บันทึกข้อความ

ส่วนงาน สำนักบริการเทคโนโลยีสารสนเทศ (สำนักงานสำนัก โทร. 43822)
ที่ อว 8394(2)/14 **วันที่** 8 มกราคม 2569
เรื่อง แนวทางการบริหารจัดการการเปลี่ยนแปลง (Change Management) สำหรับระบบเทคโนโลยีสารสนเทศ และแนวทางการบริหารจัดการผู้ให้บริการภายนอกด้านระบบเทคโนโลยีสารสนเทศ (IT Outsource Management Procedure)

เรียน คณบดี/ ผู้อำนวยการ/ หัวหน้าส่วนงาน

ตามที่สำนักบริการเทคโนโลยีสารสนเทศ ได้เสนอเรื่อง การบริหารจัดการการเปลี่ยนแปลง (Change Management) สำหรับระบบเทคโนโลยีสารสนเทศสำหรับส่วนงานในมหาวิทยาลัยเชียงใหม่ และแนวทางการบริหารจัดการผู้ให้บริการภายนอกด้านระบบเทคโนโลยีสารสนเทศ (IT Outsource Management Procedure) ในที่ประชุมคณะกรรมการบริหารมหาวิทยาลัย (กบม.) ให้ที่ประชุมพิจารณา ในคราวประชุมครั้งที่ ครั้งที่ 19/2568 เมื่อวันที่ 24 ธันวาคม 2568 โดยที่ประชุมพิจารณาแล้วมีมติเห็นชอบแนวทางดังกล่าว นั้น

ในการนี้ เพื่อเป็นแนวทางในการดำเนินการด้านการบริหารจัดการการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศของส่วนงานให้มีความมั่นคงปลอดภัย ป้องกันการแก้ไขโดยไม่ได้รับอนุญาต และลดผลกระทบต่อผู้ใช้งานหรือส่วนงาน รวมถึงการกำกับดูแลผู้ให้บริการภายนอกให้เป็นไปอย่างมีประสิทธิภาพ ครบถ้วนตามข้อกำหนดและระเบียบที่เกี่ยวข้อง เพื่อยกระดับการรักษาความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องกับนโยบายของมหาวิทยาลัย สำนักบริการเทคโนโลยีสารสนเทศ จึงขอนำส่งแนวทางการบริหารจัดการการเปลี่ยนแปลง (Change Management) และแนวทางการบริหารจัดการผู้ให้บริการภายนอกด้านระบบเทคโนโลยีสารสนเทศ (IT Outsource Management Procedure) มาเพื่อโปรดพิจารณาดำเนินการ โดยมีรายละเอียดดังเอกสารแนบมาพร้อมนี้ หากมีข้อสงสัยสามารถติดต่อสอบถามได้ที่เบอร์โทร 053-943822

จึงเรียนมาเพื่อโปรดทราบและโปรดพิจารณาดำเนินการต่อไปด้วย จักขอบคุณยิ่ง

(รองศาสตราจารย์ ดร.จักรพงศ์ นาทวิชัย)
ผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศ

แนวทางการบริหารจัดการการเปลี่ยนแปลง (Change Management)
สำหรับระบบเทคโนโลยีสารสนเทศสำหรับส่วนงานในมหาวิทยาลัยเชียงใหม่

1. หลักการและเหตุผล

การเปลี่ยนแปลงทางด้านระบบเทคโนโลยีสารสนเทศของส่วนงานภายในมหาวิทยาลัยเชียงใหม่มีความสำคัญอย่างยิ่ง หากขาดหลักเกณฑ์หรือมาตรฐานการปฏิบัติงานที่เหมาะสม อาจก่อให้เกิดความเสี่ยงจากการปรับเปลี่ยนโดยไม่ได้รับอนุญาต (Unauthorized Change) ซึ่งส่งผลกระทบต่อการให้บริการของส่วนงานทั้งในด้านการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) หรือเรียกโดยรวมว่า CIA รวมไปถึงการคุ้มครองข้อมูลส่วนบุคคล (Personal Identifiable Information หรือ PII) ดังนั้น จึงจำเป็นต้องกำหนดแนวทางการบริหารจัดการการเปลี่ยนแปลง (Change Management) เพื่อใช้เป็นแนวทางในการดำเนินการและเพื่อให้สอดคล้องกับประกาศมหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567 และมาตรฐานสากล ISO/IEC 27001 รวมไปถึง ISO/IEC 27701

2. วัตถุประสงค์

1) เพื่อกำหนดขั้นตอนมาตรฐานในการปรับเปลี่ยนระบบเทคโนโลยีสารสนเทศ ให้มีการควบคุมที่เหมาะสม ลดความผิดพลาดของการดำเนินการ และป้องกันการปรับเปลี่ยนโดยไม่ได้รับอนุญาต
2) เพื่อลดผลกระทบหรือข้อขัดแย้งที่อาจเกิดขึ้นกับหน่วยงานอื่นโดยไม่ตั้งใจจากการปรับเปลี่ยนระบบเทคโนโลยีสารสนเทศ

3. ขอบเขต

ครอบคลุมระบบงานด้านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ และระบบสารสนเทศทั้งหมดของส่วนงานภายในมหาวิทยาลัยเชียงใหม่

4. ประเภทของการเปลี่ยนแปลง

แบ่งการดำเนินงานออกเป็น 3 รูปแบบ ตามระดับผลกระทบ ดังนี้

4.1 การเปลี่ยนแปลงแบบเล็กน้อยที่ไม่มีผลกระทบอย่างมีนัยสำคัญ (Minor Change)

เป็นการพัฒนาหรือปรับเปลี่ยนที่อยู่ภายใต้ความรับผิดชอบของงานนั้น ๆ โดยอยู่ในการกำกับดูแลของหัวหน้างาน และมีการปรับเปลี่ยนแบบเล็กน้อยและไม่มีผลกระทบที่เป็นนัยสำคัญ ผู้รับผิดชอบต้องบันทึกรายละเอียดการเปลี่ยนแปลงตามแบบฟอร์มที่ส่วนงานกำหนด เพื่อให้สามารถติดตามตรวจสอบการแก้ไขระบบสารสนเทศได้ในภายหลัง

4.2 การเปลี่ยนแปลงแบบปกติที่มีผลกระทบอย่างมีนัยสำคัญ (Normal/Major Change)

เป็นการพัฒนาหรือปรับเปลี่ยนที่มีผลกระทบที่มีนัยสำคัญต่อการทำงานของระบบเทคโนโลยีสารสนเทศที่ใช้งานจริง เช่น โครงการจัดซื้อจัดจ้างประจำปี ระบบที่กระทบผู้ใช้งานจำนวนมาก การเปลี่ยนแปลงที่เสี่ยงต่อการหยุดชะงักของการให้บริการ การเปลี่ยนแปลงที่มีความเสี่ยงสูงและไม่เคยปฏิบัติมาก่อนหรือไม่มีคู่มือการปฏิบัติ หรือระบบที่พัฒนาขึ้นใหม่ การดำเนินงานต้องอยู่ภายใต้การกำกับดูแลของผู้บริหารส่วนงาน และต้องได้รับอนุมัติการเปลี่ยนแปลงก่อนดำเนินการ ผู้รับผิดชอบต้องบันทึกการเปลี่ยนแปลงตามแบบฟอร์มที่ส่วนงานกำหนด เพื่อให้สามารถติดตามตรวจสอบการแก้ไขระบบสารสนเทศได้ในภายหลัง

4.3 การเปลี่ยนแปลงเร่งด่วน (Emergency Change)

กรณีระบบเกิดปัญหาและจำเป็นต้องมีการแก้ไขอย่างเร่งด่วน หัวหน้างานที่รับผิดชอบจะต้องรายงานให้ผู้บริหารส่วนงานทราบทันที ผู้รับผิดชอบต้องบันทึกการเปลี่ยนแปลงในแบบฟอร์มโดยทันทีภายหลังจากที่ได้ดำเนินการแก้ไขเสร็จสิ้น พร้อมสรุปรายงานการติดตามการแก้ไขระบบสารสนเทศให้กับผู้บริหารส่วนงานทราบเป็นประจำทุกเดือน

5. ขั้นตอนการปฏิบัติสำหรับการเปลี่ยนแปลงแบบปกติ (Normal/Major Change)

5.1. การร้องขอ (Request)

- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศ ผู้ขอจะต้องจัดทำหรือกรอกแบบฟอร์มตามที่ส่วนงานกำหนด หรือแจ้งผ่านช่องทาง E-mail หรือ บันทึกข้อความนำเสนอหัวหน้างานของตนเองพิจารณาอนุมัติ โดยมีรายละเอียดอย่างน้อย ได้แก่
  - หมายเลขระบุการเปลี่ยนแปลง (Change Identifier) ผู้ร้องขอ/ผู้ดำเนินการ/ผู้อนุมัติ
  - รายละเอียดสิ่งที่จะเปลี่ยนแปลงและเหตุผล
  - การประเมินผลกระทบ/ความเสี่ยง อย่างน้อยในประเด็น CIA และโอกาสการรั่วไหลของ PII
  - แผนทดสอบก่อนใช้งานจริง และผลทดสอบ
  - แผนย้อนกลับ (Rollback) ที่ทำได้จริง
  - แผนสื่อสารการเปลี่ยนแปลง ทั้งกับผู้รับบริการและผู้มีส่วนได้ส่วนเสีย
- หัวหน้างานของผู้ร้องขอ นำเสนอการร้องขอดังกล่าวให้ต่อผู้บริหารส่วนงานหรือคณะกรรมการบริหารประจำส่วนงาน (CAB- Change Advisory Board) เพื่อขออนุมัติให้ดำเนินการ โดยต้องมีการพิจารณาเรื่องผลกระทบที่อาจจะเกิดขึ้นในทุกด้านที่เกี่ยวข้อง เช่น ระบบงานที่เกี่ยวข้อง กระบวนการทำงานที่เกี่ยวข้อง ความมั่นคงปลอดภัย กฎหมายหรือกฎระเบียบที่เกี่ยวข้อง เป็นต้น
- ในกรณีของระบบสารสนเทศ ให้มีการกำหนดบทบาทของผู้ที่เกี่ยวข้องอย่างชัดเจน ได้แก่ เจ้าของกระบวนการ (Process Owner) ซึ่งมักเป็นผู้ดูแลเนื้องานและกระบวนการของระบบดังกล่าว, ผู้อนุมัติการแก้ไข (Approver) ที่ควรเป็นผู้บริหารระดับสูงของส่วนงาน, ผู้ดำเนินการ (Implementor) ผู้พัฒนาระบบสารสนเทศของส่วนงาน, และผู้ทบทวนด้านความมั่นคงปลอดภัยไซเบอร์และ/หรือการคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจใช้บริการของสำนักบริการเทคโนโลยีสารสนเทศได้
- โดยในการเสนอร้องขอเพื่ออนุมัติการเปลี่ยนแปลง ต้องมีการกำหนดขอบเขตการเปลี่ยนแปลงที่ชัดเจน เช่น โค้ด/โปรแกรมประยุกต์ โครงสร้างพื้นฐาน สิทธิในการเข้าถึงการเปลี่ยนแปลงผู้ให้บริการ การให้บริการ กระบวนการ และนโยบายที่จะกระทบ เพื่อให้ผู้อนุมัติมีข้อมูลที่เพียงพอในการพิจารณา
- นอกจากนั้น ส่วนงานอาจพิจารณาประเภทของการเปลี่ยนแปลงเพื่อให้สามารถดำเนินการได้อย่างมีประสิทธิผล เช่น
  - การเปลี่ยนแปลงตามมาตรฐาน (Standard Change) ซึ่งมักเปลี่ยนแปลงซ้ำๆ เดิม มีวิธีการดำเนินการที่ควบคุมได้ มีความเสี่ยงต่ำ เช่น การ Update patch รายเดือน การเปลี่ยนแปลงชนิดดังกล่าว หากสามารถวางแผนล่วงหน้าได้และต้องทำต่อเนื่อง สามารถขออนุมัติเป็นชุดได้

- การเปลี่ยนแปลงตามปกติ (Normal Change) ซึ่งอาจเกิดจากการแก้ไขข้อผิดพลาด หรืออาจมีความเสี่ยง ต้องมีการประเมินความเสี่ยง และขออนุมัติรายครั้ง
- การเปลี่ยนแปลงฉุกเฉิน (Emergency Change) เป็นการดำเนินการเพื่อแก้ไขเหตุฉุกเฉิน ซึ่งอาจกระทบกับบริการในวงกว้าง หรือมีผลกระทบสูง ซึ่งอาจพิจารณากระบวนการการอนุมัติที่รวดเร็วกว่าปกติ แต่ต้องมีการทบทวน (Review) การเปลี่ยนแปลงย้อนหลังเมื่อดำเนินการแล้วเสร็จ

5.2. การพัฒนาระบบ (Development)

- การพัฒนาหรือแก้ไขระบบสารสนเทศต้องแยกสภาพแวดล้อมการพัฒนา (Develop Environment) ออกจากระบบใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้การแบ่งแยกส่วนตามที่กล่าว สามารถแบ่งโดยใช้เครื่องคอมพิวเตอร์ หรือแบ่งแยกฐานข้อมูล หรือตามความเหมาะสมของการพัฒนาหรือเปลี่ยนแปลงนั้น ๆ
- ผู้ที่มีหน้าที่รับผิดชอบในการพัฒนาหรือแก้ไขต้องมีการบันทึกและจัดเก็บข้อมูลทั้งหมดและนำมาจัดทำเป็นรายงานการติดตามการแก้ไขระบบสารสนเทศ หรือสรุปผลการดำเนินการนำเสนอต่อหัวหน้างานและผู้บริหารเป็นประจำทุกเดือน
- ทั้งนี้ หากมีการเปลี่ยนแปลงที่เกี่ยวข้องกับ PII อาจพิจารณาปรับปรุงบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity หรือ RoPA) ด้วย
- ในกรณีที่ว่าจ้างบุคคลภายนอกพัฒนาหรือแก้ไขระบบสารสนเทศ ผู้ที่เกี่ยวข้องต้องปฏิบัติตามในลักษณะเดียวกัน และปฏิบัติตามกฎระเบียบข้อบังคับต่าง ๆ ของมหาวิทยาลัย

5.3. การทดสอบ (Testing)

- ต้องแยกสภาพแวดล้อมการทดสอบ (Test Environment) ออกจากระบบใช้งานจริง และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น
- ผู้พัฒนาต้องมีการทดสอบการใช้งานเบื้องต้นและจัดทำ/จัดเก็บหลักฐานการทดสอบไว้ใช้อ้างอิงในอนาคต เช่น Test Plan, Test Script, Test Result เป็นต้น
- ผู้ที่ร้องขอต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนนำระบบงานขึ้นใช้งานจริง รวมถึงจัดทำ/จัดเก็บหลักฐานการทดสอบไว้ใช้อ้างอิงในอนาคต เช่น Test Plan, Test Script, Test Result, UAT Signoff เป็นต้น
- การทดสอบควรมีการควบคุมการใช้งานข้อมูลจริงที่จะใช้นำมาทำการทดสอบ โดยอย่างน้อยต้องปฏิบัติตามนโยบายและระเบียบปฏิบัติงานในการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

5.4. การนำระบบงานขึ้นใช้งานจริง (Deployment)

- ผู้ที่รับผิดชอบในการพัฒนาหรือดำเนินการแก้ไขต้องขออนุมัติจากหัวหน้างานก่อนนำระบบขึ้นใช้งานจริง
- สำหรับระบบสารสนเทศ อาจแยกบทบาทระหว่างผู้ดำเนินการเปลี่ยนแปลง และผู้นำระบบสู่การใช้งานจริง (Deployment) เพื่อให้เกิดการตรวจสอบมาตรฐานอีกครั้งหนึ่ง

5.5. การจัดทำเอกสาร (Documentation)

- จัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับระบบเทคโนโลยีสารสนเทศที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
- ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน
- ต้องจัดเก็บโปรแกรม version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

5.6. การติดตามและตรวจสอบหลังการใช้งาน (Post-Implementation Review)

- กำหนดให้มีการติดตามระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน
- ต้องมีการดำเนินการตรวจสอบและประเมินช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศก่อนนำมาใช้งาน หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยดำเนินการอย่างน้อยปีละหนึ่งครั้ง สำหรับกรณีที่เป็นระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูง จะต้องมีการทดสอบการเจาะระบบ (Penetration Testing) อย่างเป็นมาตรฐาน เพื่อประเมินความสามารถในการรับมือกับภัยคุกคามจากภายนอก รวมถึงจัดทำแผนการแก้ไขช่องโหว่ภายในระยะเวลาที่กำหนดอย่างเหมาะสม และรายงานผลการดำเนินการให้ผู้บริหารทราบ
- ควรมีการทบทวนการดำเนินงาน สรุปสิ่งที่ได้เรียนรู้ เพื่อให้เกิดผลดำเนินงานที่ดีขึ้นในคราวต่อไป

5.7. การสื่อสาร (Communication)

- ผู้ที่รับผิดชอบต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง
- ผู้ที่รับผิดชอบต้องจัดทำรายงานการติดตามการแก้ไขระบบสารสนเทศ และนำเสนอต่อหัวหน้างานและผู้บริหารของส่วนงานเป็นประจำทุกเดือน

แนวทางการบริหารจัดการผู้ให้บริการภายนอกด้านระบบเทคโนโลยีสารสนเทศ (IT Outsource Management Procedure) สำหรับส่วนงานในมหาวิทยาลัยเชียงใหม่

1. หลักการและเหตุผล

ภารกิจด้านการบริหารจัดการโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ และการพัฒนาระบบสารสนเทศของส่วนงานต่าง ๆ มีความซับซ้อนและต้องการความเชี่ยวชาญเฉพาะด้านสูงขึ้น ส่งผลให้ความต้องการใช้บริการจากผู้ให้บริการภายนอก (Outsourcing) มีการปรับตัวเพิ่มสูงขึ้น ทั้งนี้ เพื่อให้การบริหารจัดการต้นทุนเกิดความคุ้มค่าสูงสุด และเพื่อเพิ่มขีดความสามารถในการปรับตัว ให้การดำเนินงานมีความรวดเร็วและตอบสนองต่อความเปลี่ยนแปลงได้อย่างทันท่วงที

ดังนั้น เพื่อให้การบริหารจัดการการใช้บริการจากบุคคลภายนอกด้านงานเทคโนโลยีสารสนเทศมีประสิทธิภาพ และเกิดประสิทธิผลตามเป้าหมายของมหาวิทยาลัย จึงได้มีการจัดทำแนวทางในการบริหารจัดการผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศขึ้น เพื่อให้ทุกหน่วยงานภายในสามารถนำไปปรับใช้เป็นหลักเกณฑ์ในการกำกับดูแลและควบคุมคุณภาพการให้บริการให้เป็นไปในทิศทางเดียวกัน

2. วัตถุประสงค์

เพื่อเป็นแนวทางหรือขั้นตอนในการปฏิบัติงานเพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากผู้ให้บริการภายนอก ซึ่งอยู่ภายใต้กรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ 3 ประการ ประกอบด้วย การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability) หรือเรียกโดยรวมว่า CIA และรวมไปถึงการคุ้มครองข้อมูลส่วนบุคคล (Personal Identifiable Information หรือ PII)

3. ขั้นตอนการดำเนินการ

3.1 การคัดเลือกผู้ให้บริการภายนอก

การตัดสินใจใช้บริการจากผู้ให้บริการภายนอก (Outsourcing) ต้องสอดคล้องกับกลยุทธ์ของส่วนงาน โดยพิจารณาจากความจำเป็นทางธุรกิจ ประโยชน์ที่คาดว่าจะได้รับ ความคุ้มค่าด้านต้นทุน และความสอดคล้องกับกฎหมายและข้อบังคับที่เกี่ยวข้อง ทั้งนี้ เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพ ให้ส่วนงานระบุรายละเอียดในเอกสารขอบเขตของงาน (Terms of Reference: TOR) ตามกรอบแนวทางดังต่อไปนี้

- **คุณสมบัติของผู้ยื่นข้อเสนอ:** ต้องกำหนดคุณสมบัติให้สอดคล้องกับพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และกฎระเบียบที่เกี่ยวข้อง ได้แก่
    - มีความสามารถตามกฎหมาย
    - ไม่เป็นบุคคลล้มละลาย
    - ไม่อยู่ระหว่างเลิกกิจการ
    - ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอราคารายอื่น
    - ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน
    - ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงาน

- คุณสมบัติเฉพาะด้านอื่น ๆ ที่จำเป็นต่อการดำเนินโครงการ (ถ้ามี) เช่น หลักฐานการได้รับรองมาตรฐานต่าง ๆ ทางด้านความมั่นคงปลอดภัยไซเบอร์ หรือการคุ้มครองข้อมูลส่วนบุคคล

- **ขอบเขตงานและมาตรฐานการให้บริการ**
  - **รายละเอียดขอบเขตงาน:** ระบุขอบเขตงานเทคโนโลยีสารสนเทศที่ต้องการใช้บริการและเงื่อนไขการให้บริการอย่างละเอียด
  - **รายละเอียดด้านเทคโนโลยี:** ให้ส่วนงานระบุเทคโนโลยีที่ต้องการใช้งานอย่างชัดเจน เช่น ในการพัฒนาระบบสารสนเทศ ส่วนงานควรระบุ Technology Stack ที่สามารถดูแลโดยส่วนงานเองได้ในระยะยาว หรืออาจคำนึงถึงเทคโนโลยีที่กำลังใช้งานอยู่ในปัจจุบัน หากเป็นการขยายขอบเขตระบบเพิ่มเติม
  - **เงื่อนไขการส่งมอบและตรวจรับ:** กำหนดงวดงาน การส่งมอบผลงาน และเกณฑ์การตรวจรับที่วัดผลได้
  - **หลักประกันและบทปรับ:** ระบุเงื่อนไขหลักประกันสัญญา การรับประกันความชำรุดบกพร่อง และค่าปรับกรณีผิดสัญญา
  - **ระดับคุณภาพการให้บริการ:** กำหนดมาตรฐานขั้นต่ำที่ต้องการ อาทิ ความพร้อมใช้งานของระบบ (Availability), ความถูกต้องเชื่อถือได้ของข้อมูล (Integrity) และมาตรการรักษาความมั่นคงปลอดภัย (Security)
- **ข้อกำหนดด้านการปฏิบัติงานและความมั่นคงปลอดภัย**: ผู้ให้บริการภายนอกต้องปฏิบัติตามข้อกำหนด ซึ่งต้องมีการแจ้งผู้ให้บริการภายนอกอย่างชัดเจน และบันทึกไว้เป็นลายลักษณ์อักษร ณ การเริ่มปฏิบัติงาน (Onboard) ดังนี้

  การปฏิบัติตามกฎระเบียบ:
  - ปฏิบัติตามประกาศมหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ และ ประกาศเรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด
  - ปฏิบัติตามกฎหมายที่เกี่ยวข้อง เช่น พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายลิขสิทธิ์

  การบริหารจัดการบุคลากรและแผนงาน:
  - จัดส่งแผนการดำเนินงานและขั้นตอนการเข้าปฏิบัติงานที่ชัดเจน
  - ระบุรายชื่อบุคลากรผู้รับผิดชอบ พร้อมรายละเอียดตำแหน่ง หน้าที่ และช่องทางติดต่อ
  - จัดทำรายงานสรุปผลการปฏิบัติงาน และรายงานเหตุการณ์ผิดปกติเป็นลายลักษณ์อักษรตามรอบระยะเวลาที่ตกลงกัน
  - สำหรับการพัฒนาระบบสารสนเทศ ควรมีการตรวจสอบโค้ดให้ถูกต้องและเป็นไปตามมาตรฐาน ในการส่งมอบตามงวดงานทุกครั้ง นอกเหนือจากสิ่งส่งมอบรายชิ้น หรือส่วนงานอาจพิจารณาการตรวจสอบฯ ในรายสปรินต์ (Sprint)

  การควบคุมการเข้าถึงและการจัดการข้อมูล:
  - ปฏิบัติตามมาตรการควบคุมการเข้าพื้นที่และสิทธิการเข้าถึงระบบสารสนเทศ (Access Control) รวมถึงขั้นตอนการขออนุมัติ ปรับปรุง หรือยกเลิกสิทธิ

- ห้ามทำสำเนา แก้ไข หรือทำลายข้อมูลโดยไม่ได้รับอนุญาต
- ลงนามในข้อตกลงรักษาความลับ (NDA) เพื่อป้องกันการเปิดเผยข้อมูลสำคัญหรือข้อมูลความลับทางราชการ
- สำหรับการพัฒนาระบบสารสนเทศ ส่วนงานต้องสามารถเข้าถึงโค้ดระหว่างการพัฒนาในแพลตฟอร์มที่เป็นสากลได้ตลอดเวลาในลักษณะออนไลน์ เพื่อให้สามารถควบคุมและจัดการข้อมูลได้

ทรัพย์สินทางปัญญาและการจัดการหลังสิ้นสุดสัญญา:

- เมื่อสัญญาจ้างสิ้นสุด ผู้ให้บริการต้องดำเนินการคืนทรัพย์สิน ทำลายข้อมูลที่ตกค้าง หรือส่งมอบข้อมูลคืนตามมาตรฐานความปลอดภัยที่กำหนด

ทั้งนี้ ข้อกำหนดของผู้ว่าจ้าง (TOR – Term of reference) ต้องผ่านการพิจารณาของคณะกรรมการร่างขอบเขต TOR และจะต้องทำการตรวจสอบความถูกต้องของเนื้อหา ภาษาที่ใช้ และความหมายต่าง ๆ ที่มีอยู่ใน TOR เพื่อไม่ให้เป็นการขัดกับกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง และต้องเสนอให้ผู้บริหารพิจารณาอนุมัติตามขั้นตอนของกฎระเบียบที่เกี่ยวข้อง

3.2 การจัดทำเอกสารสัญญา

การจัดทำร่างสัญญาจ้างบริการเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก ต้องดำเนินการให้สอดคล้องกับพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และกฎระเบียบที่เกี่ยวข้อง โดยสัญญาดังกล่าวต้องครอบคลุมสาระสำคัญ ดังต่อไปนี้

หลักประกันการปฏิบัติตามสัญญา: กำหนดเงื่อนไขการวางหลักประกัน และการคืนหลักประกันเมื่อผู้รับจ้างพ้นจากข้อผูกพันตามสัญญาแล้ว

ค่าจ้างและการจ่ายเงิน: ระบุจำนวนเงินค่าจ้าง งวดงาน เงื่อนไขการส่งมอบงาน และหลักเกณฑ์การตรวจรับงานให้ชัดเจน

ระยะเวลาและการบอกเลิกสัญญา: กำหนดระยะเวลาการดำเนินงานให้แล้วเสร็จ และระบุสิทธิของส่วนงานในการบอกเลิกสัญญาหากผู้รับจ้างไม่ปฏิบัติตามเงื่อนไขความรับผิดชอบในความชำรุดบกพร่องของงานจ้าง และระยะเวลาในการแก้ไขให้เป็นที่เรียบร้อย

ความรับผิดในความชำรุดบกพร่อง: กำหนดระยะเวลาการรับประกันผลงานและความรับผิดชอบในการแก้ไขความชำรุดบกพร่องที่เกิดขึ้น

การควบคุมและกำกับดูแลงาน: ผู้รับจ้างต้องปฏิบัติงานด้วยความระมัดระวัง มีประสิทธิภาพ และความชำนาญ โดยจัดให้มีตัวแทนผู้ควบคุมงานประจำเต็มเวลา ทั้งนี้ ส่วนงานมีอำนาจในการตรวจสอบ ควบคุม สั่งการแก้ไข เพิ่มเติม หรือตัดทอนเนื้องานตามสัญญาได้

ความรับผิดต่อความเสียหาย: ผู้รับจ้างต้องรับผิดชอบต่ออุบัติเหตุ ความเสียหาย หรืออันตรายใด ๆ ที่เกิดจากการปฏิบัติงานของตนเองหรือลูกจ้างของผู้รับจ้าง

สิทธิในทรัพย์สินทางปัญญา (กรณีงานพัฒนาระบบ/ซอฟต์แวร์): ต้องระบุความเป็นเจ้าของกรรมสิทธิ์ในซอร์สโค้ด (Source Code) คู่มือระบบ และผลงานที่เกี่ยวข้องให้ชัดเจน หากกำหนดให้เป็นสิทธิของส่วนงาน ผู้รับจ้างต้องส่งมอบซอร์สโค้ดฉบับสมบูรณ์ พร้อมรับรองว่าผลงานไม่ละเมิดลิขสิทธิ์ผู้อื่น และยินยอมให้ส่วนงานมีสิทธิในการใช้งาน ดัดแปลง หรือพัฒนาต่อยอดได้โดยไม่จำกัด

Service Level Agreement (SLA): ในด้านความพร้อมใช้ของระบบที่พัฒนา รวมถึงการแก้ไขข้อผิดพลาด (Bug) หรือช่องโหว่ (Vulnerability) ซึ่งรวมไปถึงช่องทางการประสานที่เป็นทางการในกรณีต่าง ๆ

โดยเอกสารสัญญาต่าง ๆ จะต้องผ่านการตรวจสอบความถูกต้องของเนื้อหา ถ้อยคำ และความหมายทางกฎหมาย เพื่อมิให้ขัดต่อระเบียบข้อบังคับที่เกี่ยวข้อง ก่อนนำเสนอผู้บริหารพิจารณาอนุมัติตามขั้นตอนต่อไป