

รายละเอียดข้อมูลการบังคับใช้นโยบายด้านการบริหารจัดการทรัพยากรการเข้าถึง เครื่องคอมพิวเตอร์ลูกข่าย ของสำนักงานประกันสังคม มีดังนี้

1. การบริหารจัดการสิทธิ์ขององค์กร

กำหนดให้มีการ Log Off หน้าจอแบบอัตโนมัติ เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์เกิน 20 นาที หรือผู้ใช้เลือก Log Off หน้าจอโดยทำการกดคีย์บอร์ดแป้นสัญลักษณ์ Windows + L

2. การควบคุมการเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control)

เป็นการควบคุมการเข้าถึงข้อมูล ระบบเครือข่าย ระบบปฏิบัติการและโปรแกรมประยุกต์ หรือแอปพลิเคชันและสารสนเทศ ทั้งทางกายภาพและทางระบบเครือข่ายโดยการกำหนดยืนยันตัวตนบุคคล และรหัสผ่าน ดังนี้

- 1) ในการเข้าใช้งานเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายของสำนักงานประกันสังคม ผู้ใช้ต้องระบุชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองเท่านั้น
- 2) กำหนดหรือตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านต้องประกอบด้วยตัวอักขระไม่น้อยกว่า 8 อักขระ ซึ่งประกอบด้วยตัวเลข ตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ พิมพ์เล็ก และตัวอักขระพิเศษ โดยต้องไม่ตั้งรหัสผ่านด้วย ชื่อ วันเดือนปีเกิด หรือข้อความที่ง่ายต่อการลวงรู้
- 3) ไม่ใช้รหัสผ่านซ้ำกับที่เคยใช้มาแล้วอย่างน้อย 5 รหัสผ่าน
- 4) ผู้ใช้เปลี่ยนรหัสผ่านทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยน (กำหนดเปลี่ยนทุก 90 วัน)

3. การป้องกันไวรัสบนเครื่องคอมพิวเตอร์

ทำการตรวจสอบสถานการณ์ทำงานของโปรแกรมตรวจจับไวรัส และตรวจสอบการอัปเดตฐานข้อมูลไวรัสอย่างสม่ำเสมอ ซึ่งสำนักงานประกันสังคม โดยสำนักบริหารเทคโนโลยีสารสนเทศ กำหนดเวลาอัปเดตฐานข้อมูลไวรัสในเวลาประมาณ 12.30 น. จึงขอความร่วมมือหน่วยงานเปิดเครื่องคอมพิวเตอร์ลูกข่ายเพื่อการอัปเดตดังกล่าว

4. การติดตั้งและถอดถอนโปรแกรม อุปกรณ์ หรือระบบต่าง ๆ

- 1) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่ละเมิดลิขสิทธิ์ และโปรแกรมเพิ่มเติมอื่น ๆ ที่นอกเหนือจากที่สำนักงานประกันสังคมติดตั้งไว้
- 2) ในกรณีที่ต้องการติดตั้งหรือใช้งานโปรแกรมหรือประโยชน์ใดๆ ขอให้แจ้งผู้ดูแลระบบของสำนักงานประกันสังคม เพื่อตรวจสอบโปรแกรมก่อนดำเนินการติดตั้ง
- 3) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นติดตั้งเพื่อการปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง
- 4) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของสำนักงานประกันสังคมเพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้นหรือเครือข่ายของสำนักงานประกันสังคม
- 5) ห้ามถอดถอนโปรแกรมรักษาความปลอดภัยที่ติดตั้งภายในเครื่องคอมพิวเตอร์และเครือข่ายออกโดยมิได้รับอนุญาตจากผู้ดูแลระบบ ได้แก่ โปรแกรมป้องกันไวรัส โปรแกรมบริหารจัดการเครื่องคอมพิวเตอร์ เป็นต้น

5. การใช้งานอินเทอร์เน็ต และอินทราเน็ต

ห้ามใช้โปรแกรมที่ไม่ได้รับอนุญาตตามนโยบายความมั่นคงปลอดภัยสารสนเทศของสำนักงานประกันสังคม เช่น โปรแกรมประเภท Peer-to-peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิททอร์เรนท์ (Bit Torrent), อีมูล (e-mule), ftp เป็นต้น

6. การใช้งานจดหมายอิเล็กทรอนิกส์

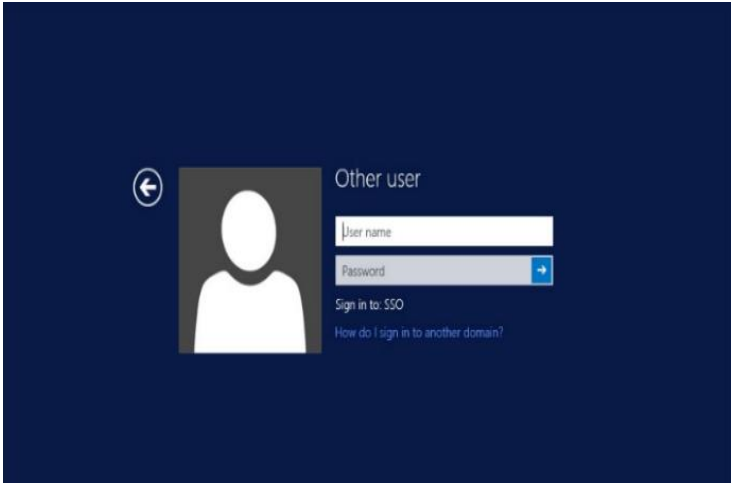
ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) จดหมายลูกโซ่ (Chain Letter) จดหมายที่ละเมิดต่อกฎหมายสินทรัพย์ทางปัญญาหรือสิทธิของบุคคลอื่น จดหมายที่มีโปรแกรมไม่ประสงค์ดีแนบไปให้กับบุคคลอื่นโดยเจตนา

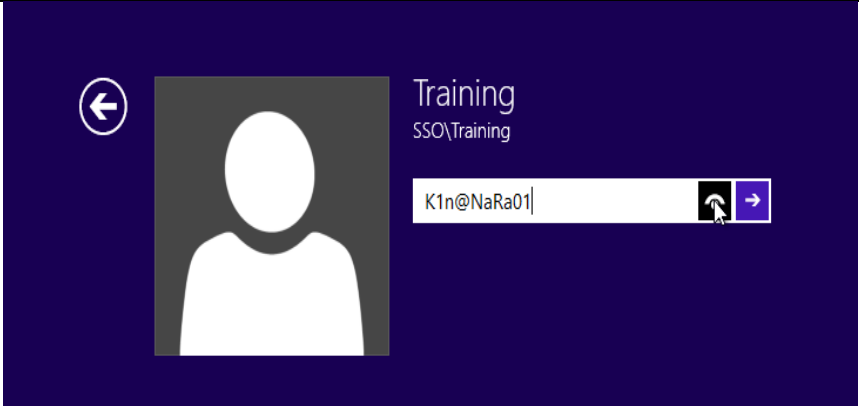
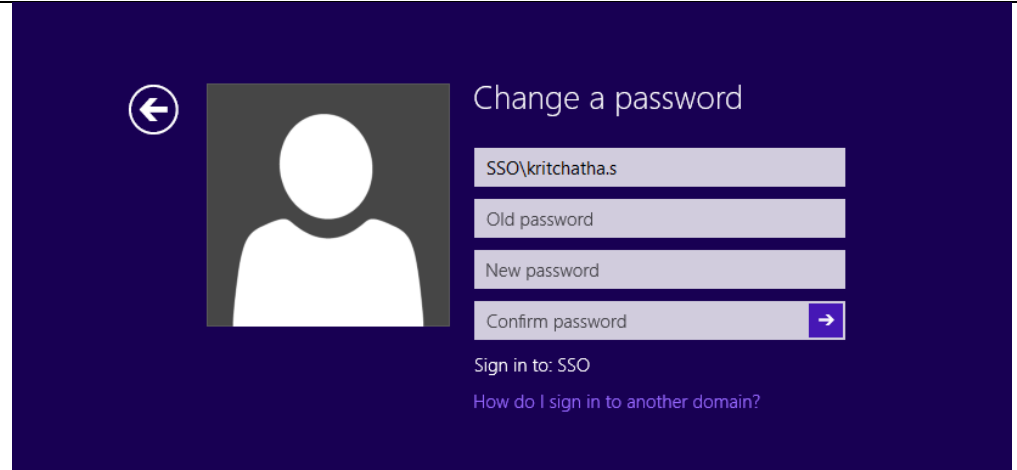
การบังคับใช้นโยบายด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย
รายละเอียดข้อมูลการบังคับใช้นโยบายด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย ประกอบด้วย

1. การบริหารจัดการสินทรัพย์ขององค์กร

ลำดับ	การดำเนินการ	รายละเอียด
1	กำหนดให้มีการ Log Off หน้าจอแบบอัตโนมัติ เมื่อไม่มีการใช้งานคอมพิวเตอร์เกิน ๒๐ นาที หรือผู้ใช้เลือก Log Off หน้าจอโดยทำการกดคีย์บอร์ดแป้นสัญลักษณ์ Windows + L	กำหนดให้มีการ ล็อกหน้าจอ แบบอัตโนมัติ เมื่อไม่มีการใช้งานเกิน 20 นาที 

2. การควบคุมการเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control)

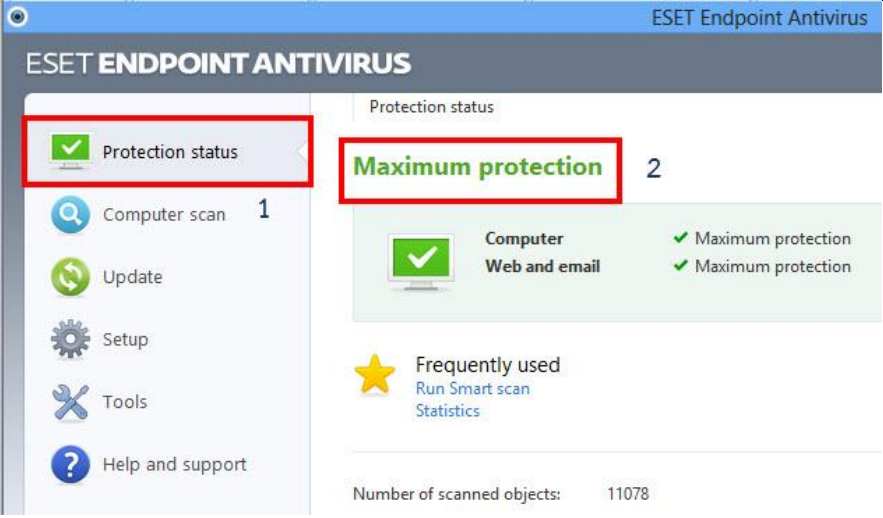
ลำดับ	การดำเนินการ	รายละเอียด
2.	เป็นการควบคุมการเข้าถึงข้อมูล ระบบเครือข่าย ระบบปฏิบัติการและโปรแกรมประยุกต์หรือแอปพลิเคชัน และสารสนเทศ ทั้งทางกายภาพและทางระบบเครือข่าย โดยการกำหนด ยืนยันตัวตนบุคคล และรหัสผ่าน ดังนี้ 1.) ในการใช้งานเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายของสำนักงานประกันสังคม ผู้ใช้ต้องระบุชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองเท่านั้น	ระบบบริหารจัดการทรัพยากรและบัญชีผู้ใช้งาน (Active Directory) จะมีการยืนยันตัวตนบุคคล โดยให้มีการใส่ ชื่อผู้ใช้งาน/รหัสผ่าน ก่อนเข้าใช้งานคอมพิวเตอร์ทุกครั้ง 
	2.) กำหนดหรือตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านต้องประกอบด้วย ตัวอักษรไม่น้อยกว่า 8 อักขระ ซึ่งประกอบด้วยตัวเลข ตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ พิมพ์เล็ก และตัวอักษรพิเศษ โดยต้องไม่ตั้งรหัสผ่านด้วย ชื่อ วันเดือนปีเกิด หรือข้อความใดที่ง่ายต่อการล่วงรู้	เงื่อนไขการตั้งรหัสผ่าน ดังนี้ 1.มีตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ 2.มีตัวอักษรภาษาอังกฤษพิมพ์เล็ก 3.มีตัวเลข 4.มีอักขระพิเศษ ** ห้ามใช้ รหัสผ่าน(Password) ตรงกับ ชื่อผู้ใช้งาน(User name) ** -ใช้เงื่อนไขอย่างน้อย 3 ใน 4 ข้อ

ลำดับ	การดำเนินการ	รายละเอียด
		 The screenshot shows a Windows login interface with a dark blue background. On the left is a white silhouette of a person. To the right of the silhouette, the text 'Training' and 'SSO\Training' is displayed. Below this is a password input field containing 'K1n@NaRa01'. To the right of the password field is a small icon of a person with a checkmark and a blue arrow pointing right.
	3.) ไม่ใช้รหัสผ่านซ้ำกับที่เคยใช้มาแล้วอย่างน้อย 5 รหัสผ่าน	 The screenshot shows a Windows 'Change a password' screen with a dark blue background. On the left is a white silhouette of a person. To the right of the silhouette, the text 'Change a password' is displayed. Below this are four input fields: 'SSO\kritchatha.s', 'Old password', 'New password', and 'Confirm password'. To the right of the 'Confirm password' field is a blue arrow pointing right. Below the input fields, the text 'Sign in to: SSO' and 'How do I sign in to another domain?' is displayed.

ลำดับ	การดำเนินการ	รายละเอียด
	4.) ผู้ใช้เปลี่ยนรหัสผ่านทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยน กำหนดการตั้ง รหัสผ่าน มีอายุการใช้งาน 90 วัน	โดยระบบจะมีข้อความแจ้งเตือนให้เปลี่ยนรหัสผ่านในระยะเวลา 5 วัน ก่อนหมดอายุ 

3. การป้องกันไวรัสบนเครื่องคอมพิวเตอร์

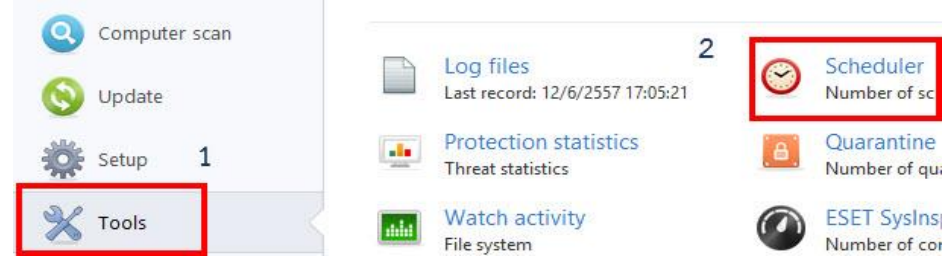
ลำดับ	การดำเนินการ	รายละเอียด
3.	3.1 ตรวจสอบสถานะ ทำการตรวจสอบสถานะการทำงานของโปรแกรมตรวจจับไวรัส และตรวจสอบการอัปเดตฐานข้อมูลไวรัสอย่างสม่ำเสมอ ซึ่ง สำนักงานประกันสังคม โดยสำนักบริหารเทคโนโลยีสารสนเทศกำหนดเวลาอัปเดตฐานข้อมูลไวรัสในเวลา 12.30 น. จึงขอความร่วมมือหน่วยงานเปิดเครื่องคอมพิวเตอร์ลูกข่ายเพื่อการอัปเดตดังกล่าว	ตรวจสอบการป้องกันไวรัส สถานการณ์ทำงานและการตรวจจับไวรัส  ดับเบิลคลิกไอคอน >ตรวจสอบสถานะการทำงาน Antivirus > ดูจาก Protection status > สถานะปกติจะขึ้น Maximum protection

ลำดับ	การดำเนินการ	รายละเอียด
		 The screenshot displays the ESET Endpoint Antivirus user interface. On the left is a navigation menu with options: Protection status (highlighted with a red box and a green checkmark icon), Computer scan (with a magnifying glass icon and a '1' badge), Update (with a circular arrow icon), Setup (with a gear icon), Tools (with a wrench icon), and Help and support (with a question mark icon). The main area on the right shows the 'Protection status' section, which includes a green checkmark icon, the text 'Maximum protection' (highlighted with a red box), and a '2' badge. Below this, it lists 'Computer' and 'Web and email' both with green checkmarks and the text 'Maximum protection'. A 'Frequently used' section contains links for 'Run Smart scan' and 'Statistics'. At the bottom, it states 'Number of scanned objects: 11078'.

3.2 ตรวจสอบการอัปเดต

ตรวจสอบเวลาการอัปเดตฐานข้อมูลไวรัส (ตั้งแบบอัตโนมัติ)

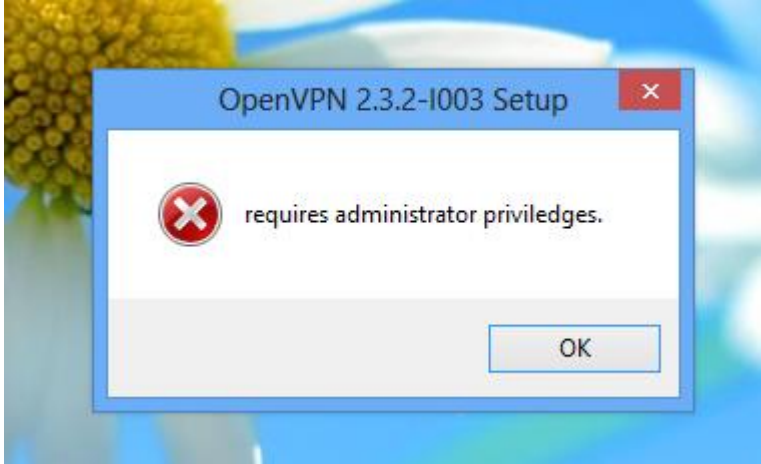
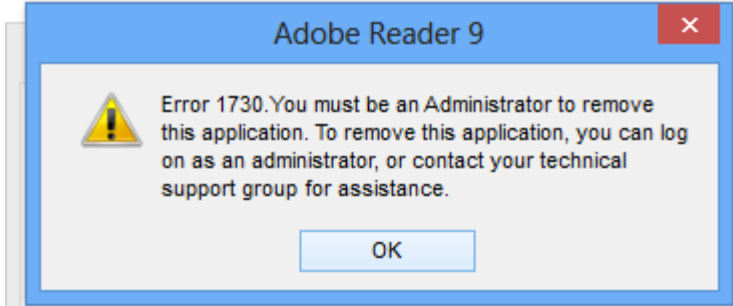
ไปที่ Tools>Scheduler>Update>



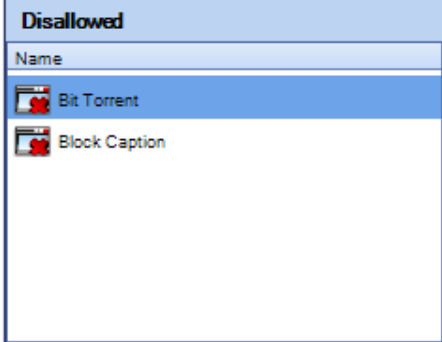
ตั้งเวลาให้เครื่องลูกข่าย Update signature ทุกวัน เวลา 12:30 น.

Name	Task	Launch time
☒ Log mainten...	Log mainten...	Task will be run every day at 9:00:00.
☒ Automatic u...	Update.	Dial-up connection to the Internet/VPN (once ...
☐ Automatic um...	Updater.	User login (once per hour at maximum).
☒ Update	Update.	Task will be run every day at 12:30:00.
☒ Automatic st...	System startup ...	User login. Task will not run if the computer is...
☒ Automatic st...	System startup ...	Successful update of the virus signature datab...

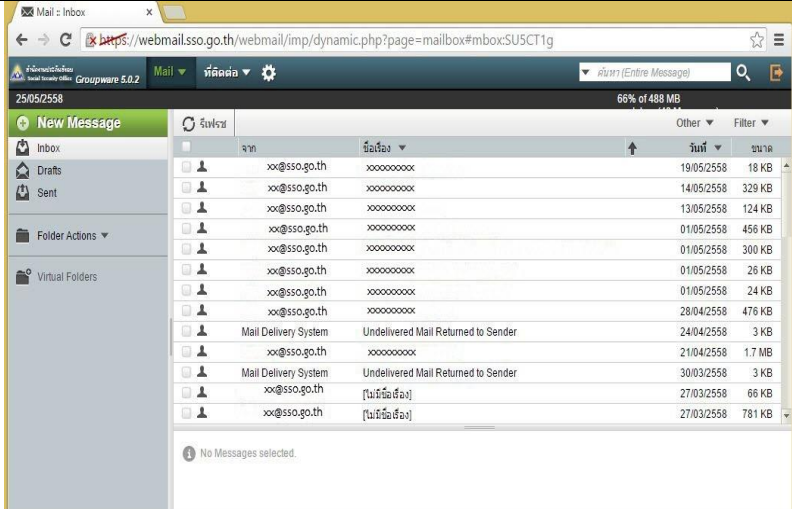
4. การติดตั้งและถอดถอนระบบ อุปกรณ์ หรือโปรแกรมต่าง ๆ

ลำดับ	การดำเนินการ	รายละเอียด
4	1.) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่ละเมิดลิขสิทธิ์ และโปรแกรมเพิ่มเติมอื่น ๆ ที่นอกเหนือจากที่สำนักงานประกันสังคมติดตั้งไว้ 2.) ในกรณีที่ต้องการติดตั้งหรือใช้งานโปรแกรม อรรถประโยชน์ใดๆ ขอให้แจ้งผู้ดูแลระบบของสำนักงานประกันสังคม เพื่อตรวจสอบโปรแกรมก่อนดำเนินการติดตั้ง 3.) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นติดตั้งเพื่อการปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง 4.) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของสำนักงานประกันสังคมเพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้น หรือเครือข่ายของสำนักงานประกันสังคม 5.) ห้ามถอดถอนโปรแกรมรักษาความปลอดภัยที่ติดตั้งภายในเครื่องคอมพิวเตอร์และเครือข่ายออกโดยมิได้รับอนุญาตจากผู้ดูแลระบบ ได้แก่โปรแกรมป้องกันไวรัส โปรแกรมบริหารจัดการเครื่องคอมพิวเตอร์ เป็นต้น	ไม่อนุญาตให้ติดตั้ง หรือ ถอดถอนโปรแกรม  

5. การใช้งานอินเทอร์เน็ต และอินเทอร์เน็ต

ลำดับ	การดำเนินการ	รายละเอียด
5	ห้ามใช้โปรแกรมที่ไม่ได้รับอนุญาตตามนโยบายความมั่นคงปลอดภัยสารสนเทศของสำนักงานประกันสังคม เช่น โปรแกรมประเภท Peer-to-peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนต์ (Bit Torrent), อีมูล (e-mule), ftp เป็นต้น	 The screenshot shows a window titled 'Disallowed' with a list of disallowed applications. The list includes 'Bit Torrent' and 'Block Caption'.

6. การใช้งานจดหมายอิเล็กทรอนิกส์

ลำดับ	การดำเนินการ	รายละเอียด
6	ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) จดหมายลูกโซ่ (Chain Letter) จดหมายที่ละเมิดต่อกฎหมายสิทธิทางปัญญาหรือสิทธิของบุคคลอื่น จดหมายที่มีโปรแกรมไม่ประสงค์ดีแนบไปให้กับบุคคลอื่นโดยเจตนา	 The screenshot shows a webmail inbox interface. The list of emails includes several from 'xx@sso.go.th' and two from 'Mail Delivery System' with the subject 'Undelivered Mail Returned to Sender'.

สามารถสอบถามข้อมูลเพิ่มเติมได้ที่
สำนักบริหารเทคโนโลยีสารสนเทศ
กลุ่มงานบริหารเครือข่ายสื่อสารและความมั่นคงคอมพิวเตอร์
นางสาวภัทธีรา คัมภีรญาณ
หมายเลขโทรศัพท์ 0 2956 2348 หมายเลข IP Phone 2348