มาตรการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

สถาบันวิจัยพฤติกรรมศาสตร์

เพื่อให้ระบบเทคโนโลยีของสถาบันวิจัยพฤติกรรมศาสตร์ หรือต่อไปนี้เรียกว่า หน่วยงาน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ หน่วยงานจึงกำหนดมาตรการรักษาความปลอดภัยของของระบบเทคโนโลยีสารสนเทศ โดยกำหนดแนวปฏิบัติให้ครอบคลุมการรักษาความลับ ความถูกต้องครบถ้วน ความปลอดภัยของระบบเทคโนโลยีสนเทศ และป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังนี้

1. จัดทำมาตรการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของหน่วยงาน ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ

2. เพื่อเป็นกรอบและแนวปฏิบัติในขั้นตอนการปฏิบัติงาน ผู้รับผิดชอบ รวมถึงสิ่งอำนวยความสะดวกดานคอมพิวเตอร์สำหรับติดตั้งและใช้งานระบบเพื่อการรักษาความมั่นคงปลอดภัยของสารสนเทศ

3. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของสารสนเทศอย่างสม่ำเสมอ

4. เพื่อเผยแพร่แก่บุคลากรของหน่วยงาน เพื่อสร้างความเข้าใจให้เกิดความตระหนักและมีส่วร่วมรับผิดชอบในการรักษาความมั่นึงปลอดภัยของสารสนเทศ

มาตรการนี้จัดทำขึ้นโดยอาศัยแนวทางนโยบายความมั่นปลอดภัยของสารสนเทศ มหาวิทยาลัยศรีนครินทรวิโรฒ พ.ศ. 2557 ที่จัดทำขึ้นโดยใช้แนวทางของ ISO/IEC27001 (https://secure.swu.ac.th/Default.aspx?tabid=7257) สถาบันฯ ได้นำแนวทางดังกล่าวมาปรับให้ สอดคล้องกับการบริหารจัดการและบริบทของหน่วยงาน อีกทั้งบุคลากรของหน่วยงานและผู้มีส่วนได้เสียจะต้องปฏิบัติตาม โดยมีรายละเอียดและแนวปฏิบัติ ดังต่อไปนี้ https://secure.swu.ac.th/Default.aspx?tabid=7257

1. ภาระความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

1) ผู้บริหาร กำกับดูแลให้นิสิตและบุคลากรได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ และปฏิบัติบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย ในวันปฐมนิเทศหรือวันก่อนเปิดภาคเรียนให้ผู้บริหารชี้แจงให้นิสิตทราบถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ และปฏิบัติบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย
2) นิสิตและบุคลากร ทุกคนรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัยและต้องแจ้งต่อมหาวิทยาลัยหรือหน่วยงาน หากพบปัญหาหรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ สำหรับบุคลากรที่สิ้นสุดการจ้าง ต้องมีการคืนสินทรัพย์ของสถาบันฯและมหาวิทยาลัย และถอนสิทธิในการเข้าถึงระบบสารสนเทศของบุคคลนั้น

3) ผู้พัฒนาและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศทุกระบบของสถาบันฯ ต้องตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ โดยมาตรการด้านความมั่นคงปลอดภัยของระบบต้องผ่านการพิจารณาและได้รับความเห็นชอบจากผู้บริหาร (เทคโนโลยีสารสนเทศระดับสูง)
4) บุคคลภายนอก หรือ ผู้มีส่วนได้เสีย ที่สถาบันฯ ขออนุญาตไปยังสำนักคอมพิวเตอร์และอนุญาตให้มีสิทธิ์ในการเข้าถึง หรือใช้ข้อมูลหรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของมหาวิทยาลัย กำหนดระยะเวลาการใช้งาน และต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย ใช้งานตามสิทธิที่ได้รับอนุญาต และต้องรับผิดชอบในการไม่เปิดเผยความลับของมหาวิทยาลัยโดยมิได้รับอนุญาต

2. การป้องกันการจารกรรมข้อมูลจากภายนอก

1) บัวศรีไอดีและรหัสผ่านของบุคลากรของสถาบันฯ และบุคคลภายนอก จัดเก็บรหัสผ่านไว้เป็นความลับ ห้ามเปิดเผยให้บุคคลอื่นรับรู้ เพื่อป้องกันการนำไปใช้เพื่อการที่จะทำให้เกิดความเสียหายต่อสถาบันฯ และมหาวิทยาลัย
2) การตั้งรหัสผ่านของแต่ละ Account และของแต่ละโปรแกรม ควรตั้งให้คาดเดายาก เช่น มีอักขระพิเศษ ไม่เป็นชื่อบัญชี มีตัวเลข ตัวอักษรเล็ก ใหญ่ ผสมอยู่ในกลุ่มรหัสผ่าน
3) เครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์แบบพกพาควรกำหนดรหัสผ่านทุกเครื่อง
4) อุปกรณ์คอมพิวเตอร์และโสตทัศนูปกรณ์ในห้องเรียน ห้องประชุม กำหนดให้มีผู้รับผิดชอบโดยตรง และจัดทำตารางการตรวจสอบพร้อมรายงานการตรวจสอบต่อผู้บังคับบัญชาทราบ
5) การเดินสายแลนเพื่อเชื่อมต่อระหว่างอุปกรณ์ต้องมีป้ายเพื่อบ่งบอกถึงตำแหน่งในการเชื่อมต่อกับอุปกรณ์

3. การใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของหน่วยงาน

1) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องตรวจสอบไวรัสก่อนใช้งาน
2) งดใช้โปรแกรมเถื่อน เพื่อป้องกันการเปิดช่องให้ผู้ไม่ประสงค์ดีเข้ามาทำลายระบบเทคโนโลยีสารสนเทศ

1) ติดตั้งและอัพเดทซอฟต์แวร์เพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี
2) Update ระบบปฏิบัติการให้มีความทันสมัยอยู่เสมอ
3) ใช้ web browser ที่น่าชื่อถือและอัพเดท web browser นั้น บ่อย ๆ
4) ไม่เข้าเว็บที่มีความน่าสงสัย เว็บที่ไม่ปลอดภัยหากเราส่งข้อมูลได้ยังเว็บดังกล่าวอาจถูกดักจับข้อมูลหรือขโมยข้อมูลได้ ดูยังไงว่าเว็บปลอม

4.1 ตรวจสอบ Domain name สังเกตุบริเวณมุมซ้ายบนของ browser ช่อง address bar ว่ามีรูปกุญแจสีเขียวหรือไม่ หากมีรูปกุญแจปรากฏถือว่ามีความปลอดภัย

ข้อมูลที่ถูกส่งไปจะไม่ถูกดักจับหรือเข้ารหัสกลางทาง ส่วนไอคอนเครื่องหมายตัว I (ไอ) การส่งข้อมูลผ่านเว็บไซต์นี้จะไม่มีความเป็นส่วนตัวอาจจะถูกดักจับข้อมูลได้ ห้ามป้อนข้อมูลส่วนตัวผ่านเว็บนี้ ส่วนเว็บที่เป็นไอคอนเครื่องหมายตกใจสีแดง เป็นเว็บที่ไม่มีความปลอดภัยเลยไม่ควรเข้าเว็บไซต์ดังกล่าว

4.1.1 URL ขยายเว็บที่ถูกย่อ URL ไว้แล้ว พิจารณาความน่าเชื่อถือต่อไป www.checkshorturl.com

4.1.2 ตรวจสอบ URL ของเว็บว่ามีความปลอดภัยหรือไม่ จาก scamadviser.com หรือ เว็บอื่น ที่น่าเชื่อถือ

4.2 ตรวจการอนุญาตการเข้าถึงกล้อง ไมโครโฟน หรือที่ตั้ง ของ web browser ของแต่ละเว็บหรือโปรแกรมที่เรียกใช้ผ่าน web browser นั้น หากอนุญาตให้เข้าถึงอุปกรณ์ ให้พิจารณาถึงความน่าเชื่อถือของโปรแกรมหรือเว็บนั้น หากพบว่า เป็นโปรแกรมหรือเว็บที่ไม่น่าเชื่อถือให้ปิดการอนุญาตการเข้าถึง

4.3 ให้เตือนตัวเองเสมอว่า “ของฟรีไม่มีในโลก” หากต้องการสิ่งนั้นจริง ๆ ให้ค้นหาข้อมูลจากกเว็บอื่น ๆ อีกหลาย ๆ แหล่ง

5) จำกัดสิทธิ์การเข้าถึงเฉพาะผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศนั้น ๆ เท่านั้น
6) เครื่อง server bsris.swu.ac.th ต้องเปลี่ยนรหัสผ่านทุกเดือน
7) เมื่อไม่ใช้งานเครื่องคอมพิวเตอร์แล้ว ต้องลงชื่อออกทุกครั้ง
8) กำหนดให้ระบบสารสนเทศระงับการใช้งานเมื่อไม่มีปฏิสัมพันธ์กับระบบนานเกิน 10 นาที
9) ห้ามให้โปรแกรมประยุกต์ที่ต้องมีชื่อผู้ใช้และรหัสผ่านที่เข้าใช้งานบันทึกรหัสผ่านและลงชื่อเข้าใช้แบบอัตโนมัติ
10) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน ให้ทำการเปลี่ยนรหัสผ่านในทันทีหลังจากใช้งานเสร็จ
11) บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิของผู้ใช้งานระบบสารสนเทศ
12) การยืมครุภัณฑ์ที่เป็นทรัพย์สินของสถาบันฯ ให้ดำเนินการตาม “แนวทางปฏิบัติเกี่ยวกับการใช้ทรัพย์สินของสถาบันวิจัยพฤติกรรมศาสตร์” ดำเนินการโดย งานพัสดุ สำนักงานผู้อำนวยการสถาบันพฤติกรรมศาสตร์ ที่ต้องกรอกแบบฟอร์มการยืมพัสดุ และนักวิชาการพัสดุลงทะเบียนคุมการยืมคืนดังกล่าว

4. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1) การจัดวางอุปกรณ์กระจายสัญญาณในที่เหมาะสม เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าใช้ระบบ
2) เลือกใช้ผู้ให้บริการเครือข่ายอินเทอร์เน็ตแบบไร้สายที่มีความน่าเชื่อถือ หรืออุปกรณ์ที่มหาวิทยาลัยจัดหาให้

5. การสำรองข้อมูล

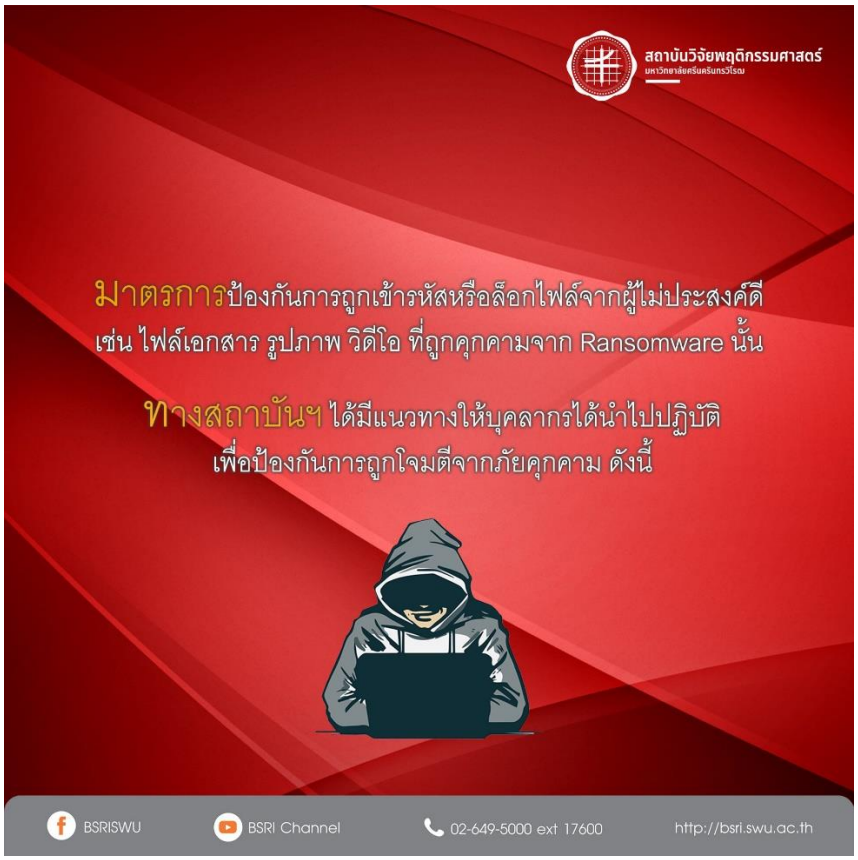
1) จัดทำบัญชีระบบสารสนเทศ ข้อมูล ไฟล์
2) ระบบสารสนเทศต้องสำรองข้อมูลทุกวัน ๆ ละ ครั้ง พร้อมบันทึก วันเวลาชื่อข้อมูลที่สำรอง
3) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ กรณีเกิดความเสียหายกับอุปกรณ์สำหรองหลัก
4) ทบทวนเพื่อปรับปรุงแผนให้สอดคล้องกับภาระกิจอย่างน้อยปีละ 1 ครั้ง

6. ประเมินความเสี่ยงด้านสารสนเทศ

จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย เพื่อตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ และจัดทำแนวทางในการตรวจสอบและประเมินความเสี่ยง

รายงานผลการดำเนินงานตามมาตรการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ดังนี้

1. การป้องกันการถูกคุกคามจาก Ransomeware โดยออกเป็น infographic เพื่อสื่อสารให้บุคลากรสถาบันฯ ได้เข้าใจมากขึ้น และเผยแพร่บน Line Group ของบุคลากรสถาบันฯ และ บน Facebook ของสถาบันฯ



สถาบันวิจัยพฤติกรรมศาสตร์
มหาวิทยาลัยศรีนครินทรวิโรฒ

1) สำรองไฟล์ ที่เป็นเอกสาร รูปภาพ วิดีโอ รวมไปถึงข้อมูลที่เกี่ยวข้องกับงานวิจัย ไว้หลายแหล่ง
เช่น Cloud Storage (Google Drive(@g.swu.ac.th)
One Drive(@m.swu.ac.th) หรือ Dropbox เป็นต้น

OneDrive
Dropbox

2) หลีกเลี่ยงหรืองดใช้ Thumb Drive

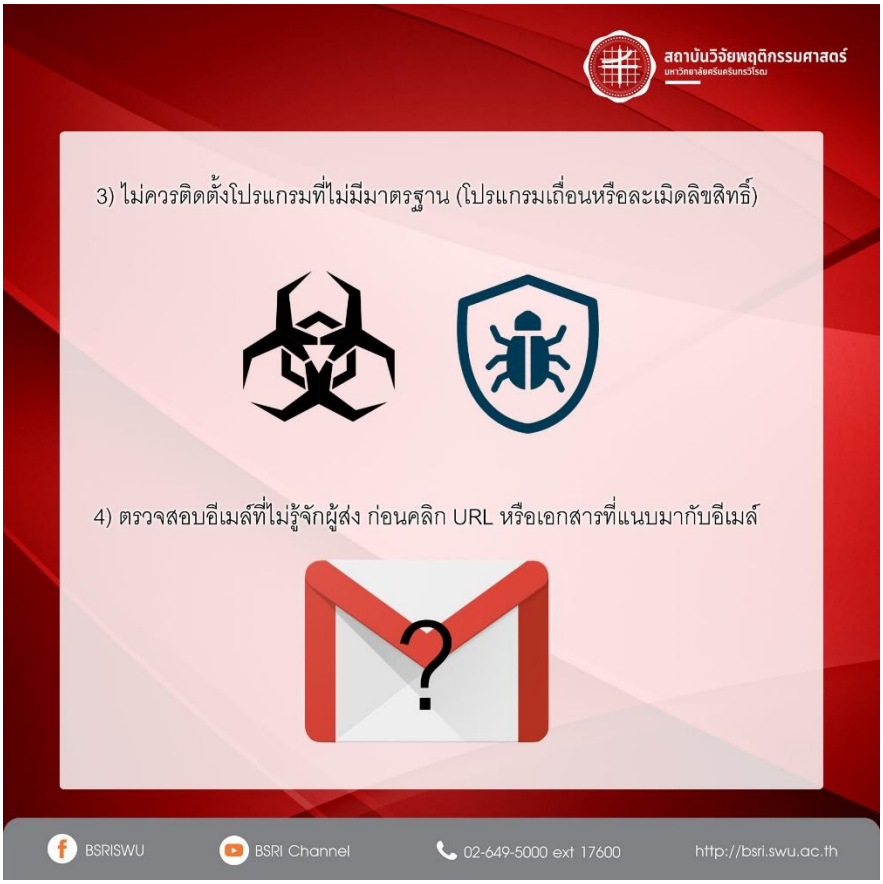
สถาบันวิจัยพฤติกรรมศาสตร์
มหาวิทยาลัยศรีนครินทรวิโรฒ

5) ไม่เข้าเว็บที่มีลักษณะสุ่มเสี่ยงหรือมีการโฆษณาแฝง เช่น เว็บการพนัน เว็บโป๊
หรือ URL ของการทำโปรโมชั่นสินค้าและบริการ (ลด แลก แจก แถม)

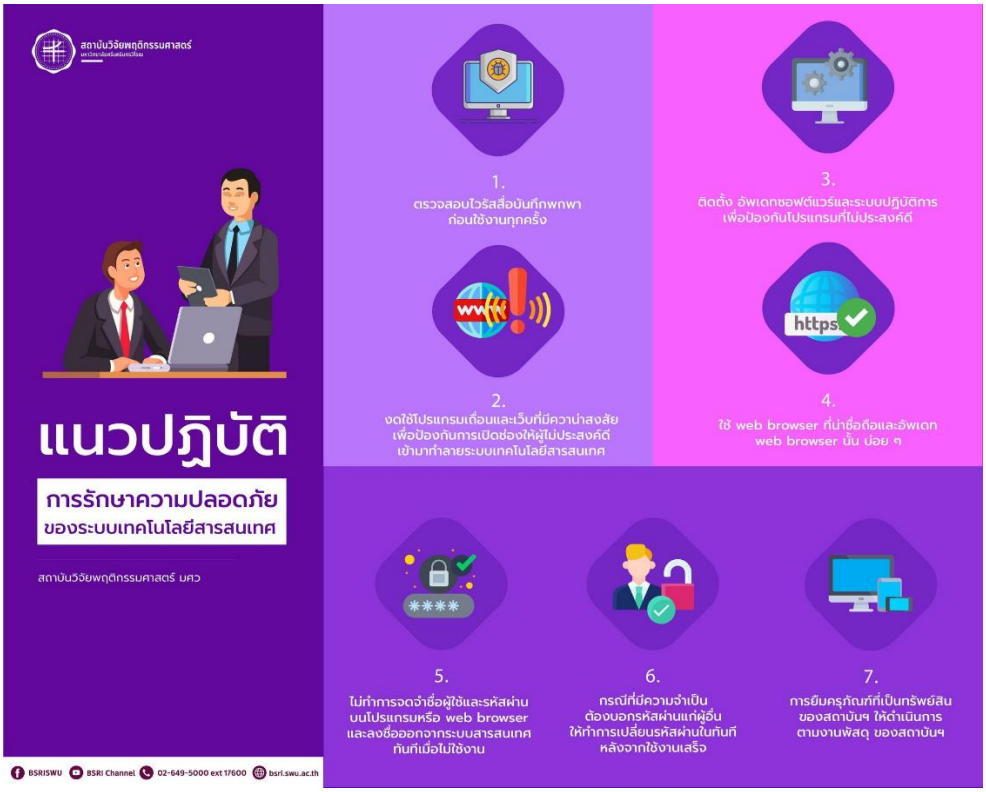
6) อัพเดทซอฟท์แวร์ในเครื่องอย่างสม่ำเสมอจะช่วยป้องกันการโจมตีที่ต้องอาศัยช่องโหว่ของซอฟต์แวร์ได้
โดยมหาวิทยาลัยได้ให้บริการระบบป้องกันไวรัส Sophos Virus Protection
โดยสามารถดาวน์โหลดเพื่อทำการติดตั้งได้ที่

http://cc.swu.ac.th/Default.aspx?tabid=19318

BSRISWU BSRI Channel 02-649-5000 ext 17600 http://bsri.swu.ac.th



2. การทำป้ายประชาสัมพันธ์แนวปฏิบัติการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศเบื้องต้นให้กับผู้ใช้งานหรือบุคลากรสถาบันฯ ไว้เป็นแนวทางการป้องกันภัยคุกคามการใช้งานบนอินเทอร์เน็ต



3. การยืมครุภัณฑ์ที่เป็นทรัพย์สินของสถาบันฯ ให้ดำเนินการตาม “แนวทางปฏิบัติเกี่ยวกับการใช้ทรัพย์สินของสถาบันวิจัยพฤติกรรมศาสตร์” ดำเนินการโดย งานพัสดุ สำนักงานผู้อำนวยการสถาบันพฤติกรรมศาสตร์ ที่ต้องกรอกแบบฟอร์มการยืมพัสดุ และนักวิชาการพัสดุลงทะเบียนคุมการยืมคืนดังกล่าว (แนบแนวปฏิบัติ)

4. จัดทำบัญชีประวัติผู้มีสิทธิ์ใช้งานระบบสารสนเทศพร้อมสถานะการใช้

งาน	ชื่อระบบ	บุคลากร	สถานะการใช้
บริการการศึกษา	Supreme.swu.ac.th	นางสาวพิจิตรา ธรรมสถิตย์	
		นางกรรณิการ์ ศรีเกตุ	
		คณาจารย์	
	Admission.swu.ac.th	นางสาวพิจิตรา ธรรมสถิตย์	
		นางกรรณิการ์ ศรีเกตุ	
	BP-ข้อมูลผู้ค้า	นางสาวพิจิตรา ธรรมสถิตย์	
บุคลากร	Huris.swu.ac.th	นางสุพิมพ์ชนก กิจสำเร็จ	
		นางสาววาสนา วงษ์เพชร	
	SWU-ERP	นางสุพิมพ์ชนก กิจสำเร็จ	
การเงิน	SWU-ERP	ผอ.สถาบันฯ	อนุมัติ, ดูรายงาน
		ผอ.สนง.สถาบันฯ	อนุมัติ, ดูรายงาน
		น.ส.สุภชาดา รัตนพิมล	การเบิกเงินงบประมาณ
		น.ส.แสงระวี ไทยแย้ม	เงินเดือน
		นางสุพิมพ์ชนก กิจสำเร็จ	บุคคล
		นางกรรณิกา ทัศนสุวรรณ	พัสดุ
ธุรการ	Saraban.swu.ac.th	นายอัครพล เลิศจุฬาลักษณ์	ระบบสารบรรณ
		น.ส.วาสนา วงษ์เพชร	ระบบสารบรรณ
		น.ส.จุฑารัตน์ กิตติเขมากร	
	e-document	นายอัครพล เลิศจุฬาลักษณ์	คำสั่ง
		น.ส.วาสนา วงษ์เพชร	คำสั่ง
		นางสุพิมพ์ชนก กิจสำเร็จ	คำสั่ง
	e-tran	น.ส.วาสนา วงษ์เพชร	จองรถมหาวิทยาลัย