<u>แบบสอบถามการปฏิบัติงานของหน่วยงานตามแนวนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมปศุสัตว์</u>

โปรดทำเครื่องหมาย ✓ ประเมินผลการปฏิบัติงานของหน่วยงานตามรายการต่อไปนี้ พร้อมทั้งระบุเอกสารอ้างอิง

กรณีไม่มี/ไม่ใช่ โปรดระบุรายละเอียดว่าได้มีการดำเนินการอย่างไรในช่อง "ICT ดำเนินการอย่างไร"

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	**มี/ใช่**	**ไม่มี / ไม่ใช่**		
1.	***นโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายใน กรมปศุสัตว์***				
	1.1 มีเอกสารและมีการประกาศใช้นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่าง<u>เป็นลายลักษณ์อักษร</u> โดยกำหนดหลักการ วัตถุประสงค์ และเป้าหมาย รวมทั้งข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยอย่างชัดเจน				
	1.2 นโยบาย<u>มีเนื้อหาครอบคลุม</u> ถึง การควบคุมการเข้าถึง การควบคุมการใช้งานสารสนเทศ ระบบสำรองของสารสนเทศ แผนเตรียมความพร้อมกรณีฉุกเฉิน การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ และการทบทวนนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ				
	1.3 ศูนย์ ICT มีการ<u>เผยแพร่ประชาสัมพันธ์และสื่อสารผ่านช่องทางต่างๆที่กรมปศุสัตว์กำหนด เพื่อให้ความรู้ สร้างความเข้าใจ</u> เกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยกับ<u>บุคลากรภายในกรมปศุสัตว์</u> ให้รับทราบหลักเกณฑ์ วิธีการ ขั้นตอนและให้ถือปฏิบัติตามกฎ ระเบียบ ข้อบังคับ ที่เกี่ยวข้องเป็นประจำทุกปี				
	1.4 ศูนย์ ICT มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีการจัดทำแผนการลดความเสี่ยง เสนอผู้มีอำนาจอนุมัติให้ดำเนินการตามแผนและรายงานผลการดำเนินการให้ผู้บังคับบัญชาทราบอย่างสม่ำเสมอทุกปี				
	1.5 ศูนย์ ICT ได้รับการตรวจสอบโดยผู้ตรวจสอบภายใน (Internal Auditor) หรือโดยผู้ตรวจสอบภายนอก (External Auditor) ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบระหว่างผู้ตรวจสอบกับผู้รับตรวจเป็นประจำทุกปี				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	**มี/ใช่**	**ไม่มี / ไม่ใช่**		
	1.6 กรณีมีการจ้างเหมาบริการเกี่ยวกับการปฏิบัติงานด้านสารสนเทศ ศูนย์ ICT ได้กำหนดเจ้าหน้าที่เพื่อควบคุมดูแล ตรวจสอบการให้บริการของผู้ให้บริการภายนอกที่ดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมปศุสัตว์ให้ดำเนินการตามเงื่อนไขของสัญญาจ้างอย่างเคร่งครัด				
2	***การบริหารจัดการสินทรัพย์ด้านสารสนเทศของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ICT)***				
	2.1 ศูนย์ ICT มีการมอบหมายแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบด้านความรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและสินทรัพย์ด้านสารสนเทศ โดยกำหนดเป็นลายลักษณ์อักษร และมีการกำหนดเจ้าหน้าที่สำรองในการปฏิบัติหน้าที่แทนกรณีเจ้าหน้าที่หลักไม่สามารถปฏิบัติงานได้				
	2.2 ศูนย์ ICT มีการบริหารจัดการและมีขั้นตอนกระบวนการในการควบคุมดูแลการใช้งานอุปกรณ์ด้านเทคโนโลยีสารสนเทศ โดย 2.2.1 มีการจัดทำทะเบียนทรัพย์สิน ทั้งครุภัณฑ์ โปรแกรม วัสดุด้านสารสนเทศต่างๆอย่างครบถ้วน และมีบันทึกควบคุมการรับและเบิกจ่ายแยกตามชนิดประเภทไวอย่างครบถวนถูกตองเปนปจจุบันสามารถตรวจสอบได้				
	2.2.2 ระบุขอบเขตเครือข่ายบริการที่สำคัญและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรง				
	2.2.3 กรณีมีการเปลี่ยนแปลง ได้ปรับปรุงทะเบียนทรัพย์สินให้เป็นปัจจุบันและมีการตรวจสอบทะเบียนทรัพย์สินเป็นประจำทุกปี				
	2.3 มีการแยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไปโดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้ เช่น Router, Switch และ Server ต่างๆ มีการจัดเก็บอุปกรณ์ต่างๆ ในที่ที่เหมาะสม เพื่อสะดวกในการบำรุงรักษา และไม่วางอุปกรณ์ต่างๆ ในตำแหน่งใกล้ประตูหน้าต่าง เพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น				
	2.4 ในการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ได้มีการกำหนดขั้นตอนการรักษาความมั่นคงปลอดภัย (Secure areas) เช่น ห้องควบคุมคอมพิวเตอร์แม่ข่าย (Server Room) ครุภัณฑ์ วัสดุอุปกรณ์สารสนเทศต่างๆ				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	มี/ใช่	ไม่มี / ไม่ใช่		
	2.5 กรณีสถานที่ เช่น ห้องควบคุมคอมพิวเตอร์แม่ข่าย (Server Room) 2.5.1 ผู้เข้าใช้งานต้องเป็นผู้ที่ได้รับสิทธิ์การเข้าใช้งานพื้นที่เท่านั้น				
	2.5.2 มีระบบยืนยันตัวตน/ยืนยันสิทธิก่อนเข้าใช้งาน				
	2.5.3 ติดตั้งกล้องวงจรปิดเพื่อติดตาม/เฝ้าระวังการเข้าพื้นที่ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์				
	2.5.4 มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบดูแลรักษาห้องควบคุมแม่ค่ายอย่างเป็นลายลักษณ์อักษร				
	2.5.5 ในช่วง 1 ปี ที่ผ่านมาห้องควบคุมคอมพิวเตอร์แม่ข่ายเคยถูกน้ำท่วม ไฟไหม้ ระบบไฟฟ้าขัดข้องหรือถูกโจรกรรมข้อมูลหรือไม่				
	2.6 กรณีครุภัณฑ์สารสนเทศ 2.6.1 เจ้าหน้าที่พัสดุมีทะเบียนบัญชีพัสดุครุภัณฑ์และเอกสารที่เกี่ยวข้องครบถ้วนสามารถตรวจสอบได้				
	2.6.2 ครุภัณฑ์ ได้ปิดรหัสทรัพย์สินที่ตัวครุภัณฑ์ชัดเจน				
	2.6.3 มีการจัดวางครุภัณฑ์ในที่ปลอดภัย ไม่เสี่ยงต่อการสูญเสีย/สูญหาย				
	2.6.4 กรณีครุภัณฑ์ชำรุดเสียหาย เจ้าหน้าที่มีการบันทึกประวัติการซ่อม เพื่อตรวจสอบและขออนุมัติซ่อมตามระเบียบ				
	2.7 กรณีวัสดุอุปกรณ์สารสนเทศ 2.7.1 เจ้าหน้าที่พัสดุมีทะเบียนคุมการรับ-จ่ายวัสดุ และเอกสารที่เกี่ยวข้องครบถ้วนสามารถตรวจสอบได้				
	2.7.2 มีการจัดเก็บวัสดุอุปกรณ์ไว้ในที่ที่ปลอดภัย				
	2.7.3 มีการแบ่งแยกหน้าที่กันระหว่างเจ้าหน้าที่รับวัสดุ และจ่ายวัสดุเป็นคนละคนกันเพื่อสามารถตรวจสอบซึ่งกันและกันได้				
	2.7.4 การอนุมัติเบิก-จ่ายวัสดุ มีผู้ขอเบิก ผู้จ่าย ผู้อนุมัติถูกต้องครบถ้วนสามารถตรวจสอบได้				
	2.8 ในการสร้างความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security) ศูนย์ ICT มีการจัดวางและมีระบบการป้องกันอุปกรณ์ที่ใช้สนับสนุนในการปฏิบัติงานประเภท UPS อุปกรณ์สำรองข้อมูล อุปกรณ์สำรองไฟฟ้าและอื่นๆ				
	2.9 ศูนย์ ICT มีการเดินสายไฟฟ้า สายสัญญาณสื่อสารและสายเคเบิ้ลอื่นๆ ที่ใช้ภายในห้องควบคุมและสำนักงาน อย่างเรียบร้อยปลอดภัย				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	มี/ใช่	ไม่มี / ไม่ใช่		
	2.10 ศูนย์ ICT มีการจัดสรรเครื่องคอมพิวเตอร์และอุปกรณ์ที่มีประสิทธิภาพไว้สำหรับการปฏิบัติงาน รวมถึงจัดระบบสนับสนุนการทำงานที่เพียงพอ เช่น ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบระงับเพลิง ระบบปรับอากาศและควบคุมความชื้น ระบบแจ้งเตือนกรณีเครื่องทำงานผิดปกติหรือหยุดการทำงาน				
	2.11 ศูนย์ ICT มีการตรวจสอบ ควบคุมและบำรุงรักษา เครื่องคอมพิวเตอร์ โปรแกรม และอุปกรณ์สารสนเทศต่างๆ อย่างสม่ำเสมอ 2.11.1 มีคำสั่งหรือการมอบหมายหน้าที่และกำหนดผู้รับผิดชอบเพื่อบันทึกควบคุมวัสดุ ดูแลรักษา การตรวจสอบ การอนุมัติรายการเบิก ไว้ชัดเจนเป็นลายลักษณอักษร				
	2.11.2 การเบิกจ่ายวัสดุ-ครุภัณฑ์ทุกครั้ง เจ้าหน้าที่ได้ตรวจสอบความถูกต้องของรายการกับหลักฐานใบเบิกวัสดุ และได้บันทึกรายการจ่ายในบัญชีคุมทุกครั้ง โดยใบเบิกวัสดุ ผู้ขอเบิก ผู้อนุมัติ และผู้จ่ายได้ลงนามไว้อย่างครบถ้วนถูกต้อง				
	2.11.3 การยืม/ใหยืมวัสดุ-ครุภัณฑ์ เป็นไปตามระเบียบการจัดซื้อจัดจ้างฯ ส่วนที่ 2 เรื่องการยืม และจัดเก็บหลักฐานการรับมอบส่งมอบไว้ครบถ้วนสามารถตรวจสอบได้				
	2.11.4 การรับโอนวัสดุ-ครุภัณฑ์หรือการโอนวัสดุ-ครุภัณฑ์ให้หน่วยงานอื่นศูนย์ ICT ได้บันทึกรายการโอนวัสดุในระบบ GFMIS อย่างถูกต้อง และได้จัดทำหลักฐานการรับมอบ ส่งมอบทุกครั้ง และจัดเก็บหลักฐานที่เกี่ยวข้องไว้ครบถ้วน สามารถตรวจสอบได้				
	2.11.5 ศูนย์ ICT ได้เก็บรักษาวัสดุ-ครุภัณฑ์ทั้งหมดอยู่ในที่ปลอดภัย ยากต่อการเข้าถึง เป็นระเบียบเรียบร้อยเสมอไม่เสี่ยงต่อการสูญหาย/เสียหาย และความชื้น				
	2.11.6 ห้องควบคุมที่ใช้สำหรับจัดเก็บแม่ข่ายและศูนย์ควบคุมต่างๆ ได้ตั้งอยู่ในที่ปลอดภัย ยากต่อการเข้าถึง การจัดวางวัสดุอุปกรณ์เป็นระเบียบเรียบร้อยเสมอไม่เสี่ยงต่อการสูญหาย/เสียหาย ไม่มีน้ำรั่ว ไฟฟ้าขัดข้องหรือการชำรุดใดๆของห้องควบคุม				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	มี/ใช่	ไม่มี / ไม่ใช่		
	2.11.7 มีการตรวจสอบความครบถ้วนถูกต้องของบัญชีคุมวัสดุ-ครุภัณฑ์ ทุกบัญชีกับหลักฐานเอกสารการรับและเบิกจ่ายที่เกี่ยวของและวัสดุ-ครุภัณฑ์ที่คงเหลือจริง เป็นประจำ				
	2.11.8 มีการแต่งตั้งคณะกรรมการตรวจสอบพัสดุประจำปี ดำเนินการตรวจสอบและรายงานผลการตรวจสอบพัสดุทั้งวัสดุและครุภัณฑ์ให้หัวหน้าส่วนราชการและหัวหน้างานพัสดุทราบโดยถูกต้องครบถ้วน ภายในระยะเวลากำหนด				
	2.11.9 กรณีพบวัสดุที่ชำรุด ศูนย์ ICT ได้ดำเนินการขออนุมัติซ่อมตามแบบฟอร์มที่กำหนดเป็นไปตามระเบียบการจัดซื้อจัดจางฯ ถูกต้องครบถ้วน สามารถตรวจสอบได้				
	2.11.10 กรณีจำหน่าย แลกเปลี่ยน โอน แปรสภาพหรือทำลาย ศูนย์ ICT ได้ดำเนินการขออนุมัติซ่อมตามแบบฟอร์มที่กำหนดเป็นไปตามระเบียบการจัดซื้อจัดจางฯ ถูกต้องครบถ้วน สามารถตรวจสอบได้				
	2.12 ศูนย์ ICT มีมาตรการควบคุมการนำสินทรัพย์ด้านสารสนเทศออกนอกหน่วยงาน และมีการตรวจสอบทะเบียนคุมสินทรัพย์และปรับปรุงทะเบียนคุมให้เป็นปัจจุจันสามารถตรวจสอบได้ โดยศูนย์ ICT มีการตรวจสอบทะเบียนคุมทรัพย์สินเป็นประจำทุกปี				
	2.10 ศูนย์ ICT มีระบบที่ใช้สำหรับตรวจสอบและควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น แล็ปท็อป พอร์ต USB เพื่อป้องกันมัลแวร์ที่จะมาพร้อมกับอุปกรณ์ดังกล่าว ก่อนการเชื่อมต่อ ศูนย์ ICT มีระบบให้ผู้ใช้งานต้องขออนุมติการเชื่อมต่อและขึ้นทะเบียนก่อนเข้าระบบเครือข่าย พร้อมทั้งมีการบันทึกข้อมูลการเข้าระบบที่สามารถตรวจสอบได้				
	2.11 ศูนย์ ICT มีระบบการควบคุมการเข้าถึงและอุปกรณ์ประมวลผลข้อมูล ซึ่งผู้ใช้งานต้องได้รับอนุญาตจากผู้ดูแลระบบและได้รับอนุญาตในการมีสิทธิ์เข้าใช้งานระบบจาก ผอ.ศูนย์ ICT เป็นลายลักษณ์อักษรเท่านั้น ซึ่งสามารถตรวจสอบได้				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	**มี/ใช่**	**ไม่มี / ไม่ใช่**		
	2.12 ศูนย์ ICT มีระบบควบคุมป้องกันอุปกรณ์ขณะที่ไม่มีผู้ใช้งานอุปกรณ์ โดยมีระบบอัตโนมัติแจ้งล็อคหน้าจอเพื่อให้เข้ารหัสใช้งานใหม่อีกครั้ง กรณีที่ไม่ได้ใช้งานเกินกว่า 30 นาที ถ้าผู้ใช้งานต้องการเข้าระบบให้ทำการใส่รหัสผ่านอีกครั้งก่อนเข้าใช้งาน ให้เป็นไปตามแนวปฏิบัติเพื่อควบคุมทรัพย์สินสารสนเทศ ไม่ให้อยู่ในภาวะเสี่ยงต่อการเข้าถึงระบบและข้อมูลโดยผู้ที่ไม่มีสิทธิ์				
	2.13 ศูนย์ ICT มีระบบควบคุมและป้องกันมิให้ผู้ใช้งานเปิดหรือใช้งาน โปรแกรมประเภท Peer-to-Peer โปรแกรมที่มีความเสี่ยง เช่น บิทเทอร์เรนท์ โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง การเผยแพร่สื่อที่ขัดต่อกฎหมายและศีลธรรม หรือใช้ระบบสารสนเทศของกรมปศุสัตว์เพื่อหาประโยชน์ทางการค้าของตน โดยศูนย์ ICT มีระบบตรวจจับและแจ้งเตือนอัตโนมัติมิให้ใช้งานโปรแกรมที่มีความเสี่ยงดังกล่าวได้				
3.	***การบริหารจัดการและการดำเนินการด้านสารสนเทศ และระบบสารสนเทศ***				
	3.1 ศูนย์ ICT มีการกำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้ **ศูนย์ ICT มีควบคุมการเข้าถึงเครือข่าย ควบคุมการเข้าถึงระบบต่างๆ ควบคุมการเข้าถึง ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ เครือข่ายไร้สาย อินเทอร์เน็ต อีเมลล์ และเครือข่ายสังคมออนไลน์ ดังนี้** **3.1.1 การควบคุมการเข้าถึงเครือข่าย (Network)** (1) ศูนย์ ICT ได้กำหนดให้การใช้งานระบบใช้ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น ซึ่งต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรและมีการทบทวนสิทธิ์เป็นประจำทุกปี				
	(2) ต้องมีการตรวจสอบยืนยันตัวตนก่อนเข้าใช้งานทุกครั้ง ซึ่งการอนุญาตให้ใช้ชื่อผู้ใช้งานและรหัสผ่านกำหนดให้ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของแต่ละหน่วยงานก่อน				
	(3) หน่วยงานจะติดตั้งและเชื่อมต่ออุปกรณ์เครือข่ายใด ต้องได้รับอนุญาตจากศูนย์ ICT ก่อนจึงจะดำเนินการได้และต้องดำเนินการโดยเจ้าหน้าที่ ICT หรือผู้ที่ได้รับอนุญาตเท่านั้น และผู้ดูแลระบบมีหน้าที่เชื่อมต่อสัญญาณและระงับสัญญาณทันทีเมื่อสิ้นสุดการอนุญาต				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	**มี/ใช่**	**ไม่มี / ไม่ใช่**		
	(4) ศูนย์ ICT มีการติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย โดยมีระบบแจ้งเตือนอัตโนมัติ				
	(5) มีการบันทึกควบคุมการเข้า–ออกห้องคอมพิวเตอร์แม่ข่าย หากมีเหตุผิดปกติใดขึ้นสามารถตรวจสอบได้				
	3.1.2 การควบคุมการเข้าถึงและการจัดการระบบปฏิบัติการ (Operating System) (1) ศูนย์ ICT ได้กำหนดให้การใช้งานระบบใช้ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น ซึ่งต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรและมีการทบทวนสิทธิ์เป็นประจำทุกปี				
	(2) ต้องมีการตรวจสอบยืนยันตัวตนก่อนเข้าใช้งานทุกครั้ง กรณีใช้ชื่อผู้ใช้งานและรหัสผ่านร่วมกันต้องได้รับอนุญาตจาก ผอ.ศูนย์ ICT เท่านั้น และมีกำหนดเวลาการใช้งานชัดเจน พร้อมทั้งยุติการใช้งานทันทีเมื่อพบความผิดปกติ				
	(3) มีการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ ซึ่งผู้ใช้งานต้องได้รับการอนุมัติจากผู้ดูแลระบบก่อนเท่านั้น และต้องพิสูจน์ยืนยันตัวตนทุกครั้ง เพื่อป้องกันการนำโปรแกรมที่ละเมิดลิขสิทธิ์หรือผิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและหน่วยงาน				
	3.1.3 การควบคุมการเข้าถึงและการจัดการโปรแกรมประยุกต์หรือแอปพลิเคชั่น (Application) (1) ศูนย์ ICT มีระบบตรวจสอบการดาวน์โหลดติดตั้งแอปพลิเคชั่นต่างๆ พร้อมทั้งระบบแจ้งเตือนอัตโนมัติและมีการอัพเดทระบบเพื่อพร้อมใช้งานเสมอ				
	(2) ศูนย์ ICT มีนโยบายควบคุมการดาวน์โหลดติดตั้งแอปพลิเคชั่นที่ไม่เหมาะสมและมีมาตรการเฝ้าระวังติดตามอยู่เสมอ				
	(3) ศูนย์ ICT มีแนวปฏิบัติในการดาวน์โหลดติดตั้งแอปพลิเคชั่นต่างๆ ผู้ใช้งานต้องได้รับการอนุมัติจากผู้ดูแลระบบเสียก่อน				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	มี/ใช่	ไม่มี / ไม่ใช่		
	3.1.4 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) (1) ศูนย์ ICT ได้กำหนดให้ผู้ใช้งานต้องลงทะเบียนกับผู้ดูแลระบบและต้องขออนุญาตเป็นลายลักษณ์อักษรจาก ผอ.ศูนย์ ICT ก่อนเท่านั้น				
	(2) ศูนย์ ICT ได้มีระบบควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ เพื่อป้องกันสัญญาณรั่วไหลและป้องกันการโจมตีจากสัญญาณภายนอก				
	(3) ศูนย์ ICT ใช้ซอฟแวร์และฮาร์ดแวร์เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายสม่ำเสมอ เพื่อตรวจสอบเหตุการณ์ที่น่าสงสัยและรายงาน ผอ.ศูนย์ ICT ทันทีเมื่อเกิดเหตุ				
	3.1.5 การควบคุมการใช้งานอินเทอร์เน็ต (Internet) (1) ศูนย์ ICT โดยผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์กับการใช้งานอินเทอร์เน็ตเฉพาะที่หน่วยงานจัดสรรเท่านั้นเพื่อป้องกันไวรัสหรือโปรแกรมไม่พึงประสงค์				
	(2) ศูนย์ ICT มีการติดตั้งโปรแกรมป้องกันไวรัสที่สามารถตรวจจับไวรัสและแจ้งเตือนอัตโนมัติเพื่อทำการกำจัดไวรัสได้ทันถ่วงที				
	3.1.6 การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) (1) ศูนย์ ICT ได้กำหนดให้การใช้งานระบบใช้ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น และมีการทบทวนสิทธิ์เป็นประจำทุกปี				
	(2) ศูนย์ ICT มีระบบตรวจจับการเข้ารหัสหากเข้าผิดเกินกว่าที่กำหนดระบบจะล็อคการทำงานอัตโนมัติ				
	3.1.7 การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) (1) ศูนย์ ICT มีระบบตรวจจับหากพบผู้ใช้งานเครือข่ายสังคมออนไลน์ละเมิดข้อกำหนดของหน่วยงาน โดยการเปิดเผยความลับและแสดงความคิเห็นยั่วยุที่ทำให้เกิดความเสื่อมเสียต่อหน่วยงาน				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	มี/ใช่	ไม่มี / ไม่ใช่		
	3.2 มีการควบคุม การปรับปรุง เปลี่ยนแปลง แก้ไขระบบหรืออุปกรณ์ประมวลสารสนเทศ				
	3.3 มีการแยกระบบและอุปกรณ์สำหรับพัฒนา ทดสอบ และการให้บริการออกจากกัน				
	3.4 มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสม เพื่อให้ความเสี่ยงที่เหลืออยู่อยู่ในระดับที่ยอมรับได้ โดยกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (KRI) เพื่อใช้ติดตามและทบทวนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์				
	3.5 ศูนย์ ICT มีการวางแผนและการกำหนดความต้องการใช้ทรัพยากรด้านสารสนเทศภายในหน่วยงานอย่างชัดเจน				
	3.6 ศูนย์ ICT มีการป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against Malware) สำหรับคอมพิวเตอร์ภายในหน่วยงาน เช่น โปรแกรมป้องกันตรวจจับไวรัส สแปม มัลแวร์ เป็นต้น				
	3.7 ศูนย์ ICT มีการสำรองข้อมูล (Back up) พร้อมทั้งมีมาตรการจัดการสื่อที่ใช้ในการบันทึกข้อมูลสำรอง โดยมีขั้นตอนการกำจัด การทำลาย การเก็บรักษา การอนุญาตและการใช้งานอย่างชัดเจน มีการจัดทำระบบสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ				
	3.8 ศูนย์ ICT มีระบบทดสอบและมีขั้นตอนการปฏิบัติการกู้คืนข้อมูลอย่างสม่ำเสมอ สำหรับกรณีฉุกเฉินการกู้คืนข้อมูลที่สำคัญ ศูนย์ ICT สามารถดำเนินการกู้คืนข้อมูลให้แล้วเสร็จภายในระยะเวลาที่เหมาะสม				
	3.9 ศูนย์ ICT มีการเฝ้าระวังและติดตามทางด้านความมั่นคงปลอดภัย (Monitoring) โดย 3.9.1 มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ มีการบันทึกเหตุการข้อผิดพลาด และมีการป้องกันข้อมูลที่บันทึกเหตุการณ์ดังกล่าว				
	3.9.2 มีการตรวจสอบการใช้งานระบบสารสนเทศ ให้สามารถใช้งานได้อย่างมีประสิทธิภาพอยู่เสมอ				
	3.9.3 ศูนย์ ICT มีการติดตามและตรวจสอบช่องโหว่ทางเทคนิค มีการทดสอบการเจาะระบบ เช่น การทดสอบเจาะระบบโฮส เครือข่าย และแอปพลิเคชั่นของบริการที่สำคัญ โดยมีระบบแจ้งเตือนเมื่อตรวจพบความผิดปกติ ซึ่งศูนย์ ICT มีการดำเนินการทดสอบระบบเป็นประจำทุกปี				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	มี/ใช่	ไม่มี / ไม่ใช่		
4	***การควบคุมการเข้าถึงระบบสารสนเทศและฐานข้อมูลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร** (Access control information System and database)*				
	4.1 การบริหารจัดการ การควบคุมการเข้าถึงระบบสารสนเทศของผู้ใช้งานระบบภายในกรมปศุสัตว์ โดย 4.1.1 ศูนย์ ICT ได้กำหนดนโยบายและมาตรการการควบคุมการเข้าถึงระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร				
	4.1.2 มีการลงทะเบียนผู้ใช้งาน โดยมีการบริหารจัดการสิทธิการใช้งานและมีการทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งาน				
	4.1.3 ศูนย์ ICT มีการควบคุมการเข้าถึงบริการที่สำคัญของกรมปศุสัตว์ โดยมีการใช้เทคนิคการตรวจสอบสิทธิ์ก่อนการเข้าใช้บริการ มีการตรวจสอบการบันทึกการเข้าใช้งานทั้งหมดเพื่อหากิจกรรมที่ผิดปกติเป็นประจำ สม่ำเสมอ ซึ่งมีรายงานที่สามารถตรวจสอบได้				
	4.2 ศูนย์ ICT มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน และมีการใช้งานรหัสผ่าน โดย 4.2.1 มีแนวปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย กำหนดคุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี อนุญาตให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง โดยมีรอบระยะเวลาการเปลี่ยนรหัสผ่านเพื่อความมั่นคงปลอดภัย กำหนดให้ผู้ใช้งานยืนยันรหัสผ่านใหม่ทุกครั้งที่ตั้งรหัสผ่านใหม่ และมีข้อระวังในการใช้งานรหัสผ่านที่ปลอดภัย				
	4.3 ศูนย์ ICT มีการควบคุมการเข้าถึงระบบสารสนเทศ โดย 4.3.1 มีขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย ชัดเจน				
	4.3.2 มีการระบุรหัสผ่านเพื่อพิสูจน์ตัวตนก่อนเข้าใช้งานระบบของผู้ใช้งาน ซึ่งการตั้งรหัสผ่านต้องตั้งให้มีความยากในการเดาไม่น้อยกว่า 8 หลัก (digits) โดยต้องประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข สัญลักษณ์พิเศษ และกำหนดให้การเข้ารหัสผิดได้ไม่เกิน 3 ครั้ง กรณีผู้ใช้งานเข้ารหัสผิดเกินจำนวนที่กำหนดไม่สามารถเข้าใช้งานได้ ให้ติดต่อผู้ดูแลระบบเพื่อแจ้งความจำนงค์ขอตั้งรหัสใหม่ โดยขออนุมัติ				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	มี/ใช่	ไม่มี / ไม่ใช่		
	4.3.3 มีการจำกัดการเข้าถึงระบบสารสนเทศของผู้ใช้งาน กรณีที่มีการเข้าใช้งานที่ผิดปกติ เช่น เข้ารหัสผิดเกินกว่าที่กำหนด ศูนย์ ICT มีระบบตรวจแจ้งเตือนอัตโนมัติและมีการอัพเดทระบบแจ้งเตือนอยู่เสมอ เพื่อให้ทันต่อสถานการณ์และป้องกันการเข้าถึงของผู้ที่ไม่มีสิทธิ์				
	4.4 ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ของหน่วยงานที่เป็นข้อมูลลับหรือเป็นข้อมูลสำคัญที่มิให้นำไปเปิดเผย โดยได้เปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ (ตามมาตร 72 แห่ง พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562) ศูนย์ ICT มีบทกำหนดโทษต่อผู้ละเมิดนั้นอย่างชัดเจน				
	4.5 ศูนย์ ICT มีระบบตรวจจับการเข้าถึงระบบโดยการเชื่อมต่อระยะไกล ซึ่งเป็นการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต หากระบบตรวจพบจะมีการแจ้งเตือนอัตโนมัติ ทั้งนี้ ศูนย์ ICT ได้มีบทลงโทษผู้ฝ่าฝืนไว้อย่างชัดเจน				
	4.6 ศูนย์ ICT มีระบบควบคุมป้องกันการแบ่งปันข้อมูลเพื่อป้องกันภัยคุกคามทางไซเบอร์ที่จะเกิดกับ ผู้ใช้งาน ผู้ให้บริการ เจ้าของคอมพิวเตอร์ ระบบคอมพิวเตอร์ เป็นต้น เพื่อให้การปฏิบัติงานเป็นมาตรฐานและมีประสิทธิภาพ จึงได้กำหนดขั้นตอนการแบ่งปันข้อมูล โดยหากตรวจพบว่าผู้ใดฝ่าฝืนไม่ปฏิบัติตามข้อกำหนดดังกล่าว ได้ระบุบทลงโทษไว้อย่างชัดเจน				
	4.7 ศูนย์ ICT จัดแบ่งประเภทของข้อมูลและจัดลำดับความสำคัญหรือชั้นความลับของข้อมูลตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ซึ่งได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้อย่างชัดเจน หากตรวจพบว่าผู้ใดฝ่าฝืนไม่ปฏิบัติตามข้อกำหนดดังกล่าว ได้ระบุบทลงโทษไว้อย่างชัดเจน				
	4.8 ศูนย์ ICT ได้กำหนดช่องทางการเข้าถึงข้อมูลที่ต้องได้รับสิทธิ์จากผู้ดูแลระบบ ซึ่งมีการกำหนดบัญชีผู้เกี่ยวข้องตามระดับการเข้าถึง แยกประเภทความรับผิดชอบ มีการพิสูจน์ตัวตนตามสิทธิ์ในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูลที่ตนได้รับอนุญาตเท่านั้น หากพบว่าผู้ใดฝ่าฝืน ได้ระบุบทลงโทษไว้อย่างชัดเจน				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	มี/ใช่	ไม่มี / ไม่ใช่		
	4.9 ศูนย์ ICT ได้ควบคุมการเข้าถึงสารสนเทศตามภารกิจ โดยผู้ดูแลระบบได้ติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ มีการบันทึกรายละเอียดเพื่อเป็นหลักฐานในการตรวจสอบภายหลัง โดยแบ่งผู้ใช้งานออกเป็น 5 กลุ่มตามสิทธิ์และภารกิจ หากพบว่าผู้ใดละเมิดสิทธิ์ของผู้อื่น ได้ระบุบทลงโทษไว้อย่างชัดเจน				
5	***ความมั่นคงปลอดภัยที่เกี่ยวข้องกับเจ้าหน้าที่ภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร***				
	5.1 ศูนย์ ICT มีการกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ภายในหน่วยงาน โดยมีการแบ่งแยกหน้าที่ที่เกี่ยวข้องด้านระบบสารสนเทศ กำหนดคุณสมบัติผู้รับผิดชอบในการดูแลระบบสารสนเทศจากผู้ที่มีความรู้ความสามารถในการดูแลระบบอย่างชัดเจน				
	5.2 มีกำหนดการให้เข้าถึงและถอดถอนสิทธิ์ในการเข้าถึงสถานที่ อุปกรณ์ ระบบสารสนเทศ และการส่งคืนสินทรัพย์ 5.2.1 ศูนย์ ICT ได้กำหนดให้มีการยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ ให้ตัดออกจากทะเบียนผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โยกย้าย หรือสิ้นสุดสัญญาจ้าง ซึ่งต้นสังกัดได้แจ้งศูนย์ ICT เป็นลายลักษณ์อักษร				
	5.2.2 กรณีผู้ใช้งานขออนุมัติความเห็นชอบจากต้นสังกัดและ ผอ.ศูนย์ ICT อนุมัติให้ใช้สิทธิ์พิเศษนอกเหนือจากภาระงานที่กำหนดโดยมีช่วงเวลาที่ชัดเจน ซึ่งได้จัดทำคำร้องเป็นลายลักษณ์อักษร นั้น เมื่อพ้นกำหนดการใช้สิทธิ์พิเศษดังกล่าว ให้ศูนย์ ICT ระงับสิทธิ์การใช้งานทันที				
	5.2.3 ศูนย์ ICT มีขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานเมื่อลาออกหรือปรับเปลี่ยนตำแหน่ง ต้องดำเนินการภายใน 15 วัน ชัดเจน				
	5.3 ศูนย์ ICT มีการสร้างความตระหนักรู้ การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยแก่เจ้าหน้าที่ภายในหน่วยงาน				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	**มี/ใช่**	**ไม่มี / ไม่ใช่**		
	5.3.1 ศูนย์ ICT ได้กำหนดการตั้งชื่อบัญชีผู้ใช้งานและรหัสผ่านการเข้าใช้งาน โดยชื่อผู้ใช้งานและผู้ดูแลระบบต้องแยกกัน ตั้งรหัสผ่านชั่วคราวต้องยากต่อการคาดเดาและต้องแตกต่างกัน รหัสผ่านมีอักษรตัวเล็ก ตัวใหญ่และสัญลักษณ์พิเศษ ผสมกันอย่างน้อย 8 ตัวอักษร และการตั้งชื่อบัญชีผู้ใช้งานและรหัสผ่านต้องแยกบัญชีและตั้งรหัสผ่านไม่เหมือนกัน				
	5.3.2 กรมปศุสัตว์ ได้จัดให้มีการอบรมเพื่อสร้างความรู้ และสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและรู้เท่าทันต่อภัยคุกคามรวมถึงผลกระทบที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่ระมัดระวังแก่ผู้ใช้งาน โดยศูนย์ ICT ได้ดำเนินการจัดฝึกอบรมอย่างน้อยปีละ 1 ครั้ง				
<u>แผนสำรองฉุกเฉิน / แผนเผชิญเหตุ</u>					
6	***การจัดทำแผนเตรียมความพร้อมฉุกเฉิน***				
	6.1 ศูนย์ ICT มีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการได้ตามภาวะปกติ เพื่อให้สามารถปรับใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย 6.1.1 มีการกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด				
	6.1.2 มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญ รวมทั้งมาตรการเพื่อลดความเสี่ยง เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ เป็นต้น ที่ทำให้ไม่สามารถเข้าใช้งานระบบสารสนเทศได้				
	6.1.3 มีการกำหนดขั้นตอนปฏิบัติการกู้คืน (Recover) ระบบสารสนเทศ และระยะเวลาในการกู้คืนที่เหมาะสม				
	6.1.4 มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบและการทดสอบแผนฉุกเฉิน				
	6.1.5 มีการกำหนดช่องทางการติดต่อเมื่อเกิดกรณีฉุกเฉิน เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น				
	6.1.6 มีการสร้างความตระหนักรู้และให้ความรู้แก่เจ้าหน้าที่ที่เกี่ยวข้องให้ทราบถึงขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุฉุกเฉินเร่งด่วน				
	6.2 ศูนย์ ICT มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อให้สามารถปรับใช้ได้อย่างต่อเนื่องเป็นปกติและสอดคล้องกับการใช้งานตามภารกิจ				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	**มี/ใช่**	**ไม่มี / ไม่ใช่**		
	6.3 ศูนย์ ICT มีการจัดเตรียมแหล่งกำเนิดกระแสไฟฟ้าสำรองในช่วงเกิดเหตุฉุกเฉิน เพื่อสนับสนุนกระบวนการทำงานของระบบสารสนเทศที่สำคัญ				
	6.4 ศูนย์ ICT มีการจัดทำสวิตช์ฉุกเฉินไว้ใกล้กับบริเวณทางออกของห้องควบคุมเพื่อให้สามารถเปิดสวิตช์ดับอุปกรณ์ทั้งหมดได้โดยทันทีทันใดและอย่างรวดเร็วกรณีที่เกิดเหตุฉุกเฉิน				
	6.5 ศูนย์ ICT มีระบบระงับหรือป้องกันเหตุ เพลิงไหม้ หรือไฟฟ้าลัดวงจรได้ทันทีทันใดกรณีเกิดเหตุฉุกเฉิน				
	6.6 ศูนย์ ICT มีการติดตั้งระบบแจ้งเตือนในกรณีที่การทำงานภายในห้องควบคุมทำงานผิดปกติหรือหยุดการทำงาน				
	6.7 ศูนย์ ICT มีระบบสายสื่อสารสำรอง ซึ่งเชื่อมต่อไปยังผู้ให้บริการเครือข่ายหรือผู้ให้บริการโทรคมนาคมเพื่อใช้เป็นเส้นทางสำรองกรณีที่เกิดเหตุฉุกเฉิน				
	6.8 ศูนย์ ICT ได้จัดทำมาตรการรักษาและแผนฟื้นฟูความเสียหายกรณีเกิดเหตุฉุกเฉิน พร้อมทั้งมีการฝึกซ้อมแผน เป็นประจำทุกปี				
7	***การจัดทำแผนเผชิญเหตุ***				
	7.1 ศูนย์ ICT มีมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ โดย 7.1.1 ศูนย์ ICT ได้จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์โดยการสื่อสาร การฝึกซ้อม การทบทวนและปรับปรุงแผนเป็นประจำทุกปี				
	7.1.2 ศูนย์ ICT ได้จัดทำแผนการสื่อสารในภาวะวิกฤตพร้อมทั้งฝึกซ้อมแผน และฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นประจำทุกปี				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ	การดำเนินการ		กรณีไม่มี / ไม่ใช่ ICT ดำเนินการอย่างไร	เอกสารอ้างอิง
	(ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	**มี/ใช่**	**ไม่มี / ไม่ใช่**		
	7.1.3 ศูนย์ ICT ได้จัดทำมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ โดยจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) และกำหนดบริการสำคัญที่ส่งผลกระทบต่อความต่อเนื่องทางธุรกิจ (BIA) พร้อมทั้งมีการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) เป็นประจำทุกปี				

1. โปรดระบุระบบปฏิบัติการ โปรแกรมประยุกต์ และเครือข่ายสารสนเทศที่อยู่ในความดูแลรับผิดชอบของศูนย์ ICT

.....

.....

.....

.....

.....

.....

.....

2. หน่วยงานท่านพบ ปัญหา อุปสรรค หรือความเสี่ยงในการปฏิบัติงาน ตามนโยบายและประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมปศุสัตว์ พ.ศ.2566 หรือไม่

.....

.....

.....

.....

.....

.....

.....

3. โปรดระบุภัยคุกคามทางไซเบอร์ ที่ ศูนย์ ICT เคยตรวจพบ พร้อมทั้งระบุสาเหตุและแนวทางการแก้ไข ฟื้นฟู ที่ได้ดำเนินการ

.....

.....

.....

.....

.....

.....

.....

ลงชื่อ.....ผู้กรอกข้อมูล/ผู้ประสานงาน

(.....)

ตำแหน่ง .....

วันที่ .....

เบอร์โทรติดต่อ.....

ลงชื่อ.....ผู้บังคับบัญชา

(.....)

ตำแหน่ง .....

วันที่ .....