



แผนการบริหารความเสี่ยง

และ

แก้ไขปัญหามาจากภัยพิบัติและการรักษาความปลอดภัย  
ระบบฐานข้อมูลและสารสนเทศ

ศูนย์ปฏิบัติการจังหวัดนครราชสีมา

โดย

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด  
สำนักงานจังหวัดนครราชสีมา

## คำนำ

สำนักงานจังหวัดนราธิวาส ได้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงและแก้ไขปัญหาจากภัยพิบัติและการรักษาความปลอดภัยระบบฐานข้อมูลและสารสนเทศของศูนย์ปฏิบัติการจังหวัดนราธิวาส ซึ่งอาจเกิดขึ้นในระบบบริหารงานสั่งการและการปฏิบัติงานเพื่อการบำบัดทุกข์ บำรุงสุขประชาชนทั่วประเทศ จึงเห็นถึงความจำเป็นในการระมัดระวังต่อสถานการณ์ที่คุกคามต่อประสิทธิภาพการปฏิบัติงาน การบริหารงาน และอาจทำให้เกิดความเสียหายต่อระบบฐานข้อมูลสารสนเทศซึ่งเป็นเครื่องมือที่สำคัญที่สุดในการให้บริการประชาชนและการตัดสินใจของผู้บริหาร ตลอดจนคณะกรรมการ ผู้บริหารประเทศ

การรักษาความมั่นคงและปลอดภัยของระบบฐานข้อมูลและสารสนเทศจึงเป็นปัจจัยสำคัญประการหนึ่ง ที่มีผลต่อความสำเร็จของระบบบริหารราชการของจังหวัด

สำนักงานจังหวัดนราธิวาส จึงได้จัดทำแผนบริหารความเสี่ยงและแก้ไขปัญหาจากภัยพิบัติและการรักษาความปลอดภัยขึ้นเพื่อใช้เป็นแนวทางปฏิบัติประกอบการบริหารความเสี่ยง เพื่อลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นและส่งผลกระทบต่อกระบวนการบริหารราชการของจังหวัด

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด  
สำนักงานจังหวัดนราธิวาส

# สารบัญ

	หน้า
*** มาตรการบริหารความเสี่ยงของระบบสารสนเทศ	๑
*** แผนป้องกันและแก้ไขปัญหากจากภัยพิบัติและการรักษาความปลอดภัย	๑๑
*** ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗	๑๔
*** การประสานงานกับหน่วยงานที่เกี่ยวข้อง เมื่อเผชิญเหตุ	๒๑
*** แผนผังระบบเครือข่าย ( Network System )	๒๕

**มาตรการบริหารความเสี่ยงของระบบสารสนเทศ  
ศูนย์ปฏิบัติการจังหวัดนราธิวาส**

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่ต้อง ดำเนินการใน อนาคต	หมายเหตุ
๑	<b>การสร้างความปลอดภัยทางกายภาพ</b> เพื่อป้องกันผู้ที่ไม่เกี่ยวข้องเข้ามาในบริเวณซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและระบบคอมพิวเตอร์	๑.ห้ามบุคคลผู้ที่ไม่ใช้อำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่ายหรือห้องที่มีความสำคัญต่าง ๆ หากจำเป็นให้เจ้าหน้าที่ของศูนย์ที่เป็นผู้รับผิดชอบในการนำพาเข้าไป และเฝ้าดูตลอดเวลาที่บุคคลนั้นอยู่ในห้องดังกล่าวและนำกลับออกมาเมื่อเสร็จสิ้นภารกิจ ๒.การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ของเจ้าหน้าที่ฯ จะต้องทำการใส่บัญชีผู้ใช้ (Username) และ/หรือรหัสผ่าน (Password)	๑. มีการควบคุมการเข้าออกห้องห้องคอมพิวเตอร์แม่ข่าย (Server) ห้องที่มีความสำคัญต่าง ๆ รวมทั้งการควบคุมและจำกัดการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ ให้เป็นไปตามระเบียบของทางราชการฯ	๑.ปรับปรุงห้องเครื่องคอมพิวเตอร์แม่ข่าย และห้องที่มีความสำคัญต่าง ๆ ให้มีความมั่นคงมากยิ่งขึ้น	
๒	<b>การป้องกันและแก้ไขปัญหากระแสไฟฟ้าขัดข้อง</b> เพื่อป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและระบบคอมพิวเตอร์	๑. เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล	๑.การติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptible PowerSupply:UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์	๑.บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
		๒.เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่ และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในศูนย์ฯด้วย	คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล(PC) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๒๐-๓๐ นาที		
๓	การสร้างความปลอดภัยให้กับระบบปฏิบัติการ เพื่อเป็นการสร้างพื้นฐานความปลอดภัยและลดความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์แก่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และคอมพิวเตอร์ส่วนบุคคล	๑. ผู้ใช้งานจะต้องตั้งค่าให้ระบบปฏิบัติการ ทำการปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอ (Patch Update) ๒. ผู้ใช้งานจะต้องเปิดใช้งานไฟร์วอลล์ (Firewall) การกู้คืนข้อมูล (Recovery) ของระบบปฏิบัติการตลอดเวลา	๑.มีการควบคุมการติดตั้งระบบปฏิบัติการ และมีการปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอและใช้ความสามารถของระบบปฏิบัติการในการสร้างความปลอดภัยให้กับระบบคอมพิวเตอร์ ได้แก่ การควบคุมและจำกัดสิทธิของผู้ใช้ได้ตามอำนาจหน้าที่และความรับผิดชอบ การเปิดใช้งานไฟร์วอลล์ (Firewall) การกู้คืนข้อมูล เป็นต้น	๑. ให้ความรู้และความเข้าใจแก่บุคลากรของสำนักงานฯ ในการใช้งานระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
๔	การสร้างความปลอดภัยให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อเป็นการสร้างพื้นฐานความปลอดภัยและลดความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์แก่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	<p>๑. ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่าย จะต้องเฝ้าระวังภัยคุกคามทางคอมพิวเตอร์ที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายอย่างต่อเนื่อง</p> <p>๒. เจ้าหน้าที่ผู้รับผิดชอบ จะต้องทำการใส่บัญชีผู้ใช้ (Username) และ/หรือ รหัสผ่าน (password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของศูนย์ฯเสมอ</p> <p>๓. เจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่ายจะต้องทำการตั้งค่าและเปิดใช้งานบริการ (Service) ต่าง ๆ ของระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย ที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบตลอดเวลา</p>	<p>๑. มีการติดตั้งระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งเป็นระบบปฏิบัติการที่มีความสามารถในการบริหารจัดการความปลอดภัยสูง และใช้ความสามารถของระบบปฏิบัติการ ในการสร้างความปลอดภัยให้กับเครื่องคอมพิวเตอร์แม่ข่าย ได้แก่ การควบคุมและจำกัดสิทธิของผู้ใช้ได้ตามอำนาจหน้าที่และความรับผิดชอบ การเปิดใช้งานไฟลวอลล์ การกักตุนข้อมูล การสำรองข้อมูลเป็นต้นรวมทั้งการใช้โปรโตคอล Secure Shell (SSH) ในการติดต่อกับ Web Server เพื่อเพิ่มความปลอดภัยให้สูงกว่าการ FTP หรือ Telnet</p>		

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
๕	การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของศูนย์ฯ	<p>๑. เจ้าหน้าที่ผู้รับผิดชอบจะต้องเปิดใช้งานไฟร์วอลล์และระบบป้องกันไวรัสคอมพิวเตอร์ตลอดเวลา</p> <p>๒. เจ้าหน้าที่ดูแลระบบเครือข่าย จะต้องทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตของศูนย์ฯอย่างสม่ำเสมอ</p> <p>๓. เจ้าหน้าที่ผู้รับผิดชอบจะต้องตั้งค่า (Setup) ให้ซอฟต์แวร์สามารถ Update โปรแกรมสำหรับการอุดช่องโหว่โดยอัตโนมัติหรือการลงซอฟต์แวร์ที่มีเวอร์ชันใหม่กว่าตามความเหมาะสม</p> <p>๔. ผู้ใช้จะต้องบันทึกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเป็นการแสดงตนก่อนอนุญาตให้เข้าสู่ระบบต่าง ๆ ของศูนย์ฯ ตามอำนาจหน้าที่และความรับผิดชอบ</p> <p>๕. ห้ามไม่ให้ผู้ที่มีอำนาจหน้าที่เข้ามาใช้งานซอฟต์แวร์ระบบหรือ</p>	<p>๑. การติดตั้งไฟร์วอลล์ (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ส่วนบุคคลของศูนย์ฯได้</p> <p>๒. โปรแกรมป้องกันไวรัสคอมพิวเตอร์ทั่วทั้งศูนย์ฯ ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ส่วนบุคคล</p> <p>๓. มีระบบการตรวจสอบปริมาณข้อมูลการใช้งานเครือข่ายอินเทอร์เน็ตของศูนย์ฯ ผ่านซอฟต์แวร์ของศูนย์ฯ</p> <p>๔. มีการเฝ้าดูการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและใช้ความสามารถของซอฟต์แวร์ใน</p>	<p>๑. พัฒนาและปรับปรุงระบบให้มีความพร้อมใช้งานอยู่ตลอดเวลาอย่างต่อเนื่อง</p> <p>๒. การให้ความรู้อย่างต่อเนื่องแก่บุคลากรฯของศูนย์ฯในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์อย่างปลอดภัย</p>	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
		ซอฟต์แวร์บางประเภทที่มีผลต่อการควบคุมการทำงานของซอฟต์แวร์อื่นหรือเป็นตัวกลางในการแก้ไขเปลี่ยนแปลงข้อมูลโดยตรง	<p>การนำข้อมูลเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย เพื่อบันทึกกิจกรรม วัน เวลาที่มีการนำเข้าสู่ข้อมูล หรือ การปรับปรุงแก้ไขข้อมูล</p> <p>๕. มีการอุดช่องโหว่ของซอฟต์แวร์คอมพิวเตอร์ทั้งซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์ประยุกต์โดยการตั้งค่า (Setup) ให้ซอฟต์แวร์สามารถ Update โปรแกรมสำหรับการอุดช่องโหว่โดยอัตโนมัติ หรือการลงซอฟต์แวร์ที่มีเวอร์ชันใหม่กว่าตามความเหมาะสม</p> <p>๖. มีระบบสารสนเทศซึ่งบังคับให้ผู้ใช้จะต้องบันทึกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเป็นการแสดงตนก่อนอนุญาตให้เข้าสู่ระบบ</p>		



ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
			๗.มีการควบคุมและป้องกันไม่ให้ผู้ที่ไม่มีอำนาจหน้าที่เข้ามาใช้งานซอฟต์แวร์ระบบหรือซอฟต์แวร์บางประเภทที่มีผลต่อการควบคุมการทำงานของซอฟต์แวร์อื่น หรือเป็นตัวกลางในการแก้ไขเปลี่ยนแปลงข้อมูลโดยตรง		
๖	การฟื้นฟูระบบ / ข้อมูลจากความเสียหาย (Recovery) เพื่อให้การฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับตลอดจนเหตุการณ์อื่นใดซึ่งอาจส่งผลให้เครื่องคอมพิวเตอร์หรือการประมวลผลของคอมพิวเตอร์หยุด	๑. ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืนข้อมูล (Recovery) ของระบบปฏิบัติการตลอดเวลา ๒.เจ้าหน้าที่ผู้รับผิดชอบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์และการติดตั้งซอฟต์แวร์ใหม่เพื่อทดแทนของเดิมที่เสียหายไป ๓.เจ้าหน้าที่ผู้รับผิดชอบจะต้องทำการบำรุงรักษาระบบเครื่องคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ	๑.มีการตั้งค่าให้ระบบปฏิบัติการของเครื่องคอมพิวเตอร์ทำการฟื้นฟูระบบ/ข้อมูลจากความเสียหาย โดยอัตโนมัติหรือการดำเนินการโดยผู้ใช้งานในการฟื้นฟูระบบ/ข้อมูลจากความเสียหาย ๒. มีการจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์และการติดตั้งซอฟต์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหาย ๓. มีการบำรุงรักษาระบบเครื่องคอมพิวเตอร์และอุปกรณ์สนับสนุนเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ	๑. การดำเนินการตามมาตรการดังกล่าวอย่างต่อเนื่อง	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
๗	การสำรองข้อมูล (Back up) เพื่อลดความเสี่ยงจากที่อาจเกิดขึ้นกับข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ฮาร์ดิสก์เสียหาย ไวรัสคอมพิวเตอร์ ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูล โดยผู้ใช้งานเอง	<p>๑.เจ้าหน้าที่ผู้รับผิดชอบจะต้องตั้งค่าระบบให้มีสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบ แต่ไม่ต่ำกว่า ๑ ครั้ง / เดือน</p> <p>๒.เจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (WebServer) จะต้องตั้งค่าระบบให้มีสำรองข้อมูลโดยอัตโนมัติ</p> <p>๓. ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป จะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม แต่ไม่ต่ำกว่า ๑ ครั้งต่อเดือน</p> <p>๔. เมื่อทางศูนย์ฯประกาศให้มีการสำรองข้อมูล เนื่องจากจะได้มีการดำเนินการที่อาจส่งผลกระทบต่อข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้ ผู้ใช้จะต้องทำการสำรองข้อมูลดังกล่าว ภายในระยะเวลาที่กำหนด</p> <p>๕. หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บไว้ในรูปของเอกสารกระดาษ (Hard Copy)</p>	<p>๑.การติดตั้งระบบสำรองข้อมูลสำหรับเครื่องคอมพิวเตอร์แม่ข่าย</p> <p>๒.การสำรองข้อมูลไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้โดยการบันทึกไว้คนละ Drive</p> <p>๓. การสำรองข้อมูลไว้ใน แผ่น CD</p> <p>๔. การสำรองข้อมูลโดยการพิมพ์ (Print) ออกมาเก็บไว้ในกระดาษสำหรับข้อมูลที่สำคัญ</p> <p>๕. มีการทดสอบความถูกต้องของข้อมูลสำรองและการรายงานผลการตรวจสอบเป็นครั้งคราว ทั้งนี้ขึ้นอยู่กับความสำคัญของข้อมูลในแต่ละระบบฐานข้อมูลหรือของผู้ใช้งานเครื่องคอมพิวเตอร์นั้น ๆ</p>	<p>๑. มีการกำหนดมาตรการและแนวทางในการสำรองข้อมูลที่เป็นระบบมากยิ่งขึ้น</p> <p>๒. มีการทดสอบและเรียกใช้งานข้อมูล สำรองตามระยะเวลาที่เหมาะสม</p>	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
		<p>๖.เจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายและผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไปจะต้องมีการทดสอบความถูกต้องของข้อมูลสำรองและการรายงานผลตรวจสอบเป็นครั้งคราว ทั้งนี้ขึ้นอยู่กับความสำคัญของข้อมูลในแต่ละระบบฐานข้อมูลหรือของผู้ใช้งานเครื่องคอมพิวเตอร์นั้น ๆ</p>			
๘	<p>การป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) เพื่อให้การบริหารและจัดการกับระบบสารสนเทศและเครือข่ายคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ในกรณีเกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติขึ้น</p>	<p>๑. เมื่อเกิดภัยพิบัติ เช่น อัคคีภัยให้ผู้ใช้งานรีบเก็บแผ่นCD ซึ่งบรรจุข้อมูลสำรองซึ่งมีความสำคัญไปด้วยแล้วดำเนินการตามหลักปฏิบัติ/ขั้นตอน ในแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ</p> <p>๒. เมื่อเกิดกรณีการเชื่อมโยงเครือข่ายล้มเหลวเจ้าหน้าที่ผู้รับผิดชอบจะต้องรีบรายงานให้ผู้บังคับบัญชาทราบและดำเนินการประสานผู้ที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยด่วนที่สุดและให้ใช้การเชื่อมโยงเครือข่ายสำรองแทนการเชื่อมโยงหลักในระหว่างที่ดำเนินการแก้ไข ทั้งนี้หากมีเหตุจำเป็นที่ต้องใช้เวลามากกว่า๑วันในการดำเนินการแก้ไขให้ออกประกาศแจ้งแก่ผู้ใช้ งานทราบพร้อมกำหนด เวลาที่จะทำการ แก้ไขเสร็จสิ้น</p>	<p>๑. มีการจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ</p> <p>๒. มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนดังกล่าว</p>	<p>๑. มีการประชาสัมพันธ์และดำเนินการให้เป็นไปตามแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ของศูนย์ฯ</p>	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
		<p>๓. เมื่อเกิดกรณีที่อุปกรณ์จัดเก็บข้อมูลเสียหายให้เจ้าหน้าที่ผู้รับผิดชอบ ทำการตรวจสอบเหตุแห่งความเสียหายนั้นในเบื้องต้นพร้อมรายงานให้ผู้บังคับบัญชาทราบพบว่า</p> <p>หากมีแนวทางที่จะทำการกู้คืนข้อมูลในอุปกรณ์นั้นกลับมาได้ให้ดำเนินการโดยด่วน ทั้งนี้อาจประสานงานขอความช่วยเหลือจากผู้ที่ชำนาญในเรื่องดังกล่าว เพื่อดำเนินการด้วยก็ได้ หากไม่สามารถกู้คืนข้อมูลกลับมาได้ให้นำข้อมูลที่สำรองไว้มาใช้แทน</p> <p>กรณีที่เป็นผู้ใช้งานคอมพิวเตอร์ทั่วไปเมื่อเกิดเหตุอุปกรณ์จัดเก็บข้อมูลเสียหายให้รายงานผู้บังคับบัญชาของตนทราบ แล้วแจ้งให้กลุ่มงานคอมพิวเตอร์ฯ เพื่อตรวจสอบเหตุแห่งเสียหายนั้นในเบื้องต้น หากพบว่ามีแนวทางที่จะทำการกู้คืนข้อมูลในอุปกรณ์นั้นกลับมาได้ให้ดำเนินการโดยด่วน หากไม่สามารถกู้คืนข้อมูลกลับมาได้ให้นำข้อมูลที่สำรองไว้มาใช้แทน</p> <p>จากนั้นให้ทำการส่งซ่อมอุปกรณ์จัดเก็บข้อมูลที่เสียหายดังกล่าวตามระเบียบของทางราชการ ต่อไป</p>			

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
		<p>๔. เมื่อมีการระบาดของไวรัสคอมพิวเตอร์ในเครือข่าย เจ้าหน้าที่ผู้รับผิดชอบ จะต้องทำการวิเคราะห์ความรุนแรงของ ไวรัสคอมพิวเตอร์และตัดการเชื่อมต่อของเครือข่ายคอมพิวเตอร์ เพื่อดำเนินการแก้ไขปัญหาโดยรีบด่วนที่สุด พร้อมทั้งรายงานให้ผู้บังคับบัญชาทราบ</p>			

## แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติและการรักษาความปลอดภัย (Contingency Plan) ศูนย์ปฏิบัติการจังหวัดนครราชสีมา

ศูนย์ปฏิบัติการจังหวัดนครราชสีมา ได้มีมาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติและการรักษาความปลอดภัยที่อาจเกิดขึ้น และสร้างความเสียหายแก่ทรัพย์สินของทางราชการ รวมทั้งระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ดังนี้

### หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัย

เพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติของบุคลากรในศูนย์ปฏิบัติการจังหวัดนครราชสีมา ดังนี้

๑. ไม่กระทำการใด ๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร
๒. ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด
๓. ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบดูทางออกฉุกเฉินไม่ปิดตาย หรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉินทั้งสองทาง เพื่อให้ไปถึงทางหนีฉุกเฉินได้ ถึงแม้ว่าจะดับหรือปกคลุมไปด้วยควัน
๔. เมื่อเกิดเพลิงไหม้ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้ จากนั้นหนีจากอาคารแล้วโทรศัพท์แจ้งหน่วยดับเพลิง โทร ๑๙๙ ทันที หรือแจ้ง ๑๖๖๙
๕. เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ ให้รีบหาทางหนีออกจากอาคารทันที
๖. ถ้าเพลิงไหม้ในห้องทำงานให้หนีออกมาแล้วปิดประตูห้องทันที รีบแจ้งฝ่ายอาคารและสถานที่ เพื่อโทรศัพท์แจ้งหน่วยดับเพลิงต่อไป
๗. ถ้าเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนจะหนีออกมาให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อย ๆ ปิดประตู แล้วหนีไปยังทางหนีไฟฉุกเฉินที่อยู่ใกล้ที่สุด
๘. ถ้าเพลิงไหม้อยู่บริเวณใกล้ ๆ ประตูจะมีความร้อน ห้ามเปิดประตูเด็ดขาด ให้รีบโทรศัพท์เรียกหน่วยดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งถูกเพลิงไหม้ หาผ้าเช็ดตัวเปียกๆ ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง
๙. เมื่อต้องเผชิญกับควันไฟที่ปกคลุม ให้ใช้วิธีคลานหนีไปทางฉุกเฉินเพราะอากาศบริสุทธิ์จะอยู่ด้านล่าง (เหนือพื้นห้อง) นำกุญแจห้องทำงานไปด้วยหากหมดหนทางหนีได้สามารถกลับเข้าห้องได้
๑๐. ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

## ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ จะมีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับสูงมาก ดังนั้น สิ่งที่มีมักจะเกิดขึ้นและยากที่จะหลีกเลี่ยงได้ ก็คือ ผลกระทบต่าง ๆ ที่เกิดขึ้นจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลที่สำคัญ รวมถึงการสูญเสียเวลา จากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ซึ่งประกอบด้วย

### ๑. ไฟฟ้าตก (Sag หรือ Brownout)

ไฟฟ้าตก คือ สภาวะที่แรงดันไฟฟ้าลดต่ำลงจากปกติในช่วงเวลาสั้น ๆ ซึ่งเป็นปัญหาทางไฟฟ้าที่พบบ่อยที่สุด

สาเหตุ เกิดจากการเปิดสวิตช์อุปกรณ์บางชนิดที่ต้องการใช้กระแสไฟฟ้ามาก เช่น เครื่องปรับอากาศ ลิฟต์ และเครื่องมือเครื่องจักร เป็นต้น อุปกรณ์เหล่านี้ต้องการกระแสไฟฟ้ามากในการติดเครื่อง เมื่อเทียบกับการทำงานในภาวะปกติ ส่งผลให้แรงดันไฟฟ้าในสายส่งการไฟฟ้าฯลดต่ำลง

### ๒. ไฟฟ้าดับ (Blackout)

ไฟฟ้างดับ คือ สภาวะที่กระแสไฟฟ้าหยุดไหล

สาเหตุ เกิดจากความต้องการกระแสไฟฟ้าจากสายส่งการไฟฟ้าฯที่มากเกินไป,เกิดไฟฟ้าลัดวงจรในสายส่ง,พายุฟ้าคะนอง,แผ่นดินไหว และปัญหาที่เกิดกับสายส่งการไฟฟ้าฯ เช่น เสายไฟฟ้างลัม หรือหม้อแปลงระเบิด ฯลฯ ซึ่งส่งผลให้ไม่สามารถจ่ายไฟจากการไฟฟ้าได้

ผลกระทบ การทำงานของ RAM หยุดชะงักทันที ทำให้ข้อมูลปัจจุบันสูญหายได้ รวมถึง การบันทึกข้อมูลของตารางการจัดการแฟ้ม (FAT) สูญหายได้ มีผลให้ข้อมูลที่เก็บไว้ทั้งหมดสูญหายได้

### ๓. ไฟฟ้ากระชาก (Spike)

ไฟฟ้ากระชาก คือ สภาวะที่แรงดันไฟฟ้าเพิ่มสูงขึ้นอย่างกะทันหัน โดยสามารถเข้าไปยังอุปกรณ์ไฟฟ้าได้ทั้งจากสายส่งการไฟฟ้าฯ เครือข่ายสื่อสาร และสายโทรศัพท์

สาเหตุ เกิดจากฟ้าผ่าในบริเวณใกล้เคียง หรืออาจเกิดจากสายส่งการไฟฟ้าฯ ที่หยุดการทำงานไปและกลับมาทำงานใหม่อย่างกะทันหัน

ผลกระทบ สร้างความเสียหายหรือทำลายชิ้นส่วนอุปกรณ์อิเล็กทรอนิกส์ของอุปกรณ์ไฟฟ้าได้ รวมถึงข้อมูลเกิดการสูญหาย

### ๔. ไฟฟ้าเกิน (Surge)

ไฟฟ้าเกิน คือ สภาวะที่มีแรงดันไฟฟ้าไหลมาเกินไปในช่วงเวลาสั้น ๆ (๑/๑๒๐ วินาที)

สาเหตุ เกิดจากการใช้อุปกรณ์ไฟฟ้าที่มีมอเตอร์เกินไฟมาก เช่น เครื่องปรับอากาศ หรืออุปกรณ์ไฟฟ้าอื่น ๆ ที่ลักษณะใกล้เคียงกัน ฯลฯ เนื่องจากอุปกรณ์เหล่านี้เมื่อหยุดทำงาน แรงดันไฟฟ้าส่วนหนึ่งที่เหลืออยู่ในมอเตอร์ จะไหลกลับเข้าไปในสายส่งการไฟฟ้าฯ ทำให้เกิดแรงดันไฟฟ้าสูงเกิน

ผลกระทบ ทำให้ชิ้นส่วนอุปกรณ์ภายในเสื่อมสภาพเร็วกว่าปกติหรือเสียหายได้ รวมถึง หน่วยความจำของคอมพิวเตอร์สูญหายและคลาดเคลื่อน, Power supply เสียหาย และการทำงานของระบบสื่อสารผิดพลาด

## ๕. สัญญาณรบกวน (Noise)

**สัญญาณรบกวน** คือ สัญญาณรบกวนที่เกิดจากสนามแม่เหล็กไฟฟ้า (EMI) และสัญญาณคลื่นความถี่วิทยุ (RFI) ซึ่ง ๒ สัญญาณเหล่านี้จะไปรบกวนสัญญาณคลื่นไซน์ (Sine Wave) ของสายส่งการไฟฟ้าฯ

**สาเหตุ** เกิดขึ้นได้จากปรากฏการณ์ทางธรรมชาติ (เช่น พายุฟ้าผ่า), การเปิด-ปิดสวิตช์อุปกรณ์ไฟฟ้า, เครื่องส่งวิทยุ เป็นต้น โดยสัญญาณรบกวนอาจเกิดขึ้นเป็นระยะ ๆ หรืออาจเกิดอย่างสม่ำเสมอก็ได้

**ผลกระทบ** ทำให้การประมวลผลของโปรแกรมและแฟ้มข้อมูลทำงานผิดพลาดและเกิดข้อบกพร่องสำนักงานสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ได้มีการป้องกันปัญหาจากกระแสไฟฟ้างกล่าว โดยการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptible Power Supply ; UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer : PC)

### หลักปฏิบัติของบุคลากร

เพื่อป้องกันการมีให้เกิดความเสียหายอันเกิดจากกระแสไฟฟ้า และบุคลากรสามารถปฏิบัติตนได้ถูกต้องเมื่อเกิดปัญหาจากกระแสไฟฟ้า จึงกำหนดหลักปฏิบัติของบุคลากรในสังกัดสำนักงานสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ดังนี้

๑) เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์ทั้งเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล

๒) เมื่อเกิดกระแสไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่ และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในสำนักงานฯ ด้วย

### **ระบบป้องกันการโจรกรรม**

๑) ดำเนินการในส่วนที่เกี่ยวข้องตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ บทที่ ๕ การรักษาความปลอดภัยเกี่ยวกับสถานที่

2) ห้ามผู้ที่ไม่มีความเกี่ยวข้องเข้าไปในบริเวณห้องคอมพิวเตอร์แม่ข่าย

3) มีการติดตั้งกล้องวงจรปิดทั่วทั้งอาคาร

4) จัดให้มีระบบควบคุมการเข้าออกอาคารในวันหยุด หรือนอกเวลาราชการ

### หลักปฏิบัติของบุคลากร

เพื่อป้องกันการโจรกรรม จึงกำหนดหลักปฏิบัติของบุคลากรในศูนย์ปฏิบัติการจังหวัดนราธิวาส ดังนี้

๑) ปฏิบัติตนให้เป็นไปตามระเบียบของทางราชการในส่วนที่เกี่ยวข้องกับการดูแลรักษาสถานที่ราชการ และระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ บทที่ ๕ การรักษาความปลอดภัยเกี่ยวกับสถานที่

๒) เฝ้าระวัง และสอดส่องดูแลเพื่อป้องกันมิให้เกิดการโจรกรรมขึ้น ทั้งนี้หากพบเห็นเหตุการณ์หรือบุคคลซึ่งคาดว่าจะนำไปสู่การโจรกรรมทรัพย์สินของทางราชการ หรือข้อมูลสารสนเทศต่าง ๆ ให้รีบรายงานให้ผู้บังคับบัญชาทราบโดยด่วนที่สุด เพื่อจะได้ประสานงานกับเจ้าหน้าที่ที่เกี่ยวข้อง หรือเจ้าหน้าที่ตำรวจในการที่จะระงับ หรือจับกุมผู้ที่จะกระทำการดังกล่าวต่อไป



ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗  
 บทที่ ๕ การรักษาความปลอดภัยเกี่ยวกับสถานที่

.....

๓๘. คำจำกัดความ

การรักษาความปลอดภัยเกี่ยวกับสถานที่ คือมาตรการที่กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่ที่สงวน อาคาร และสถานที่ของส่วนราชการ ตลอดจนวัสดุ อุปกรณ์ เจ้าหน้าที่และเอกสารในอาคารสถานที่ดังกล่าวให้พ้นจากการโจรกรรม การจารกรรมและการก่อวินาศกรรมหรือเหตุอื่นใดอันอาจทำให้เสื่อมรรถภาพในการปฏิบัติภารกิจของส่วนราชการได้

๓๙. ความมุ่งหมาย

การรักษาความปลอดภัยเกี่ยวกับสถานที่ที่มีความมุ่งหมายเพื่อ

๓๙.๑ กำหนดมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ของส่วนราชการ

๓๙.๒ เป็นแนวทางในการวางแผนรักษาความปลอดภัยเกี่ยวกับสถานที่ของส่วนราชการที่ตั้งขึ้นใหม่หรือขยายออกไป และเป็นแนวทางในการประเมินค่าแห่งการรักษาความปลอดภัยเกี่ยวกับสถานที่ที่มีอยู่แล้ว

๓๙.๓ เป็นแนวทางให้ส่วนราชการดำเนินมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่ตามความเหมาะสมกับระดับความสำคัญของสถานที่นั้นๆ

๓๙.๔ ช่วยเจ้าหน้าที่รับผิดชอบในการพิทักษ์รักษาสถานที่และวัตถุต่าง ๆ ที่มีค่าสูงของชาติให้ปฏิบัติงานได้อย่างมีประสิทธิภาพ

๔๐. ข้อพิจารณาในการวางแผนมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่

๔๐.๑ ปัจจัยสำคัญที่จะต้องพิจารณาในการวางแผนมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ ได้แก่ ความสำคัญของภารกิจของส่วนราชการนั้น ๆ สภาพของสถานที่ ลักษณะทางภูมิศาสตร์ สถานการณ์ทางเศรษฐกิจ อุดมการณ์ทางการเมืองของประชาชนในพื้นที่นั้น ๆ และพฤติการณ์ของฝ่ายที่อาจเป็นศัตรู ตลอดจนการสนับสนุนช่วยเหลือที่จะพึงได้รับจากส่วนราชการอื่น ๆ

๔๐.๒ ระดับการรักษาความปลอดภัยของสถานที่หนึ่ง ๆ ย่อมมีความแตกต่างกันแล้วแต่ความสำคัญของภารกิจ สิ่งที่เป็นความลับ ทรัพย์สิน และอาคารสถานที่ จึงต้องแยกพิจารณาการวางแผนมาตรการการป้องกันแต่ละอาคารสถานที่ เช่น อาคารสถานที่บางแห่ง พื้นที่ทั้งหมดอาจต้องการมาตรการการรักษาความปลอดภัยเพียงแบบเดียว แต่สถานที่อีกแห่งหนึ่งมีกิจการเฉพาะอย่าง หรือพื้นที่ภายในเฉพาะแห่งที่ต้องการมาตรการการรักษาความปลอดภัยมากแบบเป็นพิเศษ เช่น การจัดแยกกิจการให้อยู่ต่างหาก และการเพิ่มมาตรการการป้องกันให้มากขึ้น เป็นต้น

๔๐.๓ ในการออกแบบก่อสร้างที่สงวน อาคารสถานที่หรือเครื่องกีดขวางทางราชการที่มีความสำคัญหรือความลับจะต้องพิทักษ์รักษา ให้สถาปนิก และ/หรือวิศวกรผู้ออกแบบพิจารณาในด้านการรักษาความปลอดภัยด้วย โดยหารือกับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของส่วนราชการนั้น ๆ หรือองค์การรักษาความปลอดภัย ทั้งนี้ ให้อยู่ในความรับผิดชอบของหัวหน้าส่วนราชการ

๔๑. ภัยอันตรายที่ควรพิจารณาเกี่ยวกับสถานที่

มีภัยอันตรายที่ควรพิจารณาดังนี้

๔๑.๑ ภัยอันตรายที่เกิดจากปรากฏการณ์ธรรมชาติและอุบัติเหตุ เช่น พายุ น้ำท่วม ไฟป่า และเพลิงไหม้ เป็นต้น

๔๑.๒ ภัยอันตรายเกิดจากการกระทำของมนุษย์แบ่งออกเป็น ๒ ประเภท คือ

๔๑.๒.๑ การกระทำโดยเปิดเผย เช่น การโจรกรรม การจลาจล การก่อความไม่สงบ และการโจมตีของข้าศึก เป็นต้น

๔๑.๒.๒ การกระทำโดยทางลับ เช่น การจารกรรม และการก่อวินาศกรรม เป็นต้น

๔๒. การสำรวจหรือการตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่

ในการสำรวจหรือการตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่ราชการต่าง ๆ จะต้องปฏิบัติตามขั้นตอนดังต่อไปนี้

ขั้นที่ ๑ ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของส่วนราชการวางแผนทางในการสำรวจหรือการตรวจสอบ โดยวิเคราะห์สภาพแวดล้อม หลักฐานในการปฏิบัติ และข้อบกพร่องที่มีมาแล้ว

ขั้นที่ ๒ สำรวจบริเวณพื้นที่ และอาคารสถานที่โดยละเอียด

ขั้นที่ ๓ จัดทำรายงานการสำรวจหรือการตรวจสอบ โดยชี้ให้เห็นข้อบกพร่องของมาตรการการป้องกันที่ใช้อยู่ในปัจจุบัน ที่จะทำให้เกิดการละเมิดการรักษาความปลอดภัย แล้วเสนอแนะให้หัวหน้าส่วนราชการพิจารณาแก้ไขมาตรการ และวางระเบียบปฏิบัติในการรักษาความปลอดภัยในเรื่องต่าง ๆ ดังต่อไปนี้

๔๒.๑ เขตรั้วและการจำกัดช่องทางเข้าออก

๔๒.๒ การใช้เครื่องกีดขวาง

๔๒.๓ การให้แสงสว่าง

๔๒.๔ การจัดเจ้าหน้าที่รักษาความปลอดภัยสถานที่

๔๒.๕ การติดต่อสื่อสารและระบบสัญญาณแจ้งภัย

๔๒.๖ การควบคุมการเข้าออกของบุคคลภายนอก

๔๒.๗ การควบคุมการจราจร

๔๒.๘ การควบคุมการเข้าออกของเจ้าหน้าที่ภายใน

๔๒.๙ การกำหนดพื้นที่ที่มีการรักษาความปลอดภัย

๔๒.๑๐ ที่เก็บอาวุธ กระสุน วัตถุระเบิด หรือวัสดุลับของทางราชการ ซึ่งจะต้องพิทักษ์รักษาเป็นพิเศษ

๔๒.๑๑ การป้องกันอัคคีภัย

๔๒.๑๒ การตรวจตราเป็นประจำหรือการตรวจสอบตามห้วงระยะเวลา เพื่อค้นหาข้อบกพร่องและสั่งการตามความเห็นสมควร

๔๓. มาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่

ให้ส่วนราชการจัดให้มีการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้เหมาะสม โดยพิจารณาใช้มาตรการดังต่อไปนี้

### ๔๓.๑ เครื่องกีดขวาง

เครื่องกีดขวาง คือ เครื่องมือที่ใช้ป้องกัน ชัดขวาง หรือหน่วงเหนี่ยวบุคคล สัตว์หรือยานพาหนะที่ไม่มีสิทธิเข้าไปในพื้นที่รักษาความปลอดภัย โดยใช้เครื่องกีดขวางเป็นแนวเขตของพื้นที่ก่อให้เกิดภาพทางจิตวิทยา และทางวัตถุ ทำให้ไม่กล้าเข้า หรือหน่วงเหนี่ยวการล่งล่าเพื่อให้ยามรักษาการณ์มีโอกาสตรวจพบ หยุดยั้ง หรือจับกุมได้ อีกทั้งเป็นการประหยัดจำนวนเจ้าหน้าที่ยามรักษาการณ์ และเป็นการบังคับให้บุคคลหรือยานพาหนะที่จะผ่านเข้าออก ต้องผ่านเฉพาะตามทางเข้าออกที่กำหนดให้ เพื่อสะดวกในการควบคุมและตรวจสอบ

เครื่องกีดขวางโดยทั่วไปแบ่งเป็น ๒ ชนิด คือ

๔๓.๑.๑ เครื่องกีดขวางตามธรรมชาติ เช่น ทะเล แม่น้ำ ลำคลอง หน้าผา ฯลฯ ที่ได้ดัดแปลงให้เป็นประโยชน์ในการกั้น

๔๓.๑.๒ เครื่องกีดขวางที่ประดิษฐ์ขึ้น เช่น รั้วทึบ รั้วโปร่ง เครื่องกั้น ถนน ลวดทึบเพลง กำแพง ลูกกรง เหล็ก ฯลฯ

### ๔๓.๒ การให้แสงสว่าง

การให้แสงสว่างก็เพื่อจะให้มองเห็นบริเวณรั้วและเขตหวงห้ามต่าง ๆ โดยชัดเจนในเวลามืด จะได้มองเห็นผู้ที่บุกรุกเข้ามาในสถานที่ การให้แสงสว่างมี ๒ วิธี คือ

๔๓.๒.๑ การใช้แสงส่องโดยตรง คือ การพุ่งแสงสว่างส่องไปยังจุดใดจุดหนึ่งที่ต้องการ เช่น ที่ตัวอาคาร รั้ว หรือประตู เป็นต้น

๔๓.๒.๒ การใช้แสงส่องกระจายรอบตัว ทำให้มีความสว่างทั่วบริเวณ ดวงไฟควรอยู่ในระดับสูงพอที่จะช่วยให้มองเห็นเครื่องกีดขวางต่าง ๆ ได้ชัดเจน ในกรณีที่รั้วเป็นแบบทึบก็ควรให้มีแสงสว่างส่องให้เห็นได้ทั้งสองด้าน และต้องให้รั้วมีแสงสว่างของดวงหนึ่ง ๆ ทับเลยเข้าไปในรั้วของดวงข้างเคียงเพื่อมิให้มีพื้นที่อับแสงระหว่างรั้วมีดวงไฟ

### ๔๓.๓ เจ้าหน้าที่รักษาความปลอดภัยสถานที่

เจ้าหน้าที่รักษาความปลอดภัยสถานที่ คือ เจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบในการรักษาความปลอดภัย ประกอบด้วยเจ้าหน้าที่เวรรักษาความปลอดภัยประจำวัน ยามรักษาการณ์และเจ้าหน้าที่อื่น

เจ้าหน้าที่รักษาความปลอดภัยสถานที่จัดขึ้นด้วยความมุ่งหมายเพื่อให้การรักษาความปลอดภัยเกี่ยวกับสถานที่มีประสิทธิภาพยิ่งขึ้น เพราะไม่ว่าจะมีเครื่องกีดขวางชนิดใดหากไม่มีการเฝ้ารักษาแล้ว ก็อาจมีการเล็ดลอดเข้าไปได้

#### ๔๓.๓.๑ หน้าที่

เจ้าหน้าที่เวรรักษาความปลอดภัยประจำวันมีหน้าที่กำกับดูแลการปฏิบัติของยามรักษาการณ์และเจ้าหน้าที่อื่นที่ได้รับมอบหมายจากหัวหน้าส่วนราชการนั้น ๆ ยามรักษาการณ์มีหน้าที่ป้องกันบริเวณเขตหวงห้ามทั้งหมดตลอดจนวัสดุและสิ่งอุปกรณ์ทั้งปวง ทำการตรวจสอบบุคคล ยานพาหนะและสิ่งของต่าง ๆ โดยเฉพาะเกี่ยวกับการป้องกันอัคคีภัย อุบัติเหตุและภัยอันตรายอื่น ๆ

#### ๔๓.๓.๒ จำนวน

การกำหนดจำนวนเจ้าหน้าที่รักษาความปลอดภัยสถานที่ให้พิจารณาปัจจัยดังต่อไปนี้

๔๓.๓.๒.๑ จุดอ่อนของอาคารสถานที่ต่าง ๆ

๔๓.๓.๒.๒ จำนวนช่องทางเข้าออก

๔๓.๓.๒.๓ ลักษณะของงานและทรัพย์สินที่พึงได้รับการพิทักษ์รักษา

๔๓.๓.๒.๔ จำนวนผู้เยี่ยมชม

๔๓.๓.๒.๕ จำนวนบริเวณเขตหวงห้าม

๔๓.๓.๒.๖ จำนวนยานพาหนะที่ผ่านเข้าออก

๔๓.๓.๒.๗ จำนวนเจ้าหน้าที่ในส่วนราชการนั้น ๆ

๔๓.๓.๒.๘ เวลาพักผ่อนของเจ้าหน้าที่รักษาความปลอดภัย

๔๓.๓.๓ ที่ตั้ง

ที่ทำการของเจ้าหน้าที่รักษาความปลอดภัยสถานที่ ควรตั้งอยู่ในบริเวณที่สามารถปฏิบัติหน้าที่ได้สะดวก ภายในที่ตั้งควรมีที่เก็บอาวุธ เครื่องมือเครื่องใช้และเครื่องมือสื่อสาร ในที่ตั้งจะต้องมีเจ้าหน้าที่รักษาความปลอดภัยสถานที่ประจำอยู่อย่างน้อยหนึ่งคนตลอดเวลา

๔๓.๓.๔ การติดต่อสื่อสาร

ในกรณีที่มียามรักษาการณ์ ควรมีโทรศัพท์ตั้งไว้ ณ จุดอันเหมาะสมที่สุดในเส้นทางของยามรักษาการณ์ และควรกำหนดประมวลลับสำหรับใช้พิสูจน์ฝ่ายระหว่างกันขึ้น ยามรักษาการณ์จะต้องรายงานตรงตามกำหนดเวลาเสมอด้วย นอกจากโทรศัพท์ควรถูกกำหนดวิธีการหรือเครื่องมือสื่อสารอื่นสำรองไว้ในกรณีที่โทรศัพท์ขัดข้อง

๔๓.๓.๕ ระบบสัญญาณแจ้งภัย

ระบบสัญญาณแจ้งภัย คือ วิธีการใช้เครื่องมือทางเทคนิคสำหรับตรวจและแจ้งให้ทราบ ในเมื่อมีการเข้าใกล้หรือการล่วงล้ำเข้ามาในพื้นที่รักษาความปลอดภัย ระบบสัญญาณแจ้งภัยนี้อาจเป็นเครื่องมือเทคนิคทางอิเล็กทรอนิกส์ ทางไฟฟ้า หรือทางเครื่องกล เช่น แผ่นโลหะ เส้นลวด คลื่นแสง คลื่นเสียง กัดัก เป็นต้น ที่จะทำให้เกิดสัญญาณเมื่อมีผู้บุกรุก โดยใช้ติดกับประตู หน้าต่าง ตู้เก็บเอกสาร ห้องนิรภัย กำแพง รั้ว พื้น ฯลฯ

๔๓.๓.๖ การฝึกอบรม

เจ้าหน้าที่รักษาความปลอดภัยสถานที่ควรได้รับการฝึกอบรมและมีความรู้ในเรื่องต่าง ๆ ดังนี้

๔๓.๓.๖.๑ การป้องกันการจลาจลและการก่อวินาศกรรม

๔๓.๓.๖.๒ บริเวณสถานที่ทั้งหมด จุดสำคัญของสถานที่นั้น รวมทั้งที่ตั้งสวิทซ์ไฟฟ้าที่สำคัญ ๆ เครื่องมือเครื่องใช้ในการดับเพลิง ตลอดจนรถยนต์ต่าง ๆ ที่อาจเกิดขึ้นแก่สถานที่ราชการนั้น ๆ

๔๓.๓.๖.๓ การติดต่อสื่อสารในหน่วยรักษาความปลอดภัย

๔๓.๓.๖.๔ วิธีต่อสู้ป้องกันตัวตามความเหมาะสม

๔๓.๓.๖.๕ ระบบที่ใช้สำหรับแสดงตนซึ่งสถานที่นั้นได้กำหนดไว้

๔๓.๓.๗ เครื่องแบบและอาวุธของยามรักษาการณ์

ยามรักษาการณ์ควรแต่งเครื่องแบบ และในขณะที่ปฏิบัติหน้าที่ถ้ามีอาวุธก็ต้องเป็นอาวุธที่ถูกต้องตามกฎหมาย พร้อมทั้งมีความรู้ความสามารถในเรื่องการใช้อาวุธเป็นอย่างดี

๔๓.๔ การควบคุมบุคคลและยานพาหนะ

๔๓.๔.๑ การควบคุมบุคคล พึงปฏิบัติดังต่อไปนี้

๔๓.๔.๑.๑ จัดให้มีบัตรผ่านสำหรับบุคคลภายในเพื่อใช้แสดงว่าเป็นผู้ที่ได้รับอนุญาตให้ผ่านเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัยได้ การออกแบบบัตรผ่านควรมีลักษณะมิให้ปลอมแปลง

ได้ง่าย และควรเปลี่ยนรูปแบบตามห้วงระยะเวลาที่เห็นสมควร อย่างน้อยให้มีรายละเอียดแสดงชื่อส่วนราชการ ชื่อ รูปภาพ ส่วนสูง น้ำหนัก และลายมือชื่อของผู้ถือบัตร ลายมือชื่อผู้ออกบัตร หมายเลขประจำบัตร วัน เดือนปีที่ออกบัตร วันเดือนปีที่บัตรหมดอายุ กับจะต้องควบคุมการจัดทำและการจ่ายบัตรโดยกวดขัน

๔๓.๔.๑.๒ จัดให้มีป้ายแสดงตนสำหรับบุคคลภายในและภายนอก เพื่อแสดงว่าเป็นบุคคลที่ได้รับอนุญาตให้เข้าไปในพื้นที่ใดได้ในฐานะอะไร ก่อนที่บุคคลดังกล่าวจะเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัยของส่วนราชการนั้น ๆ ให้ติดป้ายแสดงตนไว้ในที่ที่เห็นได้ชัด เช่น ทอกเสื้อ เป็นต้น

๔๓.๔.๑.๓ จัดให้มีการบันทึกหลักฐานสำหรับบุคคลภายนอก เช่น ผู้มา ประชุม ติดต่อกับ หรือเยี่ยม ตลอดจนช่างก่อสร้าง ช่อมแซม ผู้นำส่งหรือรับสิ่งของจากส่วนราชการหรือหน่วยงาน เป็นต้น โดยให้มีรายละเอียด คือ วันและเวลาที่ผ่านเข้า ชื่อ สัญชาติ ตำบลที่อยู่ ชื่อสถานที่ทำงาน ชื่อและหน่วยงานของผู้รับการติดต่อหรือเยี่ยม เหตุผลที่มาติดต่อหรือเยี่ยม วันและเวลาที่กลับออกไป ฯลฯ

ในกรณีที่มีการก่อสร้าง ช่อมแซม หรือรับส่งสิ่งของจากส่วนราชการ หรือหน่วยงาน ให้หัวหน้าส่วนราชการหรือหน่วยงานนั้นวางมาตรการควบคุมโดยใกล้ชิดตลอดเวลา

๔๓.๔.๑.๔ จัดให้มีที่พักรับผู้มาติดต่อหรือเยี่ยมไว้เป็นพิเศษต่างหาก ไม่ควรอนุญาตให้ผู้มาเยี่ยมเข้าไปยังที่ทำงาน นอกจากบุคคลที่มาติดต่อราชการที่เกี่ยวข้องโดยแท้จริง ในการนี้ผู้รับการเยี่ยมจะต้องรับผิดชอบในตัวผู้เยี่ยมตลอดเวลาตั้งแต่รับตัวมาจากเจ้าหน้าที่รักษาความปลอดภัยสถานที่จนถึงตัวคืน สำหรับคนรถของผู้มาติดต่อหรือเยี่ยมหรือผู้ที่โดยสารมาด้วย คงให้รออยู่ ณ บริเวณที่จอดรถ

๔๓.๔.๒ การควบคุมยานพาหนะ พึงปฏิบัติดังต่อไปนี้

๔๓.๔.๒.๑ มีเจ้าหน้าที่ตรวจสอบยานพาหนะประจำอยู่ที่ช่องทางเข้าออกของสถานที่ตั้ง ทำหน้าที่ตรวจสอบบุคคลและสิ่งของต่าง ๆ บนยานพาหนะและควบคุมบรรดาคนยานพาหนะที่อนุญาตให้ผ่านเข้าไปในสถานที่ตั้งนั้น โดยให้ใช้เส้นทางและที่จอดรถที่อนุญาตเท่านั้น

๔๓.๔.๒.๒ ทำบันทึกหลักฐานยานพาหนะเข้าออกตามหัวข้อเหล่านี้ คือ

๔๓.๔.๒.๒.๑ วันและเวลาที่ยานพาหนะผ่านเข้า

๔๓.๔.๒.๒.๒ ชื่อคนขับและชื่อผู้โดยสาร

๔๓.๔.๒.๒.๓ เลขทะเบียนยานพาหนะ

๔๓.๔.๒.๒.๔ ลักษณะและจำนวนสิ่งของที่บรรทุกยานพาหนะที่

นำเข้าและนำออก

๔๓.๔.๒.๒.๕ วัตถุประสงค์และสถานที่ที่ยานพาหนะจะเข้าไป

๔๓.๔.๒.๒.๖ วันและเวลาที่ยานพาหนะผ่านออก

๔๓.๔.๒.๓ จัดที่จอดรถให้อยู่ห่างจากตัวอาคารที่สำคัญและ/หรือสิ่งของที่ติดเพลิงง่ายประมาณไม่น้อยกว่า ๖ เมตร

๔๓.๕ พื้นที่ที่มีการรักษาความปลอดภัย

พื้นที่ที่มีการรักษาความปลอดภัย คือ พื้นที่ที่มีการกำหนดขอบเขตโดยแนชด ซึ่งมีข้อจำกัดและการควบคุมการเข้าออกเป็นพิเศษ มีความมุ่งหมายเพื่อจะพิทักษ์สิ่งที่เป็นความลับ บุคคล ทรัพย์สิน วัสดุและสิ่งอุปกรณ์ของทางราชการให้ปลอดภัย โดยกำหนดมาตรการการรักษาความปลอดภัยในแต่ละเขตให้มีระดับแตกต่างกันตามความสำคัญ

การกำหนดพื้นที่ที่มีการรักษาความปลอดภัย พึงปฏิบัติดังต่อไปนี้

๔๓.๕.๑ กำหนดให้มี “พื้นที่ควบคุม” ซึ่งเป็นพื้นที่ที่อยู่ติดต่อกับหรือที่อยู่โดยรอบ “พื้นที่หวงห้าม” ภายในเขต “พื้นที่ควบคุม” นี้ต้องมีระเบียบการควบคุมบุคคลและยานพาหนะเพื่อช่วยกั้นกรองเสียชั้นหนึ่งก่อนที่จะให้เข้าถึง “พื้นที่หวงห้าม”

๔๓.๕.๒ กำหนดให้มี “พื้นที่หวงห้าม” ซึ่งเป็นพื้นที่ที่มีการพิทักษ์รักษาสิ่งที่เป็นความลับ ตลอดจนบุคคลสำคัญ ทรัพย์สินหรือวัสดุที่สำคัญของทางราชการ “พื้นที่หวงห้าม” นี้อาจแยกออกเป็น “เขตหวงห้ามเฉพาะ” กับ “เขตหวงห้ามเด็ดขาด”

“เขตหวงห้ามเฉพาะ” คือ เขตพื้นที่ซึ่งมีสิ่งที่เป็นความลับตลอดจนบุคคลหรือสิ่งที่มีความสำคัญ ซึ่งจะต้องพิทักษ์รักษาและการเข้าไปในเขตพื้นที่นี้โดยปราศจากการควบคุม อาจทำให้สามารถเข้าถึงความลับ บุคคล และสิ่งอุปกรณ์สำคัญดังกล่าว บุคคลที่ได้รับอนุญาตให้เข้าไปใน “เขตหวงห้ามเฉพาะ” จะต้องได้รับความไว้วางใจตามชั้นความลับที่เหมาะสมกับ “เขตหวงห้ามเฉพาะ” นั้น ๆ หรือมิฉะนั้นก็ต้องจัดเจ้าหน้าที่ควบคุม และกำหนดระเบียบการควบคุมภายในชั้น ตัวอย่าง “เขตหวงห้ามเฉพาะ” เช่น ที่เก็บอาวุธ ที่เก็บเชื้อเพลิง ขุมสายโทรศัพท์ กองบังคับการของทหาร และห้องปฏิบัติการลับ ห้องปฏิบัติงานของหัวหน้าส่วนราชการที่เห็นสมควร เป็นต้น

“เขตหวงห้ามเด็ดขาด” คือ เขตพื้นที่ซึ่งมีสิ่งที่เป็นความลับตลอดจนบุคคลหรือสิ่งที่มีความสำคัญยิ่ง ซึ่งจะต้องพิทักษ์รักษา การเข้าไปในเขตพื้นที่นี้อาจทำให้สามารถเข้าถึงความลับบุคคลและสิ่งที่มีความสำคัญยิ่งในการรักษาความปลอดภัยดังกล่าวโดยตรง บุคคลที่ได้รับอนุญาตให้เข้าไปใน “เขตหวงห้ามเด็ดขาด” จะต้องได้รับความไว้วางใจตามชั้นความลับที่เหมาะสมกับ “เขตหวงห้ามเด็ดขาด” นั้น ๆ เท่านั้น ตัวอย่าง “เขตหวงห้ามเด็ดขาด” เช่น ศูนย์ปฏิบัติการสื่อสาร ห้องปฏิบัติการลับ ห้องปฏิบัติงานของผู้บังคับบัญชาชั้นสูง ห้องหรือสถานที่ขณะที่ใช้ในการประชุมลับและห้องนิรภัย เป็นต้น

#### ๔๓.๖ การป้องกันอัคคีภัย

##### ๔๓.๖.๑ การวางมาตรการการป้องกันอัคคีภัย

ให้หัวหน้าส่วนราชการกำหนดมาตรการการป้องกันอัคคีภัย โดยมีเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยเป็นผู้วางแผนและกำกับดูแลให้เป็นไปตามกฎหมายว่าด้วยกาป้องกันและระงับอัคคีภัย กฎกระทรวง แลมติคณะรัฐมนตรี ตลอดจนคำสั่งของทางราชการต่าง ๆ ที่เกี่ยวกับเรื่องนี้

##### ๔๓.๖.๒ เจ้าหน้าที่ดับเพลิง

ในเวลาราชการให้จัดข้าราชการเป็นเจ้าหน้าที่ดับเพลิง โดยแบ่งเป็นสองกลุ่ม คือ กลุ่มที่หนึ่งมีหน้าที่ดับเพลิง และอีกกลุ่มหนึ่งมีหน้าที่ขนย้ายเอกสารและควบคุมรับผิดชอบเอกสารและวัสดุ โดยให้แต่ละกลุ่มมีจำนวนเพียงพอสำหรับงานนั้น ๆ สำหรับนอกเวลาราชการให้เป็นหน้าที่ของเจ้าหน้าที่เวรรักษาความปลอดภัยประจำวัน และยามรักษาการณ์เป็นผู้รับผิดชอบ

##### ๔๓.๖.๓ การจัดเตรียมเครื่องอุปกรณ์ในการดับเพลิง

ให้มีสัญญาณแจ้งเหตุเพลิงไหม้ติดตั้งไว้ และเตรียมเครื่องมือเครื่องใช้ในการดับเพลิงขั้นต้นไว้ให้พร้อม เช่น น้ำ ทราบาย กระจบองน้ำ เชือก บันได ขวาน ไม้มือเสือ ตลอดจนเครื่องดับเพลิงให้เหมาะกับประเภทสื่อที่ทำให้เกิดเพลิงไหม้ไว้ทุกประเภท สำหรับเครื่องดับเพลิงเคมีให้ติดตั้งไว้ในที่ที่หยิบฉวยใช้งานได้ง่ายและมีจำนวนเพียงพอ โดยหมั่นตรวจสอบให้อยู่ในสภาพที่ใช้การได้อยู่เสมอ และแจ้งให้ทุกคนรู้แหล่งน้ำสำหรับใช้ดับเพลิงที่ใกล้ที่สุด ที่ตั้งและหมายเลขโทรศัพท์ของหน่วยดับเพลิงที่ติดต่อได้สะดวกและรวดเร็วที่สุด

## ๔๓.๖.๔ การฝึกอบรม

ให้อบรมเจ้าหน้าที่ให้มีความระมัดระวังเพื่อป้องกันอัคคีภัยและฝึกซ้อมให้มีความรู้ความชำนาญในการดับเพลิงขั้นต้น เจ้าหน้าที่ควรมีความรู้ในเรื่องต่าง ๆ เหล่านี้ คือ

๔๓.๖.๔.๑ ประเภทของไฟ

๔๓.๖.๔.๒ เครื่องมือเครื่องใช้ในการดับเพลิง

๔๓.๖.๔.๓ การติดต่อสื่อสาร การคมนาคม แผนผังอาคารและบริเวณโดยรอบ

๔๓.๖.๔.๔ ที่ตั้งและหมายเลขโทรศัพท์ของหน่วยดับเพลิง

๔๓.๖.๔.๕ แผนการดับเพลิงของส่วนราชการ

## ๔๔. การวางแผนรักษาความปลอดภัยเกี่ยวกับสถานที่

ในการวางแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ ต้องพิจารณาจากผลของการประมาณการและ/หรือข้อมูลตามหัวข้อดังต่อไปนี้เป็นหลัก คือ

๔๔.๑ สถานการณ์โดยทั่วไปและสภาพแวดล้อมโดยรอบพื้นที่

๔๔.๒ ข่าวดสาร สิ่งบอกเหตุ และการเตือนภัย

๔๔.๓ ภารกิจและหน้าที่ของหน่วยงาน

๔๔.๕ จำนวนเจ้าหน้าที่ที่ปฏิบัติงานและเจ้าหน้าที่รักษาความปลอดภัย

๔๔.๖ งบประมาณที่จะใช้ในการวางมาตรการการรักษาความปลอดภัย

๔๔.๗ การสนับสนุนจากหน่วยเหนือและหน่วยงานอื่น ๆ

๔๔.๘ การติดต่อสื่อสารภายในหน่วยกับหน่วยเหนือและหน่วยงานอื่น ๆ

๔๔.๙ รายงานการสำรวจหรือการตรวจสอบการรักษาความปลอดภัย

## การประสานงานกับหน่วยงานที่เกี่ยวข้องเมื่อเผชิญเหตุ

### หน่วยงาน : สำนักงานจังหวัดนครราชสีมา

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๖๔ ๒๖๑๗ - ๑๙  
 โทรศัพท์มือถือ : -  
 โทรสาร : ๐ ๗๓๖๔ ๒๖๑๗ - ๑๙  
 คลื่นความถี่วิทยุ : -

### หน่วยงาน : สถานีดับเพลิง

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๕๑ ๑๐๖๔ , ๐ ๗๓๕๑๕๗๗๕  
 โทรศัพท์มือถือ : -  
 โทรสาร : -  
 คลื่นความถี่วิทยุ : ๑๖๒.๕๕๐ MHz

### หน่วยงาน : ตำรวจภูธร อ.เมือง

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๕๑ ๑๔๑๖  
 โทรศัพท์มือถือ : -  
 โทรสาร : ๐ ๗๓๕๑ ๕๗๘๒  
 คลื่นความถี่วิทยุ : ๑๕๓.๔๕๐ MHz

### หน่วยงาน : หน่วยกู้ภัย นครา ๐๑

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๕๑ ๖๒๙๐  
 โทรศัพท์มือถือ : -  
 โทรสาร : ๐ ๗๓๕๑๖๒๙๐  
 คลื่นความถี่วิทยุ : ๑๖๘.๓๗๕ MHz



**หน่วยงาน : ศูนย์ประสานงานเหตุฉุกเฉิน จังหวัดนราธิวาส**

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๖๔ ๒๖๕๙ , ๑๘๘๑  
 โทรศัพท์มือถือ : -  
 โทรสาร : ๐ ๗๓๖๔ ๒๖๕๙  
 คลื่นความถี่วิทยุ : -

**หน่วยงาน : ศูนย์สั่งการนราธิวาส (โรงพยาบาลนราธิวาส)**

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๑๖๖๙  
 โทรศัพท์มือถือ : -  
 โทรสาร : -  
 คลื่นความถี่วิทยุ : ๑๕๕.๗๒๕ MHz

**หน่วยงาน : มุลนิธิเมตารธรรม นราธิวาส**

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๕๑ ๑๖๗๖  
 โทรศัพท์มือถือ : -  
 โทรสาร : ๐ ๗๓๕๑ ๑๖๗๖  
 คลื่นความถี่วิทยุ : ๑๔๗.๓๕๐ MHz

**หน่วยงาน : สำนักงาน การไฟฟ้า นราธิวาส**

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๕๓ ๒๓๐๕  
 โทรศัพท์มือถือ : -  
 โทรสาร : -  
 คลื่นความถี่วิทยุ : -

**หน่วยงาน : สำนักงาน ประปา จังหวัดนราธิวาส**

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๕๓ ๒๑๔๓  
 โทรศัพท์มือถือ : -  
 โทรสาร : ๐ ๗๓๕๓ ๒๑๔๓  
 คลื่นความถี่วิทยุ : -

**หน่วยงาน : ที่ว่าการอำเภอเมือง**

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๕๑ ๑๐๑๒  
 โทรศัพท์มือถือ : -  
 โทรสาร : ๐ ๗๓๕๑ ๑๐๑๒  
 คลื่นความถี่วิทยุ : ๑๕๕.๗๒๕ MHz

**หน่วยงาน : ป้องกันภัยฝ่ายพลเรือน**

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๕๓ ๒๒๑๐ - ๒  
 โทรศัพท์มือถือ : -  
 โทรสาร : ๐ ๗๓๕๓ ๒๑๓๔  
 คลื่นความถี่วิทยุ : ๑๕๓.๔๕๐ MHz

**หน่วยงาน : หน่วยกู้ภัยตำรวจทางหลวง**

ชื่อผู้ติดต่อ : ( สำนักงาน )  
 โทรศัพท์ : ๐ ๗๓๔๖ ๘๐๙๙  
 โทรศัพท์มือถือ : -  
 โทรสาร : ๐ ๗๓๔๖ ๘๐๙๙  
 คลื่นความถี่วิทยุ : ๑๕๒.๔๐๐ MHz

ตารางการสำรองฐานข้อมูล  
จังหวัดนราธิวาส

## ตารางการสำรองฐานข้อมูลจังหวัดนราธิวาส

ที่	ครั้งที่	ชื่อเครื่อง	ชนิดข้อมูล / ชื่อฐานข้อมูล	สถานที่จัดเก็บ ข้อมูล	วัน/เดือน/ ปี	ผู้จัดเก็บ	ผู้ตรวจสอบ

ที่	ครั้งที่	ชื่อเครื่อง	ชนิดข้อมูล / ชื่อฐานข้อมูล	สถานที่จัดเก็บ ข้อมูล	วัน/เดือน/ ปี	ผู้จัดเก็บ	ผู้ตรวจสอบ