



แนวปฏิบัติการควบคุมการเข้าถึง และการใช้งานระบบสารสนเทศ

การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

การจัดทำระบบการลงทะเบียนผู้ใช้งาน
เพื่อตรวจสอบสิทธิการเข้าถึง พร้อมทั้งทบทวนสิทธิ

การกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่ม

- ผู้ดูแลระบบ
- ผู้ใช้งานระบบ

การทบทวนสิทธิ

- ลาออก
- เปลี่ยนตำแหน่ง
- โอน ย้าย
- สิ้นสุดการจ้าง

ผู้ใช้งานระบบสารสนเทศต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารของหน่วยงานนั้น

ระบบสารสนเทศต้องมีการจัดแบ่งประเภทและความสำคัญ ลำดับชั้นความลับ และการเข้าถึงข้อมูล

จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด
- ข้อมูลลับมาก
- ข้อมูลลับ
- ข้อมูลทั่วไป

จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ดูแลระบบ
- ระดับชั้นสำหรับผู้ปฏิบัติงาน
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

การกำหนดเวลาที่สามารถเข้าใช้งานระบบสารสนเทศ

- ระบบยืนยันตัวตนก่อนเข้าใช้งานระบบ
- สามารถเข้าใช้งานได้ตลอด 24 ชั่วโมง 7 วัน
- ยุติการใช้งานโดยการออกจากระบบโดยอัตโนมัติ เมื่อไม่มีการใช้งานในช่วงระยะเวลา 10 นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

แนวทางการควบคุมการเข้าถึง และการแบ่งระดับชั้นและสิทธิการเข้าถึง

- ระดับผู้ดูแลระบบ มีหน้าที่ในการควบคุมการเข้าถึงข้อมูล รวมไปถึงวิธีการทำลายข้อมูล
- ระดับเจ้าของข้อมูล มีหน้าที่ตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง
- ระดับผู้ปฏิบัติงาน มีหน้าที่ในการบันทึก ตรวจสอบ ปรับปรุง และรายงานข้อมูล
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป มีสิทธิในการใช้ข้อมูลตามสิทธิที่มอบให้เท่านั้น

2. การบริหารจัดการ การเข้าถึงของผู้ใช้งาน

1. จัดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยสารสนเทศ
2. กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน
3. การบริหารจัดการสิทธิของผู้ใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม
4. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

ขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน

- จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิ
- ระบุข้อมูลผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน โดยกำหนดเป็นชื่อภาษาอังกฤษ และตัวเลข
- ตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่
- เอกสารแบบฟอร์มแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย
- การอนุญาตให้เข้าถึงระบบสารสนเทศ ต้องได้รับการอนุญาตจากผู้บริหาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย
- หลักเกณฑ์ในการยกเลิกให้เข้าถึงระบบสารสนเทศเมื่อลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

การบริหารจัดการสิทธิของผู้ใช้งาน

- กำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ
- การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึงระบบสารสนเทศ
- บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิของผู้ใช้งาน

การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

1. การตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยดังนี้

- ตัวอักษร+ตัวเลข ไม่น้อยกว่าหรือเท่ากับ 8 ตัวอักษร
- ไม่ใช่ชื่อ - นามสกุลของตนเอง หรือบุคคลใกล้ชิดตน
- วัน เดือน ปีเกิด
- เบอร์โทรศัพท์
- คำศัพท์ที่ใช้ในพจนานุกรม

ตัวอย่างรหัสผ่าน

ใช้คำภาษาไทย พิมพ์คีย์บอร์ดภาษาอังกฤษ

คำภาษาไทย = ห้ามลืม555

คำภาษาอังกฤษ = shk,]n,555

2. ห้ามส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานทาง e-mail หรือช่องทางอื่นทางโซเชียล

3. ให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีหลังจากใช้รหัสผ่านชั่วคราวเข้าระบบ

4. ไม่ให้รหัสผ่านกับผู้อื่น และ เปลี่ยนรหัสผ่านทุก ๆ 180 วันหรือตามการแจ้งเตือนจากผู้ดูแลระบบ

การรักษาห้สผ่านเพิ่มเติม

- การกำหนดวิธีปฏิบัติการใช้งานรห้สผ่าน ตามวิธีการบริหารจัดการรห้สผ่านสำหรับผู้ใช้งาน
- เก็บรักษาห้สผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
- เก็บรห้สผ่านไว้เป็นความลับ ห้ามจดไว้ในที่เปิดเผย
- ห้ามให้โปรแกรมเข้าใช้งานบนที่กรห้สผ่าน
- กรณีที่มีความจำเป็นต้องบอกรห้สผ่านแก่ผู้อื่นเนื่องจากงาน ให้ทำการเปลี่ยนรห้สผ่านโดยทันที
- ผู้ดูแลระบบต้องเปลี่ยนรห้สผ่าน ถึ่กว่าผู้ใช้งานทั่วไป

การป้องกันอุปกรณ์คอมพิวเตอร์ และระบบสารสนเทศ

- มีบัญชีควบคุมอุปกรณ์ที่ใช้งานเพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต
- อุปกรณ์ที่ไม่มีการใช้งานต้องเก็บไว้ในที่ปลอดภัย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- ต้องใส่รหัสผ่านก่อนเข้าใช้งานคอมพิวเตอร์
- ล็อกหน้าจอคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเป็นเวลา 10 นาที
- กำหนดให้ระบบสารสนเทศ ออกจากระบบอัตโนมัติเมื่อไม่ได้ใช้งานเป็นเวลา 10 นาที
- ออกจากระบบสารสนเทศทันทีที่ใช้งานเสร็จ

การควบคุมทรัพย์สินสารสนเทศ และการใช้งานระบบคอมพิวเตอร์

สำหรับห้อง Data Center

- พื้นที่ต้องติดตั้งสัญญาณเตือนภัย เพื่อแจ้งเตือนเมื่อมีการบุกรุก
- ทดสอบระบบป้องกันการบุกรุก เพื่อตรวจสอบว่าใช้งานได้ตามปกติ
- บันทึกวันและเวลาเข้า-ออก พื้นที่
- ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่
- ผู้มาเยือนต้องติดบัตรก่อนเข้าพื้นที่

มาตรการทำลายสื่อบันทึกข้อมูล/ข้อมูลอิเล็กทรอนิกส์

- สื่อบันทึกข้อมูลที่เป็นประเภทงานแม่เหล็กให้ทำการ Format หรือวิธีบดขยี้
- สื่อบันทึกข้อมูลประเภท Optical Disk ทำลาย โดยวิธีบดขยี้ หรือการหัก
- สื่อบันทึกข้อมูลขนาดเล็กแบบพกพา (Flash Drive) ให้ทำการ Format
- มีกระบวนการในการลบหรือเขียนข้อมูลทับบนข้อมูลก่อนเพื่อป้องกันการเข้าถึงข้อมูล เช่นการกู้ข้อมูล
- ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ

5. การควบคุมการเข้าถึงระบบปฏิบัติการระบบสารสนเทศ

1. ผู้ดูแลระบบ ต้องติดตั้งโปรแกรมช่วยบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงาน หรือ Active Directory
2. การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตน
3. ระบบสารสนเทศต้องมีการยืนยันตัวตนของผู้ใช้งาน
4. การบริหารจัดการรหัสผ่าน โดยผู้ใช้งานต้องเปลี่ยนรหัสผ่านในครั้งแรกที่เข้าสู่ระบบ
5. การควบคุมโปรแกรม ที่ผู้ใช้สามารถหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้
6. เมื่อไม่มีการใช้งานระบบสารสนเทศในระยะเวลาที่กำหนดให้ยุติการใช้งานระบบ ซึ่งกำหนดไว้ 10 นาที
7. การจำกัดระยะเวลาการเชื่อมต่อบนเครือข่าย กำหนดได้ไม่เกินครั้งละ 2 ชม.

6. การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

1. การจำกัดการเข้าถึงสารสนเทศ

- กรณีมีการจ้างเหมาพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก
- บริหารจัดการการเข้าถึงผู้ใช้งาน

2. ระบบซึ่งไวต่อการรบกวนและมีความสำคัญสูงต่อหน่วยงาน

- ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น เช่น ระบบทะเบียนและวัดผลนักศึกษา
- มีห้องปฏิบัติงานเป็นสัดส่วน และกำหนดสิทธิเฉพาะผู้มีสิทธิใช้งาน

3. อุปกรณ์คอมพิวเตอร์และระบบการสื่อสาร

- ผู้ใช้จึงต้องใช้งานอุปกรณ์อย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย
- โปรแกรมลิขสิทธิ์ของมหาวิทยาลัย ห้ามผู้ใช้งานไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว

4. การปฏิบัติงานจากภายนอกหน่วยงาน

- บุคคลภายนอกที่ต้องการเข้าใช้งานระบบสารสนเทศ ต้องเขียนแบบฟอร์มขออนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง
- ต้องนามในสัญญาการไม่เปิดเผยข้อมูลของมหาวิทยาลัย

7. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1. ผู้ต้องการใช้งาน ต้องทำการลงทะเบียนกับผู้ดูแลระบบ
2. ผู้ดูแลระบบเครือข่ายมหาวิทยาลัย ต้องดำเนินการดังต่อไปนี้
 - การวางอุปกรณ์กระจายสัญญาณในที่ที่เหมาะสม เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าใช้ระบบ
 - ตั้งค่าล็อกอินและรหัสผ่านการทำงานของอุปกรณ์ไร้ ที่สายคาดเดาได้ยาก
 - ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนระบบเครือข่ายไร้สาย
 - ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน
 - ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

การใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของหน่วยงาน

1. การใช้งานทั่วไป

- ผู้ใช้งานต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน
- ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว
- ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องตรวจสอบไวรัสก่อนใช้งาน

2. การสำรองข้อมูลและการกู้คืน

- ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลไว้บนสื่อบันทึกอื่น ๆ
- ผู้ใช้งานมีหน้าที่เก็บรักษาข้อมูล การสำรองข้อมูลให้เก็บไว้ในที่เหมาะสม

การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-MAIL)

การกำหนดสิทธิการเข้าถึง

- ผู้ที่ต้องการใช้งานต้องกรอกแบบฟอร์มเพื่อขอลงทะเบียน
- ผู้ใช้งานจะต้องรักษาชื่อผู้ใช้รหัสผ่านเป็นความลับ
- ห้ามเข้าถึง E-mail ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ
- หลังการใช้งานให้ออกจากระบบทุกครั้ง

การใช้งานระบบอินเทอร์เน็ต

- การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส
- ไม่ใช้ระบบอินเทอร์เน็ตของมหาวิทยาลัย หาประโยชน์ในเชิงพาณิชย์
- ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน
- ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมละเมิดลิขสิทธิ์
- การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น ที่ยั่วยุ หรือ ให้ร้าย
- ออกจากระบบเครือข่าย และปิดเว็บเบราว์เซอร์ทุกครั้งเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

การใช้งานเครือข่ายสังคมออนไลน์

- อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ ตามที่มหาวิทยาลัยได้กำหนดไว้เท่านั้น
- ผู้ใช้งานต้องตระหนักถึงความมั่นคงปลอดภัยในการใช้งาน และต้องรับผิดชอบหากเกิดความเสียหาย
- ไม่อนุญาตให้ใช้งานเผยแพร่ข้อมูลที่เป็นความลับ และมีผลกระทบต่อบุคคลอื่น
- ให้ใช้งานเครือข่ายสังคมออนไลน์ได้เท่าที่จำเป็นโดยไม่เบียดบังเวลาปฏิบัติงาน
- หากเกิดปัญหาจากการใช้งาน ต้องแจ้งผู้ดูแลระบบโดยเร็วเพื่อดำเนินการตามความเหมาะสม

การเก็บข้อมูลจราจรคอมพิวเตอร์

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ดังต่อไปนี้

1. จัดเก็บข้อมูลระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ ข้อมูลที่จัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง
2. ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้
3. กำหนดให้มีการเก็บบันทึกการทำงานของระบบ ไว้อย่างน้อย 90 วัน
4. จำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เข้าถึงได้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

แนวปฏิบัติระบบสารสนเทศ และระบบสำรองของสารสนเทศ

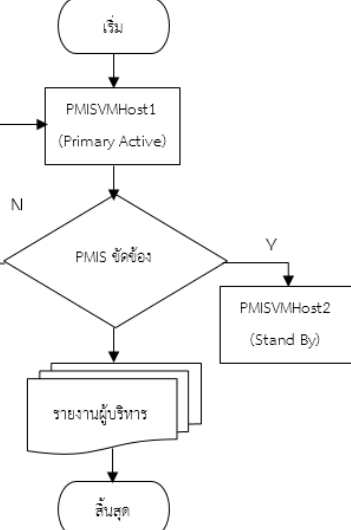
หน่วยงานภายในมหาวิทยาลัย ต้องให้ผู้รับผิดชอบระบบสารสนเทศทุกระบบ
จัดทำแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล โดยจัดระบบสำรองที่
เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

การจัดทำบัญชีระบบสารสนเทศทั้งหมดของหน่วยงาน และการสำรองข้อมูลระบบสารสนเทศ

- กำหนดความถี่ในการสำรอง พร้อมบันทึก วัน/เวลา ชื่อข้อมูลที่สำรอง
- ตรวจสอบความครบถ้วนของการสำรองข้อมูลที่เกี่ยวข้อง เช่น คอนฟิกูเรชัน และซอฟต์แวร์ร่วมต่าง ๆ
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ กรณีเกิดความเสียหายกับอุปกรณ์สำรองหลัก
- จัดทำคู่มือขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล
- มีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ

จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

- กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้อง
- กำหนดขั้นตอนปฏิบัติในการสำรอง
และทดสอบการกู้คืนระบบสารสนเทศ
- กำหนดเป็นแผนการสำรองระบบสารสนเทศ
- มีการทบทวนเพื่อปรับปรุงแผนให้สอดคล้องกับภารกิจ
อย่างน้อยปีละ 1 ครั้ง

 ม.ร.ว. เทวพรบุรณ	ขั้นตอนการปฏิบัติงาน (Work Procedure) ขั้นตอนการสำรองระบบสารสนเทศ	เขียนโดย นายไพฑูรย์ กันยา ตำแหน่ง นักวิชาการคอมพิวเตอร์ โทรศัพท์ ๐๕๖ ๗๖๗๑๐๐ ต่อ ๒๘๓๑๑ ๒๘๓๑๒ โทรศัพท์มือถือ ๐๘๖๐๗๗๒๘๕๖ อนุมัติโดย งานวิจัยและพัฒนาซอฟต์แวร์ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
ผู้รับผิดชอบ	กิจกรรม	ผู้เกี่ยวข้อง
ไพฑูรย์ กันยา	 <pre> graph TD Start([เริ่ม]) --> Host1[PMISVMHost1 (Primary Active)] Host1 --> Decision{PMIS จัดซื้อ} Decision -- Y --> Host2[PMISVMHost2 (Stand By)] Decision -- N --> Report[รายงานผู้บริหาร] Host2 --> Report Report --> End([สิ้นสุด]) </pre>	งานวิจัยและพัฒนาซอฟต์แวร์คอมพิวเตอร์ และเครือข่าย โทรศัพท์ ๐๕๖ ๗๖๗๑๐๐ ต่อ ๒๘๓๑๑ - ๓๓๑ โทรศัพท์มือถือ ๐๘๖ ๐๗๗ ๒๘๕๖

แนวปฏิบัติการตรวจสอบ และประเมินความเสี่ยงด้านสารสนเทศ

1. จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย
เพื่อตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
2. แนวทางในการตรวจสอบและประเมินความเสี่ยง

แนวปฏิบัติการใช้งานระบบสื่อสารโทรศัพท์ภายใน มหาวิทยาลัย

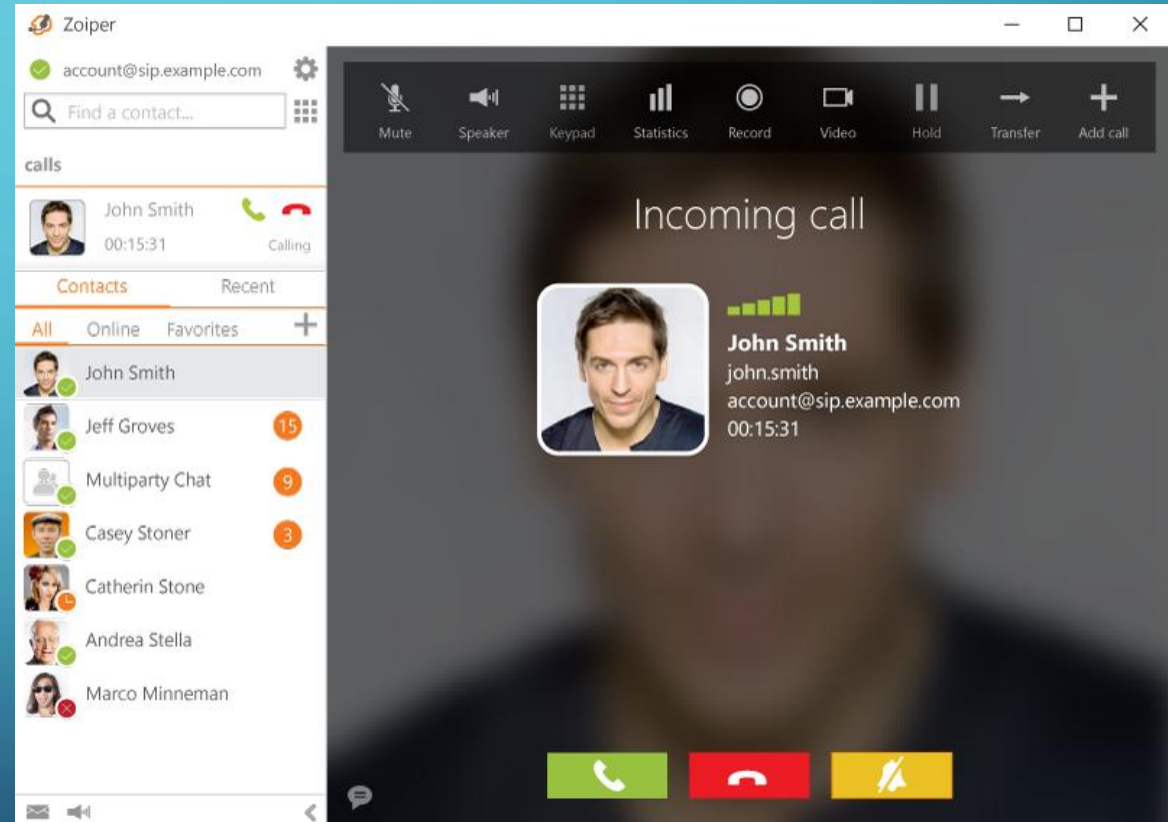
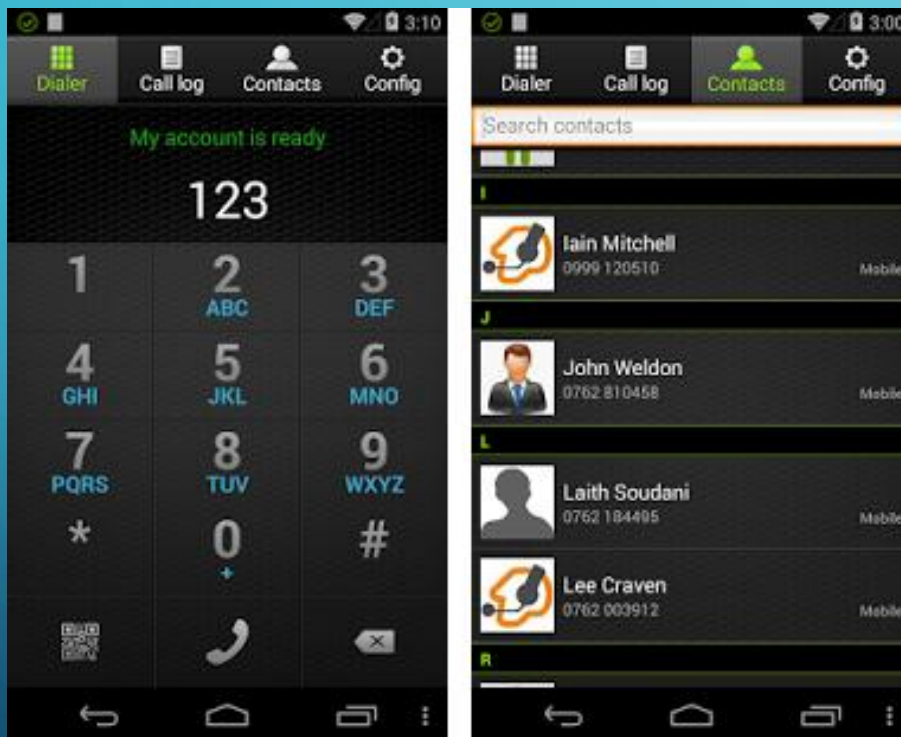
ระบบสื่อสารโทรศัพท์ ANALOG PABX



ระบบสื่อสารโทรศัพท์ DIGITAL VOIP



ระบบสื่อสารโทรศัพท์ ASTERISK VOIP



ข้อดีระบบสื่อสารโทรศัพท์ ASTERISK VOIP

- ลดค่าใช้จ่าย
- เพิ่มความยืดหยุ่นในการติดต่อสื่อสาร
- จัดการระบบเครือข่ายได้ง่าย
- รองรับการใช้งานในอนาคต

- ลดค่าใช้จ่ายในการดูแลและจัดการระบบ
- เพิ่มประสิทธิภาพการทำงาน
- ใช้ร่วมกับอุปกรณ์ไร้สายได้
- เพิ่มประสิทธิภาพในการติดต่อกับลูกค้า

ข้อดีระบบสื่อสารโทรศัพท์ ASTERISK VOIP

- 1.ลดค่าใช้จ่าย
- 2.เพิ่มความยืดหยุ่นในการติดต่อสื่อสาร
- 3.จัดการระบบเครือข่ายได้ง่าย
- 4.รองรับการขยายตัวในอนาคต
- 5.ลดค่าใช้จ่ายในการดูแลและจัดการระบบ
- 6.เพิ่มประสิทธิภาพการทำงาน
- 7.ใช้ร่วมกับอุปกรณ์ไร้สายได้
- 8.เพิ่มประสิทธิภาพในการติดต่อสื่อสาร