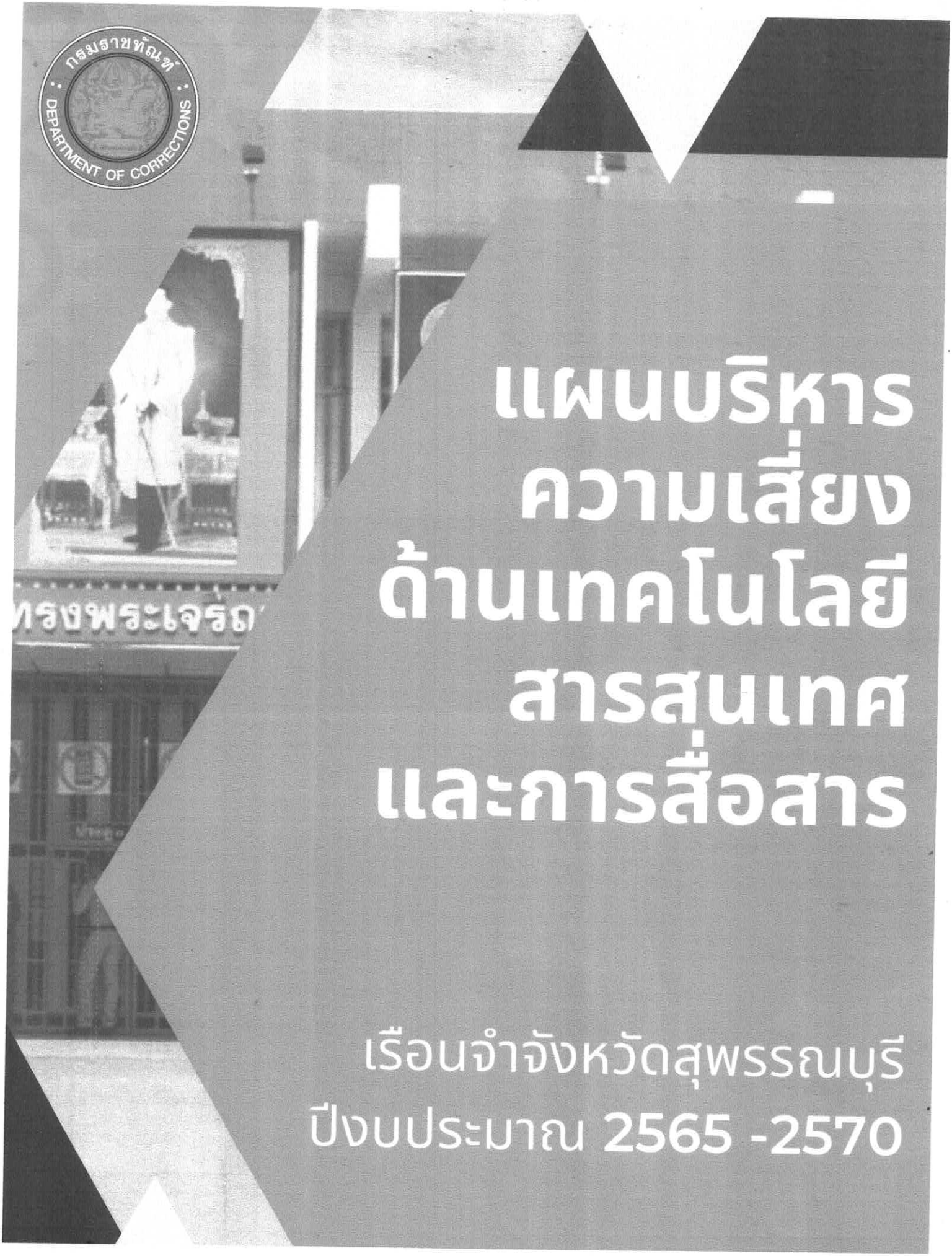


แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

เรือนจำจังหวัดสุพรรณบุรี

ปีงบประมาณ 2565 -2570

คำนำ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของเรือนจำจังหวัดสุพรรณบุรี ปี ๒๕๖๕ – ๒๕๗๐ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุม เพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าหมายขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อมกับองค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการได้อย่างเหมาะสมในการบริหารความเสี่ยงให้อยู่ในระดับที่องค์กรสามารถรองรับได้ และทำให้บรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น

เรือนจำจังหวัดสุพรรณบุรี หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับนี้จะเป็นแนวทางในการลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นอันจะส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของเรือนจำต่อไป

เรือนจำจังหวัดสุพรรณบุรี
พฤศจิกายน ๒๕๖๕

สารบัญ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่าง ๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุก ๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

๑. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของเรือนจำจังหวัดสุพรรณบุรี

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

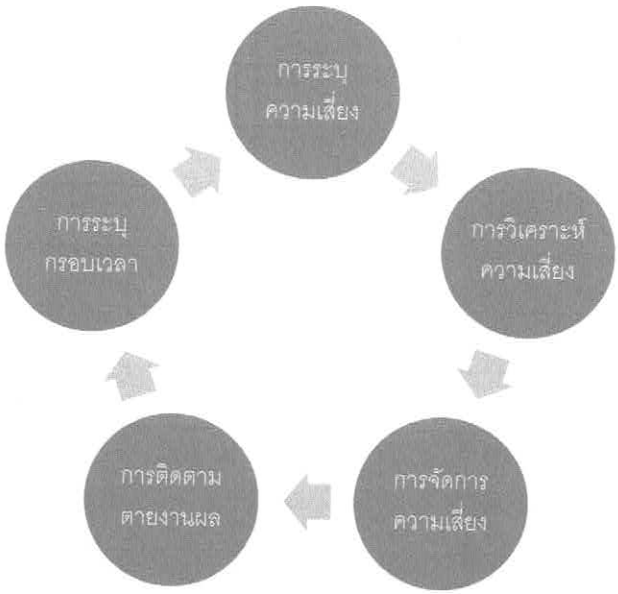
ความหมายของการบริหารความเสี่ยง

๑. ความเสี่ยง (Risk) หมายถึง เหตุการณ์บริการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายของหน่วยงานทั้งในด้านยุทธศาสตร์การปฏิบัติงาน งบประมาณ และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

๒. การบริหารความเสี่ยง หมายถึง การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่าง ๆ โดยลดมูลเหตุแต่ละโอกาสที่จะทำให้เกิดความเสียหายจากการดำเนินงานที่ไม่เป็นไปตามแผน เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ประเมินได้ ควบคุมได้ และตรวจสอบได้ อย่างมีระบบ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายของหน่วยงานเป็นสำคัญ

กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร การบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน (รูปที่ ๑) ดังนี้



รูปที่ ๑ แสดงกระบวนการบริหารความเสี่ยง

๑. การระบุปัจจัยเสี่ยง (Event Identification)

ความเสี่ยงมีสาเหตุจากปัจจัยภายในและปัจจัยภายนอก ปัจจัยเหล่านี้มีผลกระทบต่อวัตถุประสงค์และเป้าหมายของหน่วยงานหรือผลการปฏิบัติงาน ทั้งในระดับหน่วยงานและระดับกิจกรรม ในการระบุปัจจัยเสี่ยงจำเป็นต้องตั้งคำถามว่า “เหตุการณ์ใด” (Event) หรือ “กิจกรรมใด” (Actvities) ของกระบวนการปฏิบัติงาน (Process) ที่อาจเกิดความผิดพลาดเสียหาย และการไม่บรรลุวัตถุประสงค์ (Obiective) ที่กำหนด รวมทั้งมีทรัพย์สินใดที่จะต้องดูแลป้องกันรักษา

๒. การวิเคราะห์ความเสี่ยง (Risk Analysis)

หลังจากระบุปัจจัยเสี่ยงแล้วขั้นตอนต่อไปคือการวิเคราะห์ความเสี่ยง เทคนิคในการวิเคราะห์ความเสี่ยงมีหลายวิธี การวัดความเสี่ยงที่เป็นตัวเลขว่ามีผลกระทบต่อหน่วยงานเท่าไรนั้น เป็นสิ่งที่ทำได้ยากโดยทั่วไปจะวิเคราะห์โดยการประมาณโอกาส (Opportunity/Likeihood) และความถี่ (Frequency) ที่ความเสี่ยงอาจเกิดขึ้นว่ามีมากหรือน้อยเพียงใด เพื่อพิจารณา ผลกระทบ (Impact) จากความเสี่ยงและจัดลำดับความสำคัญ (Category) ของความเสี่ยงที่มีผลต่อหน่วยงาน เรือนจำจังหวัดสุพรรณบุรีได้กำหนดหลักเกณฑ์การประเมินความเสี่ยงและการควบคุมภายในดังนี้

หลักเกณฑ์การประเมินความเสี่ยงและการควบคุมภายใน

หลักเกณฑ์ที่ใช้วัดความเสี่ยง (Risk Measurement) พิจารณาจากเหตุการณ์ (Events) ที่เกิดขึ้นหรืออาจเกิดขึ้นซึ่งมีผลกระทบทำให้ปฏิบัติงานไม่บรรลุวัตถุประสงค์ โดยคำนึงถึงปัจจัยต่าง ๆ ดังนี้

๑. ความเป็นไปได้หรือโอกาสที่จะเกิดเหตุการณ์ต่าง ๆ (Likelihood)

๒. ผลกระทบ/ความรุนแรงของเหตุการณ์ที่เกิดขึ้น (Impact)

๓. ระดับความเสี่ยง (Degree of Risk)

ความหมาย ความเสี่ยงที่เกิดขึ้นเนื่องจากการปฏิบัติงานซึ่งสามารถรวบรวมข้อมูล เพื่อนำมาวิเคราะห์และวัดผลกระทบได้ เป็นตัวเลขที่นับจำนวนได้ในการวัดกำหนดให้เป็นจำนวนจริง

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likelihood) เชิงปริมาณ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	มากกว่า ๑๒ ครั้ง ต่อปี
๔	สูง	๒ – ๑๑ ครั้ง ต่อปี
๓	ปานกลาง	๑ ครั้ง ต่อปี
๒	น้อย	๑ ครั้ง ต่อ ๒ – ๓ ปี
๑	น้อยมาก	๑ ครั้ง ต่อ ๔ – ๕ ปี

ระดับความรุนแรงของผลกระทบต่อความเสี่ยง (Impact) เชิงปริมาณ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	>๑๐ ล้านบาท
๔	สูง	>๒.๕ แสนบาท – ๑๐ บาท
๓	ปานกลาง	>๕๐,๐๐๐ – ๒.๕ แสนบาท
๒	น้อย	>๑๐,๐๐๐ – ๕๐,๐๐๐ บาท
๑	น้อยมาก	ไม่เกิน ๑๐,๐๐๐ บาท

เกณฑ์การวัดความเสี่ยงเชิงคุณภาพ

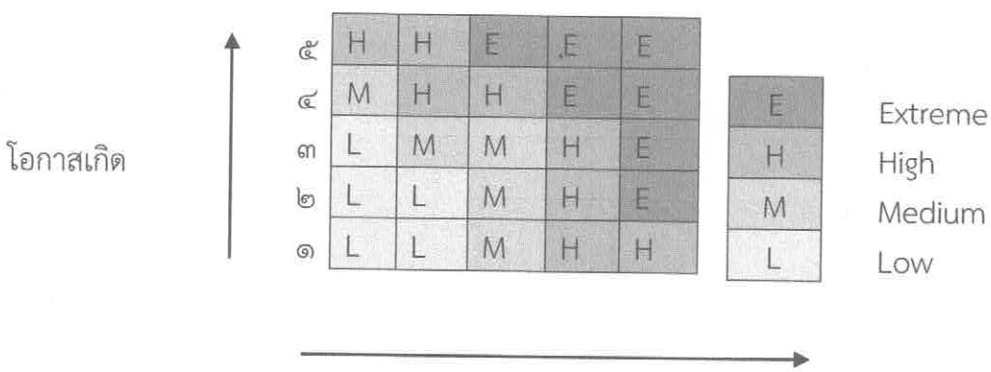
ความหมาย ความเสี่ยงที่เกิดขึ้นเนื่องจากการปฏิบัติงานซึ่งสามารถรวบรวมข้อมูล เพื่อนำมาวิเคราะห์และวัดผลกระทบได้ในเชิงคุณภาพความเสี่ยงบางเรื่องต้องใช้การพิจารณาตัดสินใจโดยผู้เชี่ยวชาญ

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likelihood) เชิงคุณภาพ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
๔	สูง	มีโอกาสในการเกิดค่อนข้างสูง
๓	ปานกลาง	มีโอกาสเกิดบางครั้ง
๒	น้อย	อาจมีโอกาสเกิดแต่นาน ๆ ครั้ง
๑	น้อยมาก	มีโอกาสเกิดในกรณียกเว้น

ระดับความรุนแรงของผลกระทบความเสี่ยง (Impact) เชิงคุณภาพ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	เกิดขึ้นอย่างต่อเนื่องแต่ไม่มีการปรับปรุงแก้ไข
๔	สูง	เกิดขึ้นอย่างต่อเนื่องและมีการปรับปรุงแก้ไขแต่ยังไม่ดีขึ้น
๓	ปานกลาง	เกิดขึ้นเป็นบางครั้งมีการปรับปรุงแก้ไขได้ส่วนใหญ่
๒	น้อย	เกิดขึ้นน้อยและแก้ไขได้เป็นส่วนใหญ่
๑	น้อยมาก	ไม่เกิดขึ้นหรือหากเกิดสามารถแก้ไขได้

เราควรให้ความสำคัญต่อความเสี่ยงที่มีระดับสูงและมีโอกาสเกิดขึ้นสูง แต่อาจลดความสนใจต่อความเสี่ยงที่มีระดับต่ำ และโอกาสที่จะเกิดความเสี่ยงมีน้อย การวิเคราะห์ความเสี่ยงของสองจุดนี้ต้องใช้วิจารณญาณอย่างมากว่าควรอยู่ระดับใด เพราะการวัดผลความเสี่ยงทำได้ยากโดยพิจารณาจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าก่อให้เกิดความเสี่ยงในระดับใด ซึ่งอาจแสดงได้ดังนี้

Risk Model



อาจกล่าวได้ว่าการวิเคราะห์ความเสี่ยงมีหลักในการวิเคราะห์ ๓ ประการ คือ

O โอกาส (Likelihood) หมายถึง โอกาสที่จะเกิดความเสี่ยงมีมากน้อยแค่ไหน มีความถี่อย่างไรมีความถี่หรือโอกาสที่จะเกิดขึ้นทั้งในเชิงปริมาณและเชิงคุณภาพ ซึ่งจะมีความถี่ตั้งแต่น้อยมากจนถึงสูงมากแบ่งเป็น ๕ ระดับ ๑ ๒ ๓ ๔ ๕

O ผลกระทบ (Impact) หมายถึงผลกระทบที่จะเกิดขึ้นหรือความรุนแรงที่จะเกิดขึ้นจากความเสี่ยงว่ามีมากน้อยแคไหน ซึ่งจะพิจารณาจากความรุนแรงของผลกระทบมีตั้งแต่รุนแรงมากจนถึงมากที่สุดมี ๕ ระดับคือ ๑ ๒ ๓ ๔ ๕

O ผลกระทบกับภารกิจหลัก (Mission) หมายถึง การพิจารณาผลกระทบที่มีต่อภารกิจหลักของเรือนจำว่ามีผลกระทบมากหรือน้อย เพียงใด การวิเคราะห์ความเสี่ยงจะต้องค้นหาปัจจัยเสี่ยงและพิจารณาประเด็นความเสี่ยงเหล่านั้นโดยใช้หลักการทั้ง ๓ หลักอย่างบูรณาการ ซึ่งการวิเคราะห์ความเสี่ยงเป็นสิ่งที่ทำได้ยากและต้องอาศัยวิจารณญาณและการไตร่ตรองอย่างถี่ถ้วน

๓ การจัดการความเสี่ยง (Risk Response)

เป็นขั้นตอนการกำหนดวิธีการเพื่อลดความเสี่ยง เมื่อทราบความเสี่ยงที่มีนัยสำคัญและโอกาสที่จะเกิดความเสี่ยงแล้ว ควรวิเคราะห์สาเหตุที่ทำให้เกิดความเสี่ยงและพิจารณาว่าจะจัดการกับความเสี่ยงนั้นอย่างไร ในการพิจารณาเลือกวิธีดำเนินการต้องคำนึงถึงค่าใช้จ่ายหรือต้นทุนในการจัดการความเสี่ยงนั้น เปรียบเทียบกับประโยชน์ที่จะได้รับว่าเหมาะสมและคุ้มค่าหรือไม่ ทั้งนี้ควรพิจารณาว่าความเสี่ยงที่เกิดขึ้นนั้นเป็นความเสี่ยงที่เกิดจากปัจจัยภายใน (Internal) เช่น ระบบการทำงานไม่เหมาะสม คุณภาพและความสามารถของบุคลากร ขนาดและโครงสร้างของเรือนจำ หรือปัจจัยภายนอก (External) เช่น การเปลี่ยนแปลงทางเศรษฐกิจ การเมือง เทคโนโลยีและกฎหมายใหม่ที่มีผลบังคับ รวมถึงต้องพิจารณาว่าเป็นความเสี่ยงด้านใด กรณีเป็นความเสี่ยงเกี่ยวกับหน่วยงานโดยรวม ส่วนใหญ่เกิดจากปัจจัยภายนอก (External) ซึ่งไม่ได้อยู่ภายใต้การควบคุม การป้องกันหรือการลดความเสี่ยงกระทำได้โดยการบริหารคามเสี่ยง (Risk Management) โดยแยกประเภทของความเสี่ยง ดังนี้

๑.ประเภทของความเสี่ยงแบ่งออกเป็น ๔ ประเภท คือ

O ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

O ความเสี่ยงในการดำเนินงาน (Operational Risk)

O ความเสี่ยงด้านการเงิน (Financial Risk)

O ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ (Compliance Risk)

๒. การจัดการความเสี่ยงการป้องกันหรือลดความเสี่ยงสามารถจัดการได้โดย

O การหลีกเลี่ยง (Avoiding) คือการหยุดดำเนินการหรือหลีกเลี่ยงการดำเนินการหรือหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยง เช่น การใช้โปรแกรมที่ไม่ถูกลิขสิทธิ์

O การแบ่งความรับผิดชอบ (Sharing/Transfer) คือการแบ่งความรับผิดชอบให้ผู้อื่นเข้ามามีส่วนช่วยในการจัดการกับความเสี่ยง เช่น การใช้โปรแกรมที่ไม่ถูกลิขสิทธิ์

O การลด (Reducing/Reduction) คือการควบคุมเพื่อลดโอกาสที่จะเกิดความเสี่ยงหรือลดผลกระทบจากความเสี่ยง

O การยอมรับ (Acceptiong) คือการยอมรับความเสี่ยงนั้นเนื่องจากได้ลดความเสี่ยงลงจนเป็นที่พอใจแล้วหรือค่าใช้จ่ายในการลดความเสี่ยงสูงและไม่คุ้มค่าที่จะดำเนินการ

๔. การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยงการลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยงเมื่อเรือนจำทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้ เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

๔.๑ พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๔.๒ เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๔.๓ กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๔.๔ ในครั้งต่อไป ให้พิจารณาผลการติดตามการบริหารความเสี่ยงในครั้งก่อนหน้า มาใช้ประกอบการดำเนินการบริหารความเสี่ยงตามกระบวนการ หากพบว่ายังมีความเสี่ยงมีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานของเรือนจำให้นำมาระบุการควบคุมในการแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้ามีเหลืออยู่ให้วิเคราะห์ว่ามีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บัญชาการเรือนจำเพื่อทราบและสั่งการ

๕.การทบทวนการบริหารความเสี่ยง โดยระบุรอบเวลาในการทบทวนอย่างชัดเจน

เป็นขั้นตอนการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยงว่ามีความเสี่ยงด้านใดบ้างแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้การทบทวนการบริหารความเสี่ยงยังเป็นการประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่เลือกใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

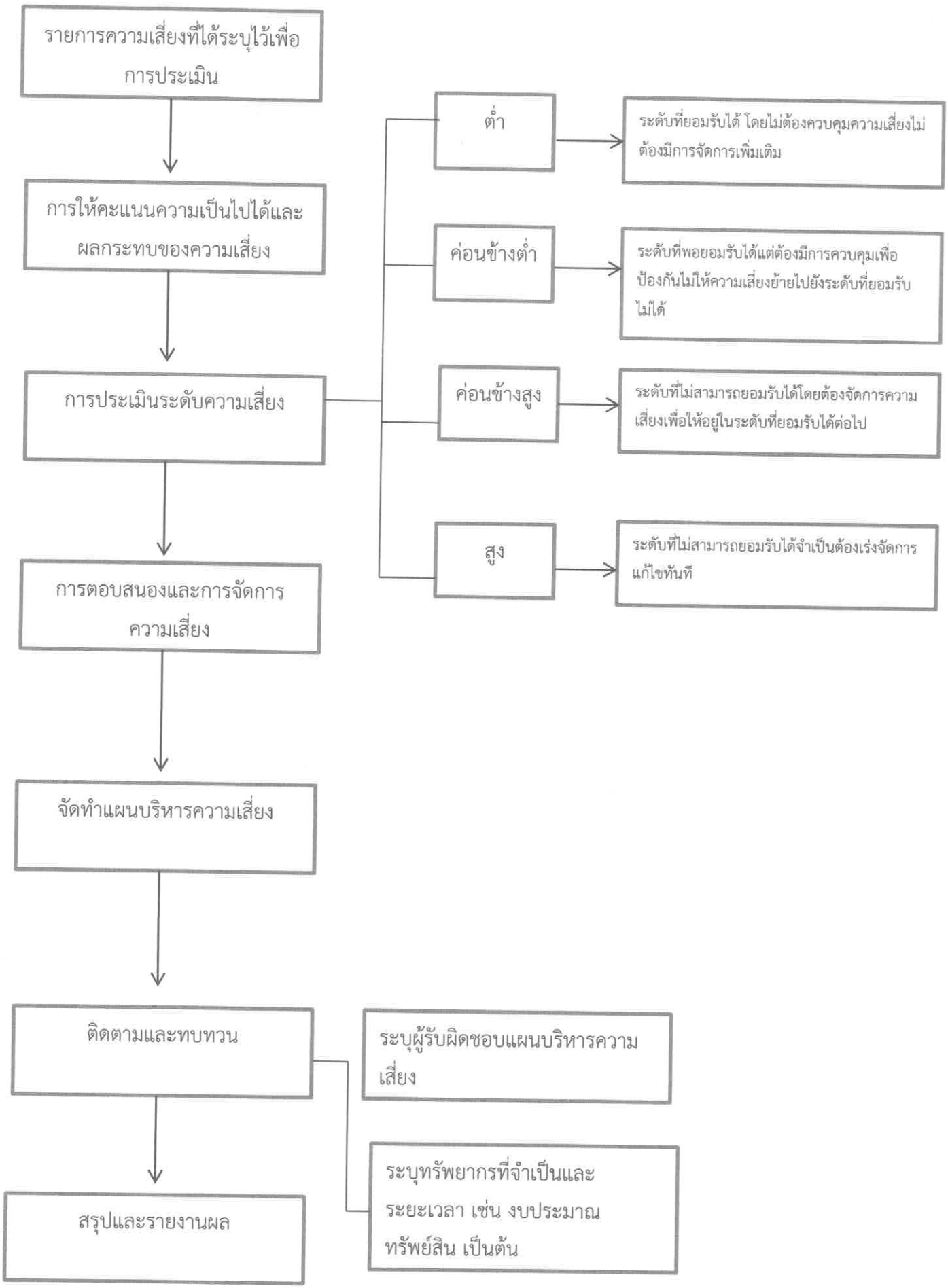
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่มนุษย์สร้างขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อเหตุจลาจล รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายและระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

๒. ความเสี่ยงด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดขึ้นกับระบบเครือข่ายเทคโนโลยีสารสนเทศต่าง ๆ เช่น ระบบเครือข่ายอินเทอร์เน็ตขัดข้อง ไวรัสคอมพิวเตอร์ ภัยคุกคามทางคอมพิวเตอร์ต่าง ๆ

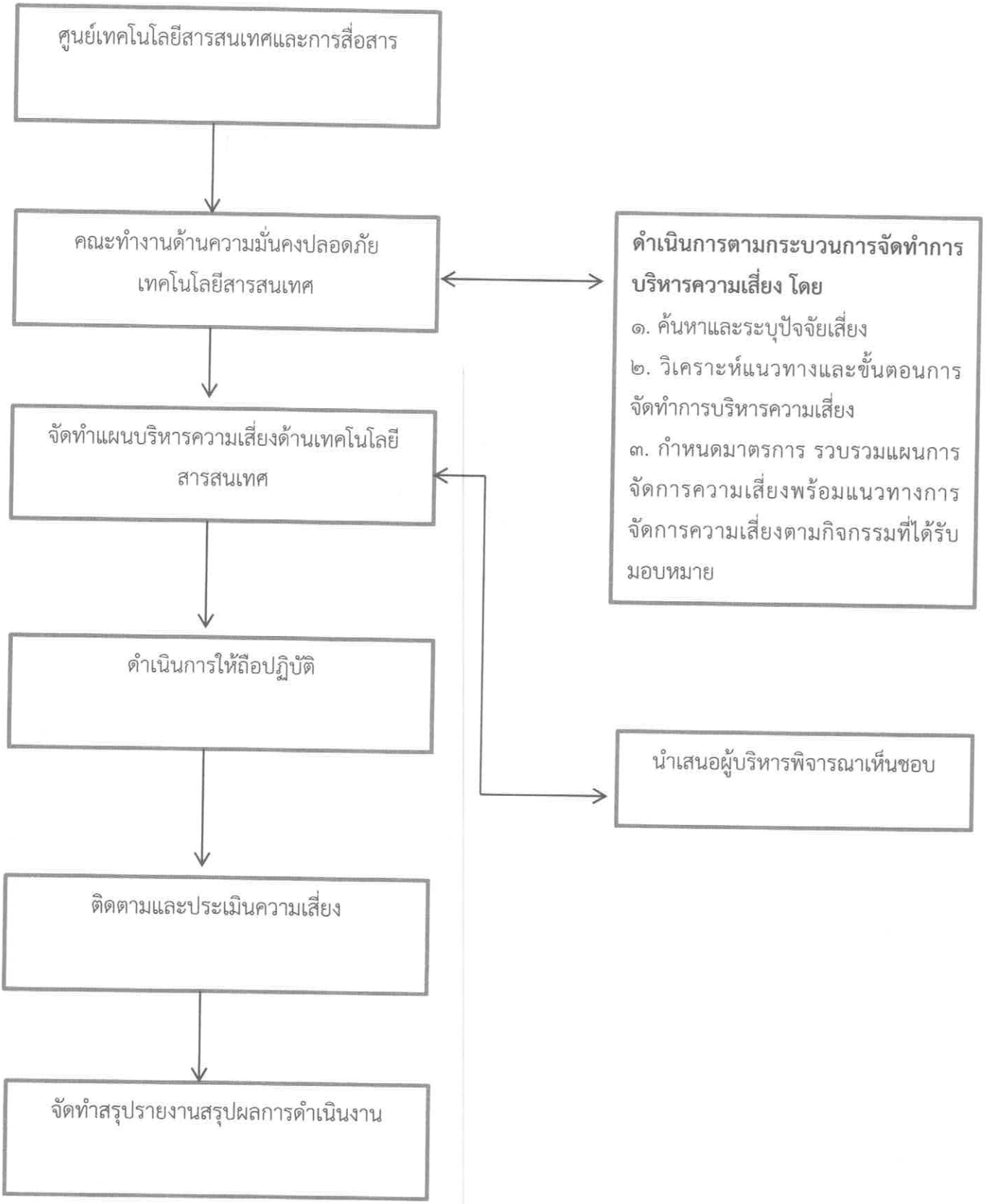
๓. ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล หมายถึง ความเสี่ยงที่เกิดจากการทำงานของระบบสารสนเทศและการจัดเก็บข้อมูลสารสนเทศ ที่อาจเกิดความเสียหายจากการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ ไม่มีการอัพเดทโปรแกรมให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ ตลอดจนความเสี่ยงจากการถูกบุกรุกข้อมูล การสูญหายของข้อมูล ความถูกต้องน่าเชื่อถือของข้อมูล และรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ

๔. ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผนการตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

๑. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



๒. กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร



๓. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
๑	ความชื้นอุณหภูมิห้องคอมพิวเตอร์แม่ข่ายกลาง	๔	๔	๑๖
๒	ระบบกระแสไฟฟ้าขัดข้อง	๔	๔	๑๖
๓	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย	๓	๕	๑๕
๔	การถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	๔	๔	๑๖
๕	การนำอุปกรณ์เคลื่อนที่ (Smart Phone,Tablet,PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่าย	๕	๓	๑๕
๖	ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	๔	๔	๑๖
๗	การบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์	๓	๔	๑๒
๘	การสูญหายของข้อมูล	๒	๕	๑๐
๙	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	๒	๕	๑๐
๑๐	การเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	๑	๕	๕
๑๑	สถานการณ์ความสงบเรียบร้อยในบ้านเมือง	๑	๕	๕
๑๒	แมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า/สายสัญญาณ	๑	๔	๔
๑๓	การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	๑	๕	๕
๑๔	การถูกโจมตีระบบจากเครือข่ายภายใน	๒	๓	๖
๑๕	ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	๒	๓	๖
๑๖	การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	๑	๔	๔

๔.ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการจัดการความเสี่ยง	ผู้รับผิดชอบ
ระดับความเสี่ยงสูง							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๑.ความเสี่ยงจากความชื้น อุณหภูมิ ห้องคอมพิวเตอร์แม่ข่ายไม่มีระบบปรับอากาศที่ได้มาตรฐานสามารถควบคุมอุณหภูมิความชื้นได้	ระบบปรับอากาศที่ไม่ได้มาตรฐานสำหรับห้องคอมพิวเตอร์แม่ข่าย	การทำงานของเครื่องอายุและอุปกรณ์สั้นลง	สูง	๑.ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ ๒.วางแผนจัดหาระบบปรับอากาศชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้	การยอมรับ	เรือนจำจังหวัดสุพรรณบุรี
	๑.ความเสี่ยงไม่สามารถใช้งานเครื่องแม่ข่าย และระบบเครือข่ายได้กรณีเกิดไฟฟ้าขัดข้อง ๒.ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่ายทั้งส่วนระบบปฏิบัติการ Operating System ระบบฐานข้อมูล อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ Shutdown อย่างเหมาะสม	๑.ระบบกระแสไฟฟ้าขัดข้อง ๒.UPS มีอายุการใช้งานมาก ไม่มีระบบการสำรองไฟ/ไม่มีระบบการแจ้งเตือนที่รวดเร็ว	๑.ระบบไม่สามารถทำงานได้ ๒.ข้อมูล/อุปกรณ์เสียหาย ๓.ระบบปฏิบัติการโปรแกรมหรือฐานข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายเสียหายต้องมีการติดตั้งใหม่	สูง	๑.ตรวจสอบการทำงานระบบสำรองไฟฟ้าอย่างสม่ำเสมอ ๒.วางแผนการจัดหาและติดตั้ง UPS และเครื่องกำเนิดไฟฟ้า	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการจัดการความเสี่ยง	ผู้รับผิดชอบ
ระดับความเสี่ยงสูง							
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๑.ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ ๒.ความเสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล	- การทำงานเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ขัดข้อง	๑.ระบบงานไม่สามารถใช้ได้ตามปกติ ๒.ข้อมูลเสียหาย	สูง	๑.ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล ๒.จัดหา Dr-Site ๓.จัดจ้างผู้ดูแลระบบ (Out Source)	การถ่ายโอน	เรือนจำจังหวัดสุพรรณบุรี
ความเสี่ยงด้านบุคลากร (Human Risk)	๑.ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของเรือนจำที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	- สิทธิ์ฐานข้อมูลผู้ใช้งานระบบเทคโนโลยีสารสนเทศไม่เป็นปัจจุบันเนื่องจากผู้ใช้งานมีการลาออก โอน ย้าย สิ้นสุดการจ้างตลอดเวลา	๑.หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน/ข้อมูล/อาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางผิดกฎหมาย ๒.ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้จะนำมาซึ่งการขาดความเชื่อถือของหน่วยงาน	สูง	หน่วยงานในสังกัดต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยในกรณีผู้ใช้งานของหน่วยงานภายในลาออก โอน ย้าย หรือสิ้นสุดการจ้างในหน่วยงานทำหนังสือแจ้งให้กับหน่วยงานผู้ดูแลระบบทราบทันทีเพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี
	๒.ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	อุปกรณ์ที่ใช้ไม่มีระบบรักษาความปลอดภัยที่ถูกต้องและเพียงพอ	๑.อาจเกิดช่องโหว่ของระบบรักษาความปลอดภัยของหน่วยงานและอาจมีการโจมตีทำให้ระบบไม่สามารถทำงานได้	สูง	๑.อบรมเผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของหน่วยงาน ๒.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยอย่างเคร่งครัด	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการจัดการความเสี่ยง	ผู้รับผิดชอบ
ระดับความเสี่ยงสูง							
	๓.ความเสี่ยงจากการที่ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	๑.เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อย่างปลอดภัย ๒.การใช้ทรัพยากรของหน่วยงานทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์ หรือเพลงที่ไม่มีลิขสิทธิ์เป็นต้น	๑.ระบบเสียหายหยุดชะงักการทำงาน ๒.สูญเสีย Bandwidth ในเครือข่ายทำให้ต้องจัดเพิ่ม Bandwidth ให้มากขึ้น ๓. อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	สูง	๑.อบรมสร้างความรู้ความเข้าใจการใช้งานที่ถูกวิธี ๒.กำหนด Policy ของอุปกรณ์รักษาความปลอดภัยของหน่วยงานให้มีความปลอดภัยและตรวจสอบการทำงานระบบอย่างสม่ำเสมอและการเปิด Port เท่าที่จำเป็น ๒.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี
ความเสี่ยงค่อนข้างสูง							
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	๑.ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hackerไวรัส Malware ต่าง ๆ เป็นต้น	การถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	๑.อาจทำให้ระบบเครือแม่ข่าย หรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นทั้งหมดในเครือข่าย ๒.ระบบ/ข้อมูลอาจจะถูกแก้ไขหรือเปลี่ยนแปลง เช่น รูปภาพ บน Web Site ของสำนักงาน ๓.อาจถูกโจรกรรมข้อมูลที่เป็นความลับ	ค่อนข้างสูง	๑.ติดตั้งโปรแกรมป้องกันไวรัสและ patchอย่าง สม่ำเสมอ ๒.ติดตั้งระบบป้องกัน และเตือนภัย ๓.ตรวจสอบการตั้งค่า policy และ Log ของ Firewall IPS อย่างสม่ำเสมอ ๔.ติดตั้ง pathc ของระบบปฏิบัติการสม่ำเสมอ ๕.จัดเจ้าหน้าที่รับผิดชอบตรวจสอบ/เฝ้าระวัง	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงค่อนข้างสูง							
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	๑.ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง	ระบบสารสนเทศที่ไม่มีการสำรองข้อมูล/ดำเนินการสำรองไม่ต่อเนื่อง	๑.ระบบเกิดขัดข้อง/ข้อมูลเสียหายไม่มีข้อมูลให้ดำเนินการกู้คืน ๒.ระบบเสียไม่สามารถใช้งานและบริการข้อมูลได้	ค่อนข้างสูง	๑.หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบอย่างสม่ำเสมอ ๒.มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	๑.การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	๑.หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้น ๆ	ค่อนข้างสูง	๑.การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น ๒.สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	ยอมรับ	เรือนจำจังหวัดสุพรรณบุรี
ความเสี่ยงต่ำ							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	๑.ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม จนไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ส่งผลให้ระบบหลักไม่สามารถใช้งานได้คอมพิวเตอร์และเครือข่ายและข้อมูลสูญหาย	-ไฟไหม้ ไฟฟ้าลัดวงจร การวางเพลิง -ภัยธรรมชาติ	๑.เสียงบประมาณในการจัดหาระบบทดแทน ๒.ไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทนได้	ต่ำ	๑.จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP) ๒.วางแผนจัดหาและติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง ๓.จัดหา Dr-Site ๔.สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงต่ำ							
	๒.ความเสี่ยงจากสถานการณ์ความสงบเรียบร้อยในบ้านเมือง	-การชุมนุมประท้วง -การจลาจล/ก่อการร้าย -การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญของเรือนจำ	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อยจนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	ต่ำ	๑.จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP Plan) ๒. จัดทำศูนย์สำรอง (Backup Site)	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี
	๓.ความเสี่ยงจากแมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์หรือ สายไฟฟ้า/สายสัญญาณ	เลี่ยงต่อการอุปกรณ์/ระบบไม่สามารถใช้งานได้ปกติ	๑.เสียประมาณในการซ่อมแซมหรือจัดหาทดแทน ๒. ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	ต่ำ	๑.ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack ๒.ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware Data Communication Risk)	๑.ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	๑.ไม่สามารถใช้งานระบบงานของสำนักงานผ่านเครือข่ายอินทราเน็ตได้ ๒.ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯ ผ่านเครือข่ายอินเทอร์เน็ตได้	๑.เจ้าหน้าที่และผู้บริหารงานสำนักงานฯ ไม่สามารถใช้งานระบบอินเทอร์เน็ตสำหรับปฏิบัติงานได้ ๒.บุคคลภายนอกไม่สามารถเข้าใช้งานข้อมูลสารสนเทศของหน่วยงานผ่านเครือข่าย	ต่ำ	๑.ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการเครือข่ายอินเทอร์เน็ต ๒.ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี
	๒.ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ	อาจส่งผลให้ระบบเครือข่ายไม่สามารถใช้หรือใช้ได้แต่ช้ามาก	ต่ำ	๑.กำหนดแนวปฏิบัติการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ ๒.การควบคุมด้วยระบบ Desktop Management	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงต่ำ							
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	๑.ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรืออุปกรณ์สำรองข้อมูลประเภทต่าง ๆ	๑.ข้อมูลที่อยู่ในชั้นความลับรั่วไหลทำให้เสียหายต่อความเชื่อถือของเรือนจำ ๒.ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	ต่ำ	๑.มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk อุปกรณ์สำรองข้อมูลประเภทต่าง ๆ ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้น ๆ ทิ้งแล้ว หากทำได้ ๒.ก่อนจำหน่าย	การยอมรับ	เรือนจำจังหวัดสุพรรณบุรี
	๒.ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	๑.เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง ๒.เสียเวลาในการกู้ระบบ ๓.เสียภาพลักษณ์ของเรือนจำ	ต่ำ	๑.ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย ๒.จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebookไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน ๓.ควบคุมการเข้าออกและขนย้ายเครื่องคอมพิวเตอร์เข้า-ออก อาคารตลอดเวลา ๔.ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ๆ มี เครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	การควบคุม	เรือนจำจังหวัดสุพรรณบุรี

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
เรือนจำจังหวัดสุพรรณบุรี
กรมราชทัณฑ์ กระทรวงยุติธรรม

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของเรือนจำจังหวัดสุพรรณบุรี บรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๖			๒๕๖๗			๒๕๖๘			๒๕๖๙			๒๕๗๐			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
๑.ความเสี่ยงจากความชื้น อุณหภูมิ ห้องคอมพิวเตอร์แม่ข่ายกลางไม่มีระบบปรับอากาศที่ได้มาตรฐานสามารถควบคุมอุณหภูมิความชื้นได้	๑.ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ ๒.วางแผนจัดหาระบบปรับอากาศชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้	-ทุกวัน ปีงบประมาณ ๒๕๖๖	←									↔					→	เรือนจำจังหวัดสุพรรณบุรี
๒.ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้อง	๑.ตรวจสอบการทำงานระบบสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ ๒.วางแผนการจัดหาและติดตั้ง UPS และเครื่องกำเนิดไฟฟ้า (Electrical Generator)	-ทุกวัน ปีงบประมาณ ๒๕๖๗	←			↔												→	เรือนจำจังหวัดสุพรรณบุรี
๓.ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักและอุปกรณ์เสียหาย	๑.ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล ๒.จัดหา Dr-Site ๓.จัดหาผู้ดูและระบบ (Out Source)	ทุกครั้งที่มีการเปลี่ยนแปลงผู้ใช้งาน	←									↔					→	เรือนจำจังหวัดสุพรรณบุรี
๔.ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	หน่วยงานในสังกัดเรือนจำจังหวัดสุพรรณบุรี ต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานภายในเรือนจำลาออก โอน ย้าย หรือสิ้นสุดการจ้างให้หน่วยงานทำหนังสือแจ้งให้กับเรือนจำ/ผู้ดูแลระบบทราบทันที เพื่อจะได้ปรับปรุงฐานข้อมูลผู้มีสิทธิ์ใช้งาน		←														→	

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๖			๒๕๖๗			๒๕๖๘			๒๕๖๙			๒๕๗๐			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
	ระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน																	
๕.ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone Tablet PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	๑.อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของหน่วยงาน ๒.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	๑ ครั้ง/ปี	←		↔			↔			↔			↔			↔	→	เรือนจำจังหวัดสุพรรณบุรี
๖.ความเสี่ยงจากการที่ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	๑.อบรม สร้างความรู้ความเข้าใจการใช้งานที่ถูกวิธี ๒.กำหนด Policy ของอุปกรณ์รักษาความปลอดภัยของหน่วยงานให้มีความปลอดภัยและตรวจสอบการทำงานระบบอย่างสม่ำเสมอและการเปิด Port เท่าที่จำเป็น ๓.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	๑ ครั้ง/ปี ๑ ครั้ง/ปี			↔			↔			↔			↔			↔		เรือนจำจังหวัดสุพรรณบุรี
๗.ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker ไวรัส Malware ต่าง ๆ เป็นต้น	๑.ติดตั้งโปรแกรมป้องกันไวรัส Malware Trojan และ Update patch สม่ำเสมอ ๒.ตรวจสอบการตั้งค่า Policy และ Log ของ Firewall IPS อย่างสม่ำเสมอ ๓.อบรม เผยแพร่ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของหน่วยงาน	๒ ครั้ง/ปี ๑ ครั้ง/ปี	←															→	เรือนจำจังหวัดสุพรรณบุรี
					↔			↔			↔			↔			↔		

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	๒๕๖๖			๒๕๖๗			๒๕๖๘			๒๕๖๙			๒๕๗๐			ผู้รับผิดชอบ
			๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	๑-๔	๕-๘	๙-๑๒	
๘.ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานกู้คืนได้หากระบบเกิดเหตุขัดข้อง	๑.หน่วยงานเจ้าของระบบสารสนเทศต้องมีการสำรองข้อมูล (Backup) ระบบอย่างสม่ำเสมอ ๒.มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	ทุกวัน/ตามความเหมาะสม ๑ ครั้ง/ปี	←		→			→			→			→			→	เรือนจำจังหวัดสุพรรณบุรี
๙.การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	๑.การจัดหาซอร์ฟแวร์ที่ถูกกฎหมายมาใช้งานตามจำเป็น ๒.สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	๑ ครั้ง/ปี	←														→	เรือนจำจังหวัดสุพรรณบุรี