



AOT Cybersecurity Incident Response Plan

This document shows the content of cybersecurity incident response plan of AOT. The content associated with the scope, role and responsibility, procedure, process, implementation in practice, recovery procedures in the PDF p. 4 as follows the content below:

1. Objective
2. Scope
3. Definition
4. Role and Responsibility
5. Detail of cybersecurity Incident Response Plan
 - 5.1 Cyber Incident Response Team: CIRT
 - 5.2 Incident Reporting Structure
 - 5.3 Criteria and process to activate and respond to the incident
 - 5.4 Containment of incident of cybersecurity
 - 5.5 Recovery Process
 - 5.6 Engagement Protocols with external person
 - 5.7 After-Action Review Process
6. Procedure and Implementation
 - 6.1 Procedure and Implementation of Recovery Process
 - 6.2 Preservation of Evidence



Procedure

แผนการรับมือภัยคุกคามทางไซเบอร์
(Cybersecurity Incident Response Plan)
ระบบควบคุมการเข้า-ออกพื้นที่หวงห้าม (ACCESS CONTROL)

ฝ่ายไฟฟ้าและเครื่องกล ท่าอากาศยานดอนเมือง

รหัสเอกสาร : Document No. PR-1056452000-002

Version: 1

ผู้จัดทำเอกสาร

ส่วนอุปกรณ์สื่อสารและคอมพิวเตอร์

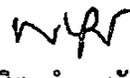
ฝ่ายไฟฟ้าและเครื่องกล ท่าอากาศยานดอนเมือง

โทรศัพท์ (801) 1370

เจ้าของเอกสาร

ฝ่ายไฟฟ้าและเครื่องกล ท่าอากาศยานดอนเมือง สายบำรุงรักษา

	แผนการรับมือภัยคุกคามทางไซเบอร์	รหัสเอกสาร : PR-1056452000-002
	(Cybersecurity Incident Response Plan)	Version : 1
	สายบำรุงรักษา	วันที่บังคับใช้ : 1 ธ.ค. 65
ระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร มาตรฐาน ISO/IEC 27001:2013		หน้า (2) ของ (20) หน้า

รายละเอียดเอกสาร	
ประเภทเอกสาร :	ขั้นตอนการปฏิบัติงาน (Procedure: PR)
ผู้จัดทำเอกสาร :	ส่วนอุปกรณ์สื่อสารและคอมพิวเตอร์ ฝ่ายไฟฟ้าและเครื่องกล ทำอากาศยานดอนเมือง
ผู้ทบทวน	ผู้อนุมัติ
 (.....นายสมเด็จ วรณทวิ.....) ตำแหน่ง ผอ.กก.ฝพค.ทดม. วันที่ / พ.ย. 65	 (.....นายชยาศิส นำรุงสวัสดิ์.....) ตำแหน่ง ผอ.กก.ฝพค.ทดม. วันที่ / พ.ย. 65

Version	วันที่บังคับใช้	ชื่อผู้จัดทำเอกสาร	สาระสำคัญของการแก้ไข/ปรับปรุง	หมายเหตุ
1	1 ธ.ค. 65	นายพีระ สุขพิศาล	เอกสารประกาศใช้ครั้งแรก	

	แผนการรับมือภัยคุกคามทางไซเบอร์	รหัสเอกสาร : PR-1056452000-002
	(Cybersecurity Incident Response Plan)	Version : 1
	สายบำรุงรักษา	วันที่บังคับใช้ : 1 ธ.ค.65
ระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร มาตรฐาน ISO/IEC 27001:2013		หน้า (3) ของ (20) หน้า

สารบัญ

หน้า

1. วัตถุประสงค์.....	5
2. ขอบเขต	5
3. คำนิยาม	5-6
4. หน้าที่และความรับผิดชอบ	6-8
5. รายละเอียดแผนรับมือภัยคุกคามทางไซเบอร์.....	9-15
5.1 โครงสร้างทีมรับมือเหตุการณ์ (Cyber Incident Response Team: CIRT).....	9
5.2 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure).....	10
5.3 เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT.....	11
5.4 ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวข้อง ความมั่นคงปลอดภัยไซเบอร์.....	12
5.5 การเรียกใช้งานกระบวนการกู้คืน (Recovery Process).....	14
5.6 ขั้นตอนในการสอบสวน (Investigate) สาเหตุ และผลกระทบของเหตุการณ์.....	14
5.7 ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก	14
5.7.1 แนวปฏิบัติการบริหารจัดการบุคคลภายนอก	14
5.8 กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process).....	14-15
6. ขั้นตอนและวิธีปฏิบัติงาน	15-16
6.1 ขั้นตอนและวิธีปฏิบัติงาน กระบวนการในการกู้คืนระบบ	15
6.1.1 แผนภูมิขั้นตอนการปฏิบัติ [กระบวนการในการกู้คืนระบบ].....	15
6.1.2 คำอธิบายขั้นตอนการปฏิบัติ [กระบวนการในการกู้คืนระบบ].....	16
6.2 ขั้นตอนและวิธีปฏิบัติงาน กระบวนการขั้นตอนเก็บรักษาหลักฐาน (Preservation of Evidance).....	17
6.2.1 แผนภูมิขั้นตอนการปฏิบัติ [กระบวนการขั้นตอนด้านนิติคอมพิวเตอร์ (Computer Forensic Procedure)].....	17
6.2.2 คำอธิบายขั้นตอนการปฏิบัติ [กระบวนการขั้นตอนด้านนิติคอมพิวเตอร์].....	18-19

	แผนการรับมือภัยคุกคามทางไซเบอร์	รหัสเอกสาร : PR-1056452000-002
	(Cybersecurity Incident Response Plan)	Version : 1
	สายบำรุงรักษา	วันที่บังคับใช้ : 1 ธ.ค.65
ระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร มาตรฐาน ISO/IEC 27001:2013		หน้า (4) ของ (20) หน้า

ภาคผนวก ก. มาตรฐานและข้อกำหนดอ้างอิง 20

ภาคผนวก ข. เอกสารอ้างอิง 20