ์ฉุกเฉินในแต่ละสถานการณ์ ต้องมีการกำหนดขั้นตอนปฏิบัติที่ชัดเจน เช่น

2.3.1 การเตรียมความพร้อมก่อนเกิดความเสียหาย กำหนดกระบวนการป้องกันความเสี่ยง

2.3.2 การตอบสนองต่อเหตุการณ์ฉุกเฉิน

2.3.3 การดำเนินการเพื่อให้ปฏิบัติงานได้ต่อเนื่อง

2.3.4 การกู้คืนระบบ หรือการกลับคืนสู่ภาวะการทำงานปกติ

2.4 ประชาสัมพันธ์ให้เจ้าหน้าที่รับทราบแผนรองรับเหตุการณ์ฉุกเฉิน

2.5 จัดให้มีการทบทวนและซักซ้อมแผนรองรับเหตุการณ์ฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคคล

นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคคล มีจุดประสงค์เพื่อให้เจ้าหน้าที่ของสำนักงานทุกคน บุคลากรของมหาวิทยาลัย รวมถึงบุคคลภายนอกที่จำเป็นต้องเข้ามาปฏิบัติงานในระบบสารสนเทศของสำนักงาน มีความตระหนักต่อหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล โดยเฉพาะข้อมูลส่วนบุคคล และเพื่อให้เจ้าหน้าที่ของสำนักงานมีความรู้ความเข้าใจเบื้องต้น เพียงพอที่จะปฏิบัติงานได้ตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย

1. **การลงนามในข้อตกลงรักษาความลับ และข้อตกลงการใช้ข้อมูลร่วมกัน**
   1.1 เจ้าหน้าที่ทุกคนต้องลงนามรับทราบและยอมรับสัญญาระหว่างเจ้าหน้าที่และสำนักงานการทะเบียน ว่าจะไม่เปิดเผยข้อมูลความลับของสำนักงานการทะเบียน และให้การลงนามนี้เป็นเงื่อนไขส่วนหนึ่งของการว่าจ้าง ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว
   1.2 เมื่อเจ้าหน้าที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนลักษณะการปฏิบัติงาน จะต้องคืนอุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์บันทึกข้อมูลของสำนักงาน บัตรผ่านเข้า-ออก และไม่นำข้อมูลใด ๆ ที่เกี่ยวข้องกับการปฏิบัติงานออกจากสำนักงานหรือเครื่องคอมพิวเตอร์โดยเด็ดขาด
   1.3 หน่วยงานภายในมหาวิทยาลัยที่ต้องการเข้าถึงฐานข้อมูลของสำนักงานการทะเบียนทั้งหมด หรือเข้าถึงข้อมูลที่เกินความจำเป็นตามบทบาทหน้าที่ของหน่วยงาน จะต้องลงนามในข้อตกลงการใช้ข้อมูลร่วมกัน โดยรายละเอียดการส่งข้อมูล และขอบเขตข้อมูล ให้เป็นไปตามที่ตกลงกัน
   1.4 บุคคลหรือหน่วยงานภายนอกที่ได้รับว่าจ้างให้เข้ามาดูแลระบบ พัฒนาระบบ เขียนโปรแกรม หรือปฏิบัติงานใดๆ ที่เกี่ยวข้องและ/หรือสามารถเข้าถึงฐานข้อมูลและระบบสารสนเทศของสำนักงาน จะต้องลงนามในข้อตกลงการใช้ข้อมูลร่วมกัน (สัญญาว่าด้วยการรักษาความลับและข้อมูลภายในระบบของสำนักงานการทะเบียน) และให้การลงนามนี้เป็นเงื่อนไขส่วนหนึ่งของการว่าจ้าง
2. **การสร้างความตระหนักรู้และการอบรมเจ้าหน้าที่**
   2.1 ผู้อำนวยการและผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ต้องให้ความสำคัญในการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้แก่เจ้าหน้าที่ หน่วยงานภายในมหาวิทยาลัย บุคคลภายนอก หรือหน่วยงานภายนอกที่เป็นบริษัทคู่สัญญา ผู้รับเหมา และผู้ให้บริการ โดยกำชับเรื่องความรับผิดชอบ ความสำคัญของการรักษาข้อมูลความลับ และสื่อสารรายละเอียดขั้นตอนการทำงานให้เป็นไปตามมนโยบายให้ชัดเจน
   2.2 ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ในการแจ้งนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต่อเจ้าหน้าที่ และบุคลากรจุฬาฯ รวมถึงการควบคุมการเข้าถึงและการกำหนดสิทธิของผู้ใช้งานภายนอกสำนักงานการทะเบียน เมื่อมีการทบทวนหรือเปลี่ยนแปลงนโยบายและแนวปฏิบัติต้องแจ้งให้ทุกคนรับทราบ
   2.3 ผู้ที่ได้รับมอบหมายต้องจัดการอบรมให้เจ้าหน้าที่มีความรู้และความตระหนักเกี่ยวกับแนวทางการปฏิบัติงานที่เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัย ทั้งในด้านกายภาพ เครือข่าย อุปกรณ์คอมพิวเตอร์ ฐานข้อมูล ข้อมูลส่วนบุคคล รวมถึงแผนรองรับเหตุการณ์ฉุกเฉิน

นโยบายการตรวจสอบและประเมินความเสี่ยง

นโยบายการตรวจสอบและประเมินความเสี่ยง เพื่อกำหนดเกณฑ์ในการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศของสำนักงาน เพื่อให้มีการจัดเตรียมมาตรการควบคุมและแผนรองรับที่เหมาะสม และเพื่อให้มีการปรับปรุงนโยบายให้ทันต่อสภานการณ์จริงและการเปลี่ยนแปลงของเทคโนโลยีที่ใช้งานในระบบสารสนเทศของสำนักงาน

1. แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยง

1.1 ระบุความเสี่ยงที่อาจเกิดขึ้นในระหว่างการปฏิบัติงาน ที่อาจกระทบต่อระบบสารสนเทศ หรือความปลอดภัยของข้อมูล เช่น

1.1.1 ความเสี่ยงที่เกิดขึ้นจากการทำข้อมูลรั่วไหล

1.1.2 ความเสี่ยงที่เกิดขึ้นจากการทำข้อมูลชื่อผู้ใช้งานและรหัสผ่านรั่วไหล

1.1.3 ความเสี่ยงที่เกิดขึ้นจากการขัดข้องของระบบสารสนเทศหรือเครือข่าย

1.1.4 ความเสี่ยงที่เกิดขึ้นจากการลักลอบเข้าระบบสารสนเทศ การโจมตีหรือบุกรุกระบบ

1.1.5 ความเสี่ยงที่เกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ไอทีไม่ถูกต้อง

1.1.6 ความเสี่ยงอื่น ๆ ที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

1.2 ตรวจสอบและประเมินความเสี่ยง โดยพิจารณาจากแนวโน้มที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบที่เกิดจากความเสี่ยง (Impact)

1.3 เลือกแนวทางการจัดการความเสี่ยง และเตรียมดำเนินการตามแผนจัดการความเสี่ยง เช่น การหาทางลดโอกาสเกิดความเสี่ยง (Reduces Likelihood) การลดผลกระทบ (Reduces Impact) และกำหนดแผนรองรับเหตุการณ์ฉุกเฉินเพื่อให้ดำเนินงานได้ต่อเนื่อง

1.4 ตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

2. การทบทวนและปรับปรุงนโยบาย

2.1 ผู้อำนวยการต้องกำหนดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปตามการประเมินความเสี่ยง สถานการณ์การปฏิบัติงานในปัจจุบัน และการเปลี่ยนแปลงของเทคโนโลยีที่ใช้งานในระบบสารสนเทศของสำนักงาน

2.2 สำนักงานการทะเบียน ขอสงวนสิทธิ์ในการเปลี่ยนแปลงแก้ไข หรือเพิ่มเติมบางส่วนของนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามการประเมินความเสี่ยง สถานการณ์การปฏิบัติงานในปัจจุบัน และการเปลี่ยนแปลงของเทคโนโลยีที่ใช้ในงานในระบบสารสนเทศของสำนักงาน

<u>อ้างอิง</u>

- นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย
- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสภาความมั่นคงแห่งชาติ พ.ศ. 2565
- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ พ.ศ. 2565

ภาคผนวก ก

ลำดับชั้นความสำคัญของข้อมูลสารสนเทศด้านงานทะเบียน

สำนักงานการทะเบียน จัดแบ่งและจัดลำดับความสำคัญของข้อมูลสารสนเทศด้านงานทะเบียน ดังนี้

ระดับ	กลุ่มข้อมูล	ความสำคัญ	การจัดกลุ่มข้อมูล/การจัดลำดับชั้นย่อย
1	<u>ข้อมูลที่เป็นข้อมูลส่วนบุคคลของนิสิต</u> เช่น เลขประจำตัวนิสิต ชื่อ-นามสกุลของนิสิต ข้อมูลการศึกษาของนิสิตรายบุคคล	เป็นข้อมูลที่มีความสำคัญมาก หากสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อสำนักงานการทะเบียนและมหาวิทยาลัย การให้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของนิสิต เป็นไปตามนโยบายการบริหารจัดการการเข้าถึงและควบคุมการใช้งานสารสนเทศ การใช้ข้อมูลส่วนบุคคลของนิสิต เป็นไปตาม - หมวด จ. การใช้งานข้อมูลส่วนบุคคลร่วมกันกับส่วนงาน/หน่วยงานภายนอก - หมวด ฉ. การส่งหรือโอนข้อมูลไปยังต่างประเทศ ในนโยบายคุ้มครองข้อมูลส่วนบุคคลของนิสิต จุฬาลงกรณ์มหาวิทยาลัย	ข้อมูลส่วนบุคคลของนิสิต[1]มีการจัดกลุ่มข้อมูล เพื่อใช้สำหรับการกำหนดสิทธิการเข้าถึง ดังนี้ 1.1 ข้อมูลประวัตินิสิต: ข้อมูล ID / ข้อมูลที่อยู่และที่ติดต่อ / ข้อมูลประวัติ / ข้อมูลอัตลักษณ์ / ข้อมูลประวัติการศึกษาเดิม / ข้อมูลบุคคลที่สาม / ข้อมูลการศึกษาที่มหาวิทยาลัย (เฉพาะข้อมูลการเข้าศึกษา ประวัติและสถานภาพนิสิต และการสำเร็จการศึกษา) 1.2 ข้อมูลส่วนบุคคลประเภทพิเศษที่มีความอ่อนไหว: ข้อมูลสุขภาพ / ข้อมูลความพิการ / ข้อมูลตามใบรับรองแพทย์ / ข้อมูลชีวภาพ 1.3 ข้อมูลด้านการศึกษา: ข้อมูลการลงทะเบียนเรียน / ประวัติและผลการลงทะเบียนเรียน / ประวัติและผลการศึกษา / ประวัติการศึกษาต่างสถาบัน / ผลการกระทำผิดเกี่ยวกับการศึกษา 1.4 ข้อมูลเกี่ยวกับการเงิน 1.5 ข้อมูลทางเทคนิค 1.6 เอกสารหลักฐาน

[1] ศึกษานิยามและรายละเอียดของแต่ละข้อมูลได้ใน หมวด ข. นโยบายคุ้มครองข้อมูลส่วนบุคคลของนิสิต จุฬาลงกรณ์มหาวิทยาลัย

2	<u>ข้อมูลที่เป็นข้อมูลจำนวนและสถิติ</u> เช่น จำนวนนิสิตลงทะเบียน จำนวนนิสิตพ้นสถานภาพฯ ในแต่ละภาคการศึกษา สถิติผู้สำเร็จการศึกษา	เป็นข้อมูลที่อนุญาตให้ใช้ภายในคณะ/ส่วนงาน ภายในมหาวิทยาลัย หรือเผยแพร่สู่สาธารณะได้ แต่ยังมีการจำกัดขอบเขตการเข้าถึงตามความเหมาะสม กรณีเป็นข้อมูลเชิงลึกที่ใช้สำหรับการบริหาร วางแผน หรือกำหนดนโยบาย	ข้อมูลจำนวนและสถิติมีการจัดลำดับชั้นย่อย โดยเรียงตามลำดับความสำคัญและขอบเขตของข้อมูล ดังนี้ 2.1 ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับส่วนงาน (แดชบอร์ดระดับคณะ หรือ ข้อมูลจำนวนในระดับคณะ/ภาควิชา/หลักสูตร แล้วแต่กรณี) 2.2 ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับมหาวิทยาลัย (แดชบอร์ด CU Management หรือ ข้อมูลจำนวนในระดับมหาวิทยาลัย) 2.3 ข้อมูลจำนวนสถิติที่เป็นสาธารณะ (แดชบอร์ด CU Public, REG Statistics สถิติการให้บริการ หรือข้อมูลอื่นใดที่อยู่บนเอกสารเผยแพร่ต่างๆ)
3	<u>ข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคลของนิสิต</u> เช่น ข้อมูลหลักสูตร ข้อมูลรายวิชา ข้อมูลอาคาร ข้อมูลรหัสคณะ	เป็นข้อมูลที่เผยแพร่สู่สาธารณะได้และไม่ส่งผลกระทบใดกับสำนักงานการทะเบียน	ไม่มีการแบ่งลำดับชั้นย่อย

ภาคผนวก ข

การควบคุมการเข้าถึงฐานข้อมูลและการกำหนดสิทธิของผู้ใช้งานภายในสำนักงานการทะเบียน

ตำแหน่ง	กลุ่มผู้ใช้งาน	สิทธิของผู้ใช้งาน	ขอบเขตการใช้ข้อมูล	การยกเลิกหรือการสิ้นสุดของสิทธิ
ผู้อำนวยการสำนักงานการทะเบียน	ผู้บริหารสูงสุด	- ดูข้อมูล (View) - อนุมัติ (Approve) 1) ให้เผยแพร่/ส่งต่อข้อมูล 2) ให้แก้ไขข้อมูล 3) ให้บันทึกข้อมูล 4) ให้ลบข้อมูล	- การดูข้อมูล ดูข้อมูลทั้งหมดในสำนักงานการทะเบียนได้ - อนุมัติให้เผยแพร่/ส่งต้อข้อมูล แก้ไขข้อมูล บันทึกข้อมูลได้ **ยกเว้น** การอนุมัติให้ลบข้อมูล ต้องผ่านความเห็นชอบของคณะกรรมการบริหารสำนักงานการทะเบียน	เมื่อพ้นจากตำแหน่ง
รองผู้อำนวยการสำนักงานการทะเบียน	ผู้บริหาร	- ดูข้อมูล (View) - เผยแพร่/ส่งต่อข้อมูล (Disclose)	- การดูข้อมูล ดูข้อมูลทั้งหมดในสำนักงานการทะเบียนได้ - การเผยแพร่/ส่งต่อข้อมูล เฉพาะข้อมูลที่เกี่ยวข้องกับภารกิจการดำเนินงาน	เมื่อพ้นจากตำแหน่ง
ผู้อำนวยการฝ่ายทะเบียนนิสิต	ทน.	- ดูข้อมูล (View) - แก้ไขข้อมูล (Edit) - ขอเผยแพร่/ส่งต่อข้อมูล ผ่านการอนุมัติของผู้อำนวยการสำนักงานการทะเบียน (Disclose)	- การดูข้อมูล ดูข้อมูลทั้งหมดในสำนักงานการทะเบียนได้ - การแก้ไขข้อมูล เฉพาะข้อมูลที่เกี่ยวข้องกับภารกิจการดำเนินงานในฝ่ายทะเบียนนิสิต และที่สามารถแก้ไขเองในระบบได้ - การเผยแพร่/ส่งต่อข้อมูล เฉพาะข้อมูลที่เกี่ยวข้องกับภารกิจการดำเนินงานในฝ่ายทะเบียนนิสิต และต้องขออนุมัติผ่านผู้อำนวยการสำนักงานการทะเบียน	เมื่อพ้นจากตำแหน่ง

ตำแหน่ง	กลุ่มผู้ใช้งาน	สิทธิของผู้ใช้งาน	ขอบเขตการใช้ข้อมูล	การยกเลิกหรือการสิ้นสุดของสิทธิ
เจ้าหน้าที่ฝ่ายทะเบียนนิสิต	ทน.	- ดูข้อมูล (View) - สร้าง นำเข้า หรือบันทึกข้อมูล (Create/Import/Save) - แก้ไขข้อมูล (Edit)	- การดูข้อมูล ดูข้อมูลที่ใช้งานตามหน้าที่ความรับผิดชอบได้ - การสร้าง นำเข้า หรือบันทึกข้อมูล เฉพาะข้อมูลและระบบงานตามหน้าที่ความรับผิดชอบ - การแก้ไขข้อมูล เฉพาะข้อมูลตามหน้าที่ความรับผิดชอบ โดยเป็นไปตามแนวปฏิบัติ หรือโดยได้รับอนุมัติจากผู้อำนวยการสำนักงานการทะเบียน หรือตามคำสั่งของมหาวิทยาลัย หรือคำสั่งอื่นใดที่โดยชอบด้วยกฎหมาย แล้วแต่กรณี	- เมื่อสิ้นสุดสถานภาพการเป็นบุคลากรของมหาวิทยาลัยที่สังกัดสำนักงานการทะเบียน หรือสิ้นสุดการจ้างโดยสำนักงานการทะเบียน - เมื่อปรับเปลี่ยนตำแหน่งหรือย้ายงานและขอบเขตหน้าที่ความรับผิดชอบเปลี่ยนไปจากเดิม
ผู้อำนวยการฝ่ายทะเบียนการศึกษา	ทก.	- ดูข้อมูล (View) - แก้ไขข้อมูล (Edit) - ขอเผยแพร่/ส่งต่อข้อมูล ผ่านการอนุมัติของผู้อำนวยการสำนักงานการทะเบียน (Disclose)	- การดูข้อมูล ดูข้อมูลทั้งหมดในสำนักงานการทะเบียนได้ - การแก้ไขข้อมูล เฉพาะข้อมูลที่เกี่ยวข้องกับภารกิจการดำเนินงานในฝ่ายทะเบียนการศึกษา และที่สามารถแก้ไขเองในระบบได้ - การเผยแพร่/ส่งต่อข้อมูล เฉพาะข้อมูลที่เกี่ยวข้องกับภารกิจการดำเนินงานในฝ่ายทะเบียนการศึกษา และต้องขออนุมัติผ่านผู้อำนวยการสำนักงานการทะเบียน	เมื่อพ้นจากตำแหน่ง
เจ้าหน้าที่ฝ่ายทะเบียนการศึกษา	ทก.	- ดูข้อมูล (View) - สร้าง นำเข้า หรือบันทึกข้อมูล (Create/Import/Save) - แก้ไขข้อมูล (Edit)	- การดูข้อมูล ดูข้อมูลที่ใช้งานตามหน้าที่ความรับผิดชอบได้ - การสร้าง นำเข้า หรือบันทึกข้อมูล เฉพาะข้อมูลและระบบงานตามหน้าที่ความรับผิดชอบ - การแก้ไขข้อมูล เฉพาะข้อมูลตามหน้าที่ความรับผิดชอบ โดยเป็นไปตามแนวปฏิบัติ หรือโดยได้รับ	- เมื่อสิ้นสุดสถานภาพการเป็นบุคลากรของมหาวิทยาลัยที่สังกัดสำนักงานการทะเบียน หรือสิ้นสุดการจ้างโดยสำนักงานการทะเบียน - เมื่อปรับเปลี่ยนตำแหน่งหรือย้ายงานและขอบเขตหน้าที่ความรับผิดชอบเปลี่ยนไปจากเดิม

ตำแหน่ง	กลุ่มผู้ใช้งาน	สิทธิของผู้ใช้งาน	ขอบเขตการใช้ข้อมูล	การยกเลิกหรือการสิ้นสุดของสิทธิ
			อนุมัติจากผู้อำนวยการสำนักงานการทะเบียน หรือตามคำสั่งของมหาวิทยาลัย หรือคำสั่งอื่นใดที่โดยชอบด้วยกฎหมาย แล้วแต่กรณี	
ผู้อำนวยการฝ่ายบริหาร	บห.	- ดูข้อมูล (View) - แก้ไขข้อมูล (Edit) - ขอเผยแพร่/ส่งต่อข้อมูล ผ่านการอนุมัติของผู้อำนวยการสำนักงานการทะเบียน (Disclose)	- การดูข้อมูล ดูข้อมูลทั้งหมดในสำนักงานการทะเบียนได้ - การแก้ไขข้อมูล เฉพาะข้อมูลที่เกี่ยวข้องกับภารกิจการดำเนินงานในฝ่ายบริหาร และที่สามารถแก้ไขเองในระบบได้ - การเผยแพร่/ส่งต่อข้อมูล เฉพาะข้อมูลที่เกี่ยวข้องกับภารกิจการดำเนินงานในฝ่ายบริหาร และต้องขออนุมัติผ่านผู้อำนวยการสำนักงานการทะเบียน	เมื่อพ้นจากตำแหน่ง
เจ้าหน้าที่ฝ่ายบริหาร	บห.	- ดูข้อมูล (View) - สร้าง นำเข้า หรือบันทึกข้อมูล (Create/Import/Save)	- การดูข้อมูล ดูข้อมูลที่ใช้งานตามหน้าที่ความรับผิดชอบได้ - การสร้าง นำเข้า หรือบันทึกข้อมูล เฉพาะข้อมูลและระบบงานตามหน้าที่ความรับผิดชอบ	- เมื่อสิ้นสุดสถานภาพการเป็นบุคลากรของมหาวิทยาลัยที่สังกัดสำนักงานการทะเบียน หรือสิ้นสุดการจ้างโดยสำนักงานการทะเบียน - เมื่อปรับเปลี่ยนตำแหน่งหรือย้ายงานและขอบเขตหน้าที่ความรับผิดชอบเปลี่ยนไปจากเดิม
ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ	ทส.	- ดูข้อมูล (View) - สร้าง นำเข้า หรือบันทึกข้อมูล (Create/Import/Save) - แก้ไขข้อมูล (Edit) - ขอเผยแพร่/ส่งต่อข้อมูล ผ่านการอนุมัติของผู้อำนวยการสำนักงานการทะเบียน (Disclose)	- การดูข้อมูล ดูข้อมูลทั้งหมดในสำนักงานการทะเบียนได้ - การสร้าง นำเข้า หรือบันทึกข้อมูล เฉพาะข้อมูลและระบบงานตามหน้าที่ความรับผิดชอบ - การแก้ไขข้อมูล เป็นไปตามแนวปฏิบัติ หรือโดยได้รับอนุมัติจากผู้อำนวยการสำนักงานการทะเบียน หรือตามคำสั่งของมหาวิทยาลัย หรือคำสั่งอื่นใดที่โดยชอบด้วยกฎหมาย แล้วแต่กรณี	เมื่อพ้นจากตำแหน่ง

ตำแหน่ง	กลุ่มผู้ใช้งาน	สิทธิของผู้ใช้งาน	ขอบเขตการใช้ข้อมูล	การยกเลิกหรือการสิ้นสุดของสิทธิ
		- ลบข้อมูล (Delete)	- การเผยแพร่/ส่งต่อข้อมูล ต้องขออนุมัติผ่านผู้อำนวยการสำนักงานการทะเบียน - การลบข้อมูล เป็นไปตามแนวปฏิบัติ หรือโดยได้รับอนุมัติจากผู้อำนวยการสำนักงานการทะเบียน โดยผ่านมติจากคณะกรรมการบริหารสำนักงานการทะเบียน หรือตามคำสั่งของมหาวิทยาลัย หรือคำสั่งอื่นใดที่โดยชอบด้วยกฎหมาย แล้วแต่กรณี	
เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ	ทส.	- ดูข้อมูล (View) - สร้าง นำเข้า หรือบันทึกข้อมูล (Create/Import/Save) - แก้ไขข้อมูล (Edit) - ลบข้อมูล (Delete)	- การดู ดูข้อมูลทั้งหมดในสำนักงานการทะเบียนได้ - การสร้าง นำเข้า หรือบันทึกข้อมูล เฉพาะข้อมูลและระบบงานตามหน้าที่ความรับผิดชอบ - การแก้ไขข้อมูล เป็นไปตามแนวปฏิบัติ หรือโดยได้รับอนุมัติจากผู้อำนวยการสำนักงานการทะเบียน หรือตามคำสั่งของมหาวิทยาลัย หรือคำสั่งอื่นใดที่โดยชอบด้วยกฎหมาย แล้วแต่กรณี - การลบข้อมูล เป็นไปตามแนวปฏิบัติ หรือโดยได้รับอนุมัติจากผู้อำนวยการสำนักงานการทะเบียน โดยผ่านมติจากคณะกรรมการบริหารสำนักงานการทะเบียน หรือตามคำสั่งของมหาวิทยาลัย หรือคำสั่งอื่นใดที่โดยชอบด้วยกฎหมาย แล้วแต่กรณี	- เมื่อสิ้นสุดสถานภาพการเป็นบุคลากรของมหาวิทยาลัยที่สังกัดสำนักงานการทะเบียน หรือสิ้นสุดการจ้างโดยสำนักงานการทะเบียน - เมื่อปรับเปลี่ยนตำแหน่งหรือย้ายงานและขอบเขตหน้าที่ความรับผิดชอบเปลี่ยนไปจากเดิม

ภาคผนวก ค

การควบคุมการเข้าถึงและการกำหนดสิทธิของผู้ใช้งานภายนอกสำนักงานการทะเบียน

ข้อมูลระดับ 1: ข้อมูลที่เป็นข้อมูลส่วนบุคคลของนิสิต										
ระบบงานของสำนักงานการทะเบียนที่เกี่ยวข้อง: 1. ระบบ REG 2. ระบบ Gloves 3. ระบบ Grading										
ตำแหน่ง	**ระดับการเข้าถึงข้อมูล**	**กลุ่มข้อมูลที่เข้าถึง[2]**				**เข้าถึงได้โดยได้รับสิทธิ User Account สำหรับระบบงานต่างๆ ของสำนักงานการทะเบียน**				**เข้าถึงโดยการทำบันทึกขอข้อมูล โดยผอ.สนท.พิจารณาอนุมัติเป็นกรณี**
		ข้อมูลประวัตินิสิต	**ข้อมูลอ่อนไหว**	**ข้อมูลด้านการศึกษา**	**ข้อมูลเกี่ยวกับการเงิน**	**จำนวนสิทธิสูงสุด ต่อ 1 ระบบงาน**	**การได้สิทธิ/การขอสิทธิ**	**การมอบสิทธิ**	**การยกเลิกหรือการสิ้นสุดของสิทธิ**	
อธิการบดี	มหาวิทยาลัย	O	O	O	O	2	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากสภามหาวิทยาลัย	ไม่ได้	เมื่อพ้นจากตำแหน่ง	
รองอธิการบดี ด้านกิจการนิสิต	มหาวิทยาลัย	O	O		O	2	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากอธิการบดี	ไม่ได้	เมื่อพ้นจากตำแหน่ง	
รองอธิการบดี ด้านการเงินและการบัญชี	มหาวิทยาลัย	O			O	2	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากอธิการบดี	ไม่ได้	เมื่อพ้นจากตำแหน่ง	

[2] ดู ภาคผนวก ก ประกอบ

ข้อมูลระดับ 1: ข้อมูลที่เป็นข้อมูลส่วนบุคคลของนิสิต										
ระบบงานของสำนักงานการทะเบียนที่เกี่ยวข้อง: 1. ระบบ REG 2. ระบบ Gloves 3. ระบบ Grading										
ตำแหน่ง	**ระดับการเข้าถึงข้อมูล**	**กลุ่มข้อมูลที่เข้าถึง[2]**				**เข้าถึงได้โดยได้รับสิทธิ User Account สำหรับระบบงานต่างๆ ของสำนักงานการทะเบียน**				**เข้าถึงโดยการทำบันทึกขอข้อมูล โดยผอ.สนท.พิจารณาอนุมัติเป็นกรณี**
		ข้อมูลประวัตินิสิต	**ข้อมูลอ่อนไหว**	**ข้อมูลด้านการศึกษา**	**ข้อมูลเกี่ยวกับการเงิน**	**จำนวนสิทธิสูงสุด ต่อ 1 ระบบงาน**	**การได้สิทธิ/การขอสิทธิ**	**การมอบสิทธิ**	**การยกเลิกหรือการสิ้นสุดของสิทธิ**	
รองอธิการบดี ด้านกฎหมาย	มหาวิทยาลัย	O				2	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากอธิการบดี	ไม่ได้	เมื่อพ้นจากตำแหน่ง	
รองอธิการบดี ด้านวิชาการ	มหาวิทยาลัย	O		O		2	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากอธิการบดี	ไม่ได้	เมื่อพ้นจากตำแหน่ง	
คณบดี	คณะ	O	O	O	O	2	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากสภามหาวิทยาลัย	ไม่ได้	เมื่อพ้นจากตำแหน่ง	
รองคณบดี ด้านบริหาร	คณะ	O			O	1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากอธิการบดี	ไม่ได้	เมื่อพ้นจากตำแหน่ง	
รองคณบดี ด้านวิชาการ	คณะ	O		O		1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากอธิการบดี	ไม่ได้	เมื่อพ้นจากตำแหน่ง	

ข้อมูลระดับ 1: ข้อมูลที่เป็นข้อมูลส่วนบุคคลของนิสิต										
ระบบงานของสำนักงานการทะเบียนที่เกี่ยวข้อง: 1. ระบบ REG 2. ระบบ Gloves 3. ระบบ Grading										
ตำแหน่ง	**ระดับการเข้าถึงข้อมูล**	**กลุ่มข้อมูลที่เข้าถึง[2]**				**เข้าถึงได้โดยได้รับสิทธิ User Account สำหรับระบบงานต่างๆ ของสำนักงานการทะเบียน**				**เข้าถึงโดยการทำบันทึกขอข้อมูล โดยผอ.สนท.พิจารณาอนุมัติเป็นกรณี**
		ข้อมูลประวัตินิสิต	**ข้อมูลอ่อนไหว**	**ข้อมูลด้านการศึกษา**	**ข้อมูลเกี่ยวกับการเงิน**	**จำนวนสิทธิสูงสุด ต่อ 1 ระบบงาน**	**การได้สิทธิ/การขอสิทธิ**	**การมอบสิทธิ**	**การยกเลิกหรือการสิ้นสุดของสิทธิ**	
รองคณบดี ด้านกิจการนิสิต	คณะ	O	O		O	1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากอธิการบดี	ไม่ได้	เมื่อพ้นจากตำแหน่ง	
นายทะเบียนคณะ	คณะ	O		O	O	1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากคณบดี	ไม่ได้	เมื่อพ้นจากตำแหน่ง	
เจ้าหน้าที่คณะที่ปฏิบัติงานด้านทะเบียน	คณะ	O		O	O	1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งหรือบันทึกแต่งตั้งจากนายทะเบียน	ไม่ได้	ตามภารกิจที่ได้รับมอบและคณะแจ้งเปลี่ยนแปลงสิทธิ	
หัวหน้าภาควิชา	ภาควิชา	O		O	O	1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งจากสภามหาวิทยาลัย	ไม่ได้	เมื่อพ้นจากตำแหน่ง	
รองหัวหน้าภาควิชา	ภาควิชา	O		O	O	1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งโดยหัวหน้าภาควิชา	ไม่ได้	เมื่อพ้นจากตำแหน่ง	

ข้อมูลระดับ 1: ข้อมูลที่เป็นข้อมูลส่วนบุคคลของนิสิต										
ระบบงานของสำนักงานการทะเบียนที่เกี่ยวข้อง: 1. ระบบ REG 2. ระบบ Gloves 3. ระบบ Grading										
ตำแหน่ง	**ระดับการเข้าถึงข้อมูล**	**กลุ่มข้อมูลที่เข้าถึง[2]**				**เข้าถึงได้โดยได้รับสิทธิ User Account สำหรับระบบงานต่างๆ ของสำนักงานการทะเบียน**				**เข้าถึงโดยการทำบันทึกขอข้อมูล โดยผอ.สนท.พิจารณาอนุมัติเป็นกรณี**
		ข้อมูลประวัตินิสิต	**ข้อมูลอ่อนไหว**	**ข้อมูลด้านการศึกษา**	**ข้อมูลเกี่ยวกับการเงิน**	**จำนวนสิทธิสูงสุด ต่อ 1 ระบบงาน**	**การได้สิทธิ/การขอสิทธิ**	**การมอบสิทธิ**	**การยกเลิกหรือการสิ้นสุดของสิทธิ**	
เจ้าหน้าที่ภาควิชา	ภาควิชา	O		O	O	1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งหรือบันทึกโดยหัวหน้าภาควิชา	ไม่ได้	ตามภารกิจที่ได้รับมอบและภาคแจ้งเปลี่ยนแปลงสิทธิ	
หัวหน้าสาขา/ประธานหลักสูตร	สาขา/หลักสูตร			O	O	1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งโดยคณบดี/หัวหน้าภาควิชา	ไม่ได้	ตามภารกิจที่ได้รับมอบ	
เจ้าหน้าที่หลักสูตร	หลักสูตร	O		O	O	1	ได้สิทธิโดยตำแหน่ง สนท.กำหนดให้เมื่อมีคำสั่งแต่งตั้งหรือบันทึกโดยหัวหน้าภาควิชา	ไม่ได้	ตามภารกิจที่ได้รับมอบ	
อาจารย์ที่ปรึกษา	นิสิตในที่ปรึกษา	O		O	O	1	เมื่อส่งข้อมูลอาจารย์ที่ปรึกษาพร้อมรายชื่อนิสิตในที่ปรึกษา โดยผ่านหัวหน้าภาควิชาหรือคณบดี	ไม่ได้	ตามภารกิจที่ได้รับมอบ	

ข้อมูลระดับ 1: ข้อมูลที่เป็นข้อมูลส่วนบุคคลของนิสิต										
ระบบงานของสำนักงานการทะเบียนที่เกี่ยวข้อง: 1. ระบบ REG 2. ระบบ Gloves 3. ระบบ Grading										
ตำแหน่ง	**ระดับการเข้าถึงข้อมูล**	**กลุ่มข้อมูลที่เข้าถึง[2]**				**เข้าถึงได้โดยได้รับสิทธิ User Account สำหรับระบบงานต่างๆ ของสำนักงานการทะเบียน**				**เข้าถึงโดยการทำบันทึกขอข้อมูล โดยผอ.สนท.พิจารณาอนุมัติเป็นกรณี**
		ข้อมูลประวัตินิสิต	**ข้อมูลอ่อนไหว**	**ข้อมูลด้านการศึกษา**	**ข้อมูลเกี่ยวกับการเงิน**	**จำนวนสิทธิสูงสุด ต่อ 1 ระบบงาน**	**การได้สิทธิ/การขอสิทธิ**	**การมอบสิทธิ**	**การยกเลิกหรือการสิ้นสุดของสิทธิ**	
ผู้รับผิดชอบรายวิชา	นิสิตที่ลงทะเบียนเรียนในรายวิชา	O		O		1	ได้สิทธิตามข้อมูลที่คณะหรอภาควิชาแจ้งมา	ไม่ได้	ตามภารกิจที่ได้รับมอบ	
นิสิต	ข้อมูลของตัวเอง	O	O	O	O	1	เมื่อมีสถานภาพเป็นนิสิต	ไม่ได้	เมื่อพ้นสถานภาพการเป็นนิสิต และ สบท. ดำเนินการลบข้อมูล CUNET Account แล้ว	
สำนักบริหารเทคโนโลยีสารสนเทศ	มหาวิทยาลัย	O				-	-	-	-	O
ศูนย์บริการสุขภาพ	มหาวิทยาลัย	O				-	-	-	-	O
ศูนย์กีฬาฯ	มหาวิทยาลัย	O				-	-	-	-	O
สำนักวิทยทรัพยากร	มหาวิทยาลัย	O				-	-	-	-	O
สำนักบริหารการเงิน การบัญชี และการพัสดุ	มหาวิทยาลัย	O				-	-	-	-	O

ข้อมูลระดับ 1: ข้อมูลที่เป็นข้อมูลส่วนบุคคลของนิสิต										
ระบบงานของสำนักงานการทะเบียนที่เกี่ยวข้อง: 1. ระบบ REG 2. ระบบ Gloves 3. ระบบ Grading										
ตำแหน่ง	**ระดับการเข้าถึงข้อมูล**	**กลุ่มข้อมูลที่เข้าถึง[2]**				**เข้าถึงได้โดยได้รับสิทธิ User Account สำหรับระบบงานต่างๆ ของสำนักงานการทะเบียน**				**เข้าถึงโดยการทำบันทึกขอข้อมูล โดยผอ.สนท.พิจารณาอนุมัติเป็นกรณี**
		ข้อมูลประวัตินิสิต	**ข้อมูลอ่อนไหว**	**ข้อมูลด้านการศึกษา**	**ข้อมูลเกี่ยวกับการเงิน**	**จำนวนสิทธิสูงสุด ต่อ 1 ระบบงาน**	**การได้สิทธิ/การขอสิทธิ**	**การมอบสิทธิ**	**การยกเลิกหรือการสิ้นสุดของสิทธิ**	
สำนักกฎหมายและนิติการ	มหาวิทยาลัย	O				-	-	-	-	O

ข้อมูลระดับ 2: ข้อมูลจำนวนและสถิติ					
ระบบงานของสำนักงานการทะเบียนที่เกี่ยวข้อง: 1. ระบบ Dashboard					
ตำแหน่ง/กลุ่มบุคคล	**ขอบเขตข้อมูล**	**จำนวนสิทธิ ต่อ 1 ระบบงาน**	**การขอรับสิทธิ**	**การมอบสิทธิ**	**การยกเลิกหรือการสิ้นสุดของสิทธิ**
อธิการบดี	ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับมหาวิทยาลัย	1	ได้โดยตำแหน่งเมื่อมีคำสั่ง		
รองอธิการบดี	ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับมหาวิทยาลัย	1	ได้โดยตำแหน่งเมื่อมีคำสั่ง		
คณบดี	- ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับมหาวิทยาลัย - ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับคณะที่สังกัด	1	ได้โดยตำแหน่งเมื่อมีคำสั่ง		
หัวหน้าภาควิชา	ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับคณะที่สังกัด	1	ได้โดยตำแหน่งเมื่อมีคำสั่ง		
หัวหน้าสาขา/ประธานหลักสูตร	ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับคณะที่สังกัด	1	ได้โดยตำแหน่งเมื่อมีคำสั่ง		
ประธานหลักสูตร	ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับคณะที่สังกัด	1	ได้โดยตำแหน่งเมื่อมีคำสั่ง		
อาจารย์ที่ปรึกษา/อาจารย์ผู้สอน	ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับคณะที่สังกัด	1	ทำบันทึกขอ		
เจ้าหน้าที่คณะที่ได้รับมอบหมาย	ข้อมูลจำนวนสถิติเชิงลึกสำหรับการใช้งานวิเคราะห์ในระดับคณะที่สังกัด	1	ทำบันทึกขอ		
นิสิต/บุคคลทั่วไป	ข้อมูลจำนวนสถิติที่เป็นสาธารณะ	ไม่ต้องขอสิทธิ โดยสามารถเข้าถึงข้อมูลสถิติสาธารณะได้จาก CU Public Dashboard, REG Statistics Dashboard หรือสถิติการให้บริการบนเว็บไซต์ของสำนักงานการทะเบียน			