

HIỆP ĐỊNH

VỀ CÙNG BẢO VỆ VÀ TRAO ĐỔI TIN MẬT

GIỮA

CHÍNH PHỦ NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA
VIỆT NAM

VÀ

CHÍNH PHỦ NƯỚC CỘNG HÒA DÂN CHỦ NHÂN DÂN
LÀO

HIỆP ĐỊNH
VỀ CÙNG BẢO VỆ VÀ TRAO ĐỔI TIN MẬT
GIỮA
CHÍNH PHỦ NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
VÀ
CHÍNH PHỦ NƯỚC CỘNG HÒA DÂN CHỦ NHÂN DÂN LÀO

Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam và Chính phủ nước Cộng hòa dân chủ nhân dân Lào (sau đây gọi là “hai Bên”),

Đã nhất trí mở rộng và thắt chặt hợp tác chính trị, kinh tế và tổ chức đối thoại về các vấn đề liên quan đến chính trị và an ninh,

Nhận thấy vai trò quan trọng của hợp tác song phương vì hoà bình, ổn định và phát triển,

Nhận thấy rằng hợp tác tốt nhằm tăng cường mối quan hệ hữu nghị, đoàn kết đặc biệt và hợp tác toàn diện giữa hai nước có thể đặt ra yêu cầu trao đổi tin mật,

Trên cơ sở nguyên tắc tôn trọng độc lập, chủ quyền, toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng và cùng có lợi, tuân theo quy định quốc tế và pháp luật và quy định quốc gia của mỗi Bên,

Mong muốn tạo ra các quy tắc về việc cùng bảo vệ tin mật được áp dụng cho bất kỳ thỏa thuận hợp tác nào trong tương lai và các hợp đồng mật sẽ được thực hiện giữa hai Bên có chứa đựng hoặc liên quan đến tin mật,

Đã thoả thuận như sau:

Điều 1
Phạm vi, mục đích

1. Hiệp định này đề ra các quy tắc về việc cùng bảo vệ tin mật được trao đổi giữa hai Bên, áp dụng đối với các cơ quan nhà nước, tổ chức, cá nhân của mỗi Bên tham gia vào hợp tác giữa hai quốc gia hoặc thực hiện các hợp đồng thuộc phạm vi điều chỉnh của Hiệp định này trong bất kỳ hoạt động hợp tác có bao gồm bảo vệ và trao đổi tin mật.

2. Lĩnh vực quân sự, quốc phòng, cơ yếu không thuộc phạm vi điều chỉnh của Hiệp định này.

3. Mục đích của Hiệp định này là nhằm bảo đảm việc bảo vệ tin mật được trao đổi giữa hai Bên trong quá trình hợp tác.

Điều 2

Giải thích từ ngữ

Trong Hiệp định này, các từ ngữ sau đây được hiểu như sau:

1. “Tin mật” là thông tin thuộc bất kỳ hình thức, loại hoặc phương pháp truyền tin nào đã được tạo ra và đã được xác định độ mật, vì lợi ích an ninh quốc gia và phù hợp với pháp luật quốc gia của mỗi Bên đòi hỏi được bảo vệ tránh việc mất, chiếm đoạt, tiếp cận trái phép, tiết lộ, phá hủy hoặc bất kỳ hình thức nào làm tổn hại đến tin mật.

2. “Tài liệu mật” là bất kỳ hình thức ghi nhận tin mật không kể đặc điểm của nó hoặc cách thức ghi nhận.

3. “Vật liệu mật” là bất kỳ tài liệu mật hay vật dụng kỹ thuật, thiết bị, sự lắp đặt, máy móc hoặc vũ khí đã được sản xuất hoặc đang trong quá trình sản xuất, cũng như các thành phần được sử dụng cho việc sản xuất mà có chứa đựng tin mật.

4. “Tiếp cận tin mật trái phép” là việc bất kỳ cá nhân hay tổ chức tiếp cận tin mật trái quy định pháp luật quốc gia của mỗi Bên và quy định tại Hiệp định này.

5. “Độ mật” là mức độ mật theo quy định pháp luật quốc gia của mỗi Bên cho thấy tầm quan trọng của tin mật, từ đó tương ứng với các biện pháp an ninh cụ thể liên quan đến việc tạo ra, tiếp cận, xử lý, lưu trữ và cung cấp tin mật đó.

6. “Dấu mật” là dấu được đóng trên vật liệu mật cho thấy mức độ mật.

7. “Bên cung cấp” là Bên chuyển tin mật.

8. “Bên nhận” là Bên tin mật được chuyển đến.

9. “Người sử dụng” là cá nhân hoặc tổ chức được phép tiếp cận tin mật theo quy định pháp luật quốc gia của mỗi bên tham gia vào các hoạt động hợp tác liên quan hoặc tham gia vào việc thực hiện các hợp đồng mật mà Hiệp định này sẽ được áp dụng.

10. “Cơ quan có thẩm quyền” là cơ quan nhà nước theo quy định pháp luật quốc gia của mỗi Bên nhằm thực hiện chính sách tổng thể của nhà nước về bảo vệ tin mật cũng như giám sát việc triển khai Hiệp định này.

11. “Bên ký hợp đồng” là cá nhân hoặc tổ chức có năng lực pháp lý để ký kết các hợp đồng trong thẩm quyền của mình.

12. “Hợp đồng mật” là thỏa thuận bằng văn bản giữa những người sử dụng của hai Bên liên quan đến việc tạo ra, sử dụng, tiếp cận, lưu trữ hoặc cung cấp tin mật.

13. “Nguyên tắc “cần biết” là nguyên tắc theo đó quyền tiếp cận tin mật chỉ được cấp cho cá nhân hoặc tổ chức liên quan tới nhiệm vụ chính thức và để thực hiện một nhiệm vụ chính thức cụ thể.

14. “Bên thứ ba” là bất kỳ cá nhân, tổ chức, nhà nước hoặc tổ chức quốc tế không phải là một Bên ký kết Hiệp định này hoặc ký kết hợp đồng mật.

15. “Giải mật” là việc xóa bỏ độ mật.

16. “Vi phạm an ninh” là hành động hoặc không hành động trái với quy định pháp luật quốc gia của mỗi Bên, dẫn đến việc tiếp cận trái phép, lộ, mất, phá hủy, chiếm đoạt trái phép hoặc bất kỳ một hình thức khác có thể làm tổn hại tin mật được trao đổi.

17. “Các trường hợp bất khả kháng” là tình huống hoặc sự kiện nằm ngoài khả năng kiểm soát của một Bên và khiến Bên xảy ra tình huống hoặc sự kiện đó không thể thực hiện nghĩa vụ của mình theo thỏa thuận.

Điều 3

Các cấp độ mật

Hai Bên đồng ý rằng các cấp độ mật sau là tương ứng và phù hợp với các cấp độ mật được quy định trong pháp luật quốc gia của mỗi Bên:

Đối với nước CHXHCN Việt Nam	Đối với nước CHDCND Lào	Tương đương trong tiếng Anh
TUYỆT MẬT	ລັບທີ່ສຸດ	TOP SECRET
TỐI MẬT	ລັບສະເພາະ	SECRET
MẬT	ລັບ	CONFIDENTIAL

Điều 4

Cơ quan có thẩm quyền

1. Cơ quan có thẩm quyền của hai Bên là:
 - Đối với nước Cộng hoà xã hội chủ nghĩa Việt Nam: Bộ Công an;
 - Đối với nước Cộng hòa Dân chủ Nhân dân Lào: Bộ Công an
2. Hai Bên sẽ thông báo cho nhau thông qua kênh ngoại giao về những thay đổi đối với cơ quan có thẩm quyền.
3. Cơ quan có thẩm quyền sẽ thông báo cho nhau về pháp luật hiện hành của quốc gia mỗi Bên quy định về bảo vệ tin mật.
4. Nhằm bảo đảm hợp tác chặt chẽ trong việc thực hiện Hiệp định này, các cơ quan có thẩm quyền có thể tổ chức tham vấn theo yêu cầu của một trong hai Bên.
5. Nhằm đạt được và duy trì các tiêu chuẩn an ninh tương đương, cơ quan có thẩm quyền, theo yêu cầu sẽ cung cấp cho nhau thông tin về tiêu chuẩn an ninh, trình tự, thủ tục đối với việc bảo vệ tin mật được áp dụng cho mỗi Bên.
6. Cơ quan có thẩm quyền của hai Bên có thể ký các văn bản hành chính liên quan đến việc thực hiện Hiệp định này.
7. Cơ quan có thẩm quyền của mỗi Bên sẽ bảo đảm tuân thủ nghiêm ngặt Hiệp định này, áp dụng với tất cả cơ quan nhà nước, tổ chức, cá nhân tham gia vào hợp tác giữa hai quốc gia hoặc thực hiện các hợp đồng thuộc phạm vi điều chỉnh của Hiệp định này.

Điều 5

Cung cấp tin mật

1. Tin mật sẽ được cung cấp thông qua kênh ngoại giao hoặc các kênh khác do hai Bên cùng chấp thuận theo quy định pháp luật quốc gia của mỗi Bên. Bên nhận sẽ khẳng định với Bên cung cấp bằng văn bản khi nhận được tin mật.
2. Đối với tin được phân loại là Tuyệt mật đã được quy định tại Điều 3 chỉ được cung cấp thông qua kênh ngoại giao.

3. Trong trường hợp cung cấp một bao kiện lớn có chứa vật liệu mật, hai Bên sẽ cùng thống nhất và quyết định về phương tiện vận chuyển, tuyến đường và các biện pháp an ninh khác.

4. Trường hợp một trong hai Bên có căn cứ cho rằng việc thực hiện yêu cầu cung cấp tin mật sẽ gây tổn hại đến chủ quyền và an ninh quốc gia hoặc trái với luật pháp quốc gia của mỗi Bên và nghĩa vụ quốc tế thì có thể từ chối yêu cầu cung cấp tin mật và phải thông báo bằng văn bản lý do từ chối cho bên đề nghị cung cấp.

Điều 6

Các biện pháp bảo vệ tin mật

1. Phù hợp với pháp luật của quốc gia mình, hai Bên sẽ triển khai mọi biện pháp phù hợp để bảo vệ tin mật được cung cấp theo Hiệp định này. Tin mật được cung cấp sẽ được bảo vệ tương đương với độ mật của Bên nhận.

2. Hai Bên sẽ kịp thời thông báo cho nhau về bất kỳ thay đổi nào về luật pháp của quốc gia mình ảnh hưởng đến việc bảo vệ tin mật. Trong trường hợp như vậy, hai Bên sẽ thông báo cho nhau nhằm trao đổi về khả năng sửa đổi Hiệp định này. Trong thời gian đó, tin mật sẽ được bảo vệ phù hợp với quy định của Hiệp định này, trừ khi có thỏa thuận khác bằng văn bản.

3. Không có cá nhân nào được quyền tiếp cận tin mật chỉ vì cấp bậc, chức vụ. Việc tiếp cận tin mật chỉ được dành cho cá nhân, tổ chức phù hợp với nguyên tắc “cần biết” được quy định tại Điều 2. Việc tiếp cận tin mật phải thực hiện theo quy định pháp luật quốc gia của mỗi Bên.

4. Trách nhiệm của Bên cung cấp tin mật:

a) Bảo đảm tin mật được đánh dấu độ mật phù hợp với quy định luật pháp quốc gia của Bên cung cấp.

b) Thông báo cho Bên nhận về bất kỳ điều kiện phát hành hoặc hạn chế đối với việc sử dụng tin mật đã được cung cấp bởi Bên cung cấp và về mọi thay đổi tiếp theo trong phân loại bảo mật.

5. Trách nhiệm của Bên nhận:

a) Không tiết lộ, cung cấp tin mật cho Bên thứ ba mà không có sự đồng ý trước bằng văn bản của Bên cung cấp;

b) Bảo đảm tin mật được đánh dấu mật tương đương với độ mật do Bên cung cấp quy định;

c) Không sử dụng tin mật cho các mục đích khác với các mục đích mà tin mật đã được cung cấp;

d) Bảo đảm việc bảo vệ tin mật với thời hạn theo quy định của Bên cung cấp, trừ trường hợp có yêu cầu khác bằng văn bản của Bên cung cấp.

Điều 7

Dịch, nhân bản và hủy tin mật

1. Vật liệu mật được đóng dấu TUYÊN MẬT/ ལྷན་ཁྲིམས་/ TOP SECRET chỉ được nhân bản khi có sự đồng ý bằng văn bản của Bên cung cấp.

2. Việc dịch thuật tin mật sẽ được thực hiện theo quy định luật pháp quốc gia của mỗi Bên. Bản dịch sẽ được Bên nhận đóng dấu mật tương đương với độ mật của Bên cung cấp và được bảo vệ như bản gốc.

3. Khi vật liệu mật được nhân bản, tất cả các con dấu mật gốc cũng sẽ được nhân bản theo. Thủ tục nhân bản vật liệu mật được thực hiện theo quy định và pháp luật quốc gia của mỗi Bên. Vật liệu mật được nhân bản này được kiểm soát như vật liệu mật gốc. Số lượng các bản sao sẽ được hạn chế theo yêu cầu vì mục đích chính thức.

4. Vật liệu mật sẽ được hủy hoặc sửa đổi tới mức nhằm ngăn ngừa tái tạo toàn bộ hoặc một phần.

5. Bên cung cấp có thể nêu rõ việc cấm nhân bản, thay đổi hoặc hủy vật liệu mật bằng cách đánh dấu vật chứa tin mật phù hợp hoặc gửi văn bản thông báo sau đó. Nếu việc hủy vật liệu mật bị cấm thì vật liệu mật đó và vật liệu mật đã được nhân bản sẽ được trả lại cho Bên cung cấp.

6. Vật liệu TUYÊN MẬT/ ལྷན་ཁྲིམས་/TOP SECRET không được phép hủy và phải được trả lại cho Bên cung cấp.

7. Trong trường hợp bất khả kháng không thể bảo vệ và trả lại vật liệu mật đã được cung cấp theo Hiệp định này, vật liệu mật sẽ được hủy ngay lập tức. Bên nhận sẽ thông báo cho Bên cung cấp về việc hủy vật liệu mật sớm nhất khi có thể.

Điều 8

Hợp đồng mật

1. Hợp đồng mật sẽ được ký kết và triển khai phù hợp với quy định pháp luật quốc gia của mỗi Bên.

2. Mỗi Hợp đồng mật được ký kết theo các điều khoản của Hiệp định này kèm theo một phụ lục bao gồm những thông tin sau:

- a) Hướng dẫn phân loại và danh sách tin mật;
- b) Các thủ tục để thông báo bất kỳ thay đổi nào về mức độ bảo mật của tin mật;
- c) Kênh được sử dụng để liên lạc;
- d) Thủ tục vận chuyển;
- e) Các cơ quan có liên quan chịu trách nhiệm về việc phối hợp bảo vệ tin mật trong Hợp đồng mật;
- f) Thông tin cơ bản của cá nhân, tổ chức dự kiến sẽ tiếp cận tin mật và chức năng, nhiệm vụ của những tổ chức này.

3. Trách nhiệm bảo vệ tin mật của mỗi Bên ký kết hợp đồng mật trong mọi trường hợp ít nhất là:

- a) Chỉ tiết lộ tin mật cho cá nhân, tổ chức tham gia việc thực hiện hợp đồng mật và phù hợp với nguyên tắc “cần biết”;
- b) Bố trí phương tiện được sử dụng để vận chuyển vật liệu mật;
- c) Bảo đảm độ mật của tin mật được cung cấp không bị thay đổi trừ khi được Bên cung cấp cho phép bằng văn bản;
- d) Thông báo về những thay đổi có thể phát sinh liên quan đến tin mật do những thay đổi về độ mật hoặc do không còn cần thiết phải bảo vệ nữa;
- e) Thông báo thủ tục phê duyệt các chuyến thăm, tiếp cận hoặc giám sát bởi nhân viên của một Bên đối với các cơ sở của Bên kia được nêu trong hợp đồng mật;
- f) Thông báo kịp thời cho Bên ký kết hợp đồng về bất kỳ sự tiếp cận, âm mưu tiếp cận hoặc nghi ngờ có sự tiếp cận trái phép tin mật của hợp đồng;

g) Sử dụng tin mật trong hợp đồng mật chỉ vì các mục đích liên quan tới nội dung của hợp đồng hoặc cho mục đích mà tin mật được cung cấp với các giới hạn do Bên cung cấp nêu ra;

h) Tuân thủ nghiêm ngặt quy trình hủy vật liệu mật;

i) Chỉ cung cấp tin mật theo hợp đồng mật cho Bên thứ ba khi có sự đồng ý bằng văn bản của Bên cung cấp.

4. Các biện pháp yêu cầu đối với việc bảo vệ tin mật cũng như quy trình thủ tục để đánh giá và nhận biết khả năng mất cho các Bên ký kết hợp đồng mật do sự tiếp cận trái phép đối với tin mật sẽ được quy định chi tiết trong hợp đồng mật tương ứng.

Điều 9

Vi phạm an ninh

1. Trong trường hợp vi phạm an ninh, cơ quan có thẩm quyền của nước mà hành vi vi phạm an ninh xảy ra sẽ thông báo sớm nhất khi có thể cho cơ quan có thẩm quyền của Bên kia và sẽ tiến hành điều tra thích hợp. Bên kia sẽ hợp tác trong công tác điều tra, nếu được yêu cầu.

2. Trong trường hợp vi phạm an ninh xảy ra ở nước thứ ba, cơ quan có thẩm quyền của Bên cung cấp sẽ thực hiện các hành động theo quy định của khoản 1 Điều này khi có thể.

3. Trong bất kỳ trường hợp nào, cơ quan có thẩm quyền của Bên có vi phạm an ninh xảy ra phải thông báo cho Bên kia về kết quả điều tra, nguyên nhân, mức độ thiệt hại xảy ra và biện pháp khắc phục.

4. Cơ quan có thẩm quyền của Bên có vi phạm an ninh xảy ra sẽ thực hiện tất cả các biện pháp phù hợp với quy định pháp luật của quốc gia mình để hạn chế hậu quả của hành vi vi phạm và để ngăn chặn vi phạm tiếp theo.

Điều 10

Các chuyến thăm

1. Các chuyên gia của hai Bên có thể hợp định kỳ nhằm trao đổi về các quy trình, thủ tục bảo vệ tin mật.

2. Những người đến thăm phải được quốc gia mình ủy quyền tiếp cận tin mật hoặc tiếp cận cơ quan tạo ra, xử lý hoặc lưu trữ tin mật và phải được sự cho phép trước bằng văn bản của nước tiếp nhận.

3. Thủ tục cho các chuyến thăm sẽ được thống nhất giữa hai Bên.

4. Bên đến thăm cần cung cấp bằng văn bản những thông tin sau:

- a) Họ tên, ngày sinh, số hộ chiếu của người đến thăm;
- b) Quốc tịch của người đến thăm;
- c) Chức vụ của người đến thăm và tên cơ quan người đó đại diện;
- d) Mục đích, dự kiến chương trình làm việc và thời gian của chuyến thăm;
- e) Tên cơ quan và cơ sở đề nghị được đến thăm;

f) Người đến thăm phải được Bên cử đi xác nhận bằng văn bản cho phép tiếp cận tin mật hoặc tiếp cận cơ quan tạo ra, xử lý hoặc lưu trữ tin mật, phạm vi, nội dung những thông tin mật được phép tiếp cận phù hợp với quy định luật pháp của mỗi Bên

g) Tin mật mà người đến thăm muốn tiếp cận và thời gian cần thiết cho việc tiếp cận đó. Bên nhận sẽ thông báo về mức độ bảo đảm an ninh của thông tin.

5. Hai Bên có thể thỏa thuận đưa ra danh sách những người được ủy quyền để thu xếp các chuyến thăm định kỳ. Danh sách đó có giá trị trong 12 tháng. Khi danh sách đó đã được hai Bên thông qua, thời hạn của chuyến thăm cụ thể sẽ được thu xếp trực tiếp với nhà chức trách của các tổ chức được những người này đến thăm, phù hợp với thời hạn và điều kiện đã được thống nhất.

6. Mỗi Bên sẽ bảo đảm công tác bảo vệ dữ liệu cá nhân của người đến thăm, phù hợp với quy định pháp luật quốc gia của mỗi Bên.

7. Mỗi Bên có quyền thay đổi danh sách những người đến thăm và thông báo lý do cho Bên kia.

Điều 11

Chi phí

Mỗi Bên sẽ tự chịu chi phí liên quan phát sinh khi áp dụng và thực thi Hiệp định này theo quy định và pháp luật quốc gia của mỗi Bên.

Điều 12
Điều khoản cuối cùng

1. Hiệp định này sẽ có hiệu lực vào ngày thứ ba mươi (30) kể từ ngày hai Bên trao đổi văn kiện ngoại giao thông báo cho nhau về việc hoàn thành các thủ tục nội bộ cần thiết để Hiệp định có hiệu lực.

2. Hiệp định này có thể được sửa đổi trên cơ sở có sự đồng ý bằng văn bản của cả hai Bên qua kênh ngoại giao. Văn bản sửa đổi, bổ sung Hiệp định là một bộ phận không tách rời của Hiệp định và có giá trị pháp lý như nhau. Việc sửa đổi như vậy sẽ có hiệu lực theo khoản 1 của Điều này.

3. Mỗi Bên có thể chấm dứt Hiệp định bằng cách thông báo bằng văn bản cho Bên kia qua kênh ngoại giao. Việc chấm dứt Hiệp định sẽ có hiệu lực vào ngày thứ một trăm tám mươi (180) kể từ ngày nhận được thông báo cuối cùng. Mặc dù chấm dứt Hiệp định này, mọi tin mật đã được cung cấp theo Hiệp định sẽ tiếp tục được bảo vệ phù hợp với quy định của các điều khoản của Hiệp định cho đến khi Bên cung cấp thông báo miễn trừ trách nhiệm bảo vệ tin mật cho Bên nhận.

4. Mọi bất đồng liên quan đến việc giải thích hay áp dụng Hiệp định này sẽ được giải quyết một cách thân thiện thông qua tham vấn giữa hai Bên mà không nhờ đến sự phán xử của Bên thứ ba.

Hiệp định này được ký tại Viên chăn, ngày 29 tháng 9 năm 2023 thành hai bản gốc, mỗi bản bằng tiếng Việt, tiếng Lào và tiếng Anh, các văn bản đều có giá trị như nhau. Trong trường hợp có sự giải thích khác nhau, bản tiếng Anh sẽ được dùng làm cơ sở.

THAY MẶT
CHÍNH PHỦ NƯỚC CỘNG HÒA
XÃ HỘI CHỦ NGHĨA VIỆT NAM



Đại tướng TÔ LÂM
Bộ trưởng Bộ Công an

THAY MẶT
CHÍNH PHỦ NƯỚC CỘNG HÒA
DÂN CHỦ NHÂN DÂN LÀO



Đại tướng Vilay LAKHAMPHONG
Phó Thủ tướng
Bộ trưởng Bộ Công an

AGREEMENT

ON

**MUTUAL PROTECTION AND EXCHANGE
OF CLASSIFIED INFORMATION**

BETWEEN

**THE GOVERNMENT OF THE SOCIALIST REPUBLIC OF
VIET NAM**

AND

**THE GOVERNMENT OF THE LAO
PEOPLE'S DEMOCRATIC REPUBLIC**

**AGREEMENT
ON MUTUAL PROTECTION AND EXCHANGE OF CLASSIFIED
INFORMATION
BETWEEN
THE GOVERNMENT OF THE SOCIALIST REPUBLIC OF VIET NAM
AND
THE GOVERNMENT OF THE LAO PEOPLE'S DEMOCRATIC REPUBLIC**

The Government of the Socialist Republic of Viet Nam and the Government of the Lao People's Democratic Republic (hereinafter referred to as “the Parties”),

Having agreed to broaden and tighten their political and economic co-operation, and to hold dialogues on political and security-related issues,

Recognizing the important role of their bilateral co-operation for peace, stability and development,

Realizing that good co-operation for enhancing the relations of friendship, special solidarity and comprehensive cooperation between the two countries may require exchange of classified information,

On the basis of respect for each other's independence, sovereignty and territorial integrity, non-interference in each other's internal affairs, equality, and mutual interest pursuant to the international regulations and the national laws and regulations of the respective Party,

Desiring to create a set of rules regulating the mutual protection of classified information applicable to any future co-operation agreements and classified contracts, which will be implemented between the Parties, containing or involving classified information,

Have agreed as follows:

**Article 1
Scope and Objective**

1. This Agreement shall set forth the rules for the mutual protection of classified information exchanged between the Parties, applicable to the State agencies, legal entities, individuals of the respective Party or the

implementation of the contracts within the scope of this Agreement in any cooperation activities including the protection and the exchange of classified information.

2. The field of military, national defence and cipher are not under the scope of this Agreement.

3. The objective of this Agreement is to ensure the protection of classified information exchanged between the Parties during cooperation process.

Article 2

Definition of Terms

In this Agreement, the following terms should be defined as follows:

1. "Classified information" means any information of whatever form, nature or method of transmission produced and specified the security classification level for the interest of the national security of the respective Party and in accordance with its national laws and regulations, to which it requires protection against the loss, misappropriation, unauthorized access, disclosure, destruction or any form damaging to the classified information.

2. "Classified document" means any form of recorded classified Information, regardless of its characteristics or types of recording.

3. "Classified material" means any classified document or technical item, equipment, installation, device or weapon either produced or under a process of manufacture, as well as the components used for their manufacture which classified information can be included.

4. "Unauthorized access to classified information" means any individual or legal entity's access to classified information contrary to the provisions of national laws and regulations of the respective Party and regulations under this Agreement.

5. "Security classification level" means a classification level, according to the national laws and regulations of the respective Party, which characterizes the importance of classified information, thereby corresponding to the specific security methods relating to the production, access, handling, storage, supply of such classified information.

6. "Classification marking" means a mark on classified material, which shows the security classification level.

7. "The Originating Party" means the Party transferring the classified information.

8. "The Receiving Party" means the Party to which the classified information is transmitted.

9. "User" means an individual or a legal entity granted access to the classified information in accordance with the national laws and regulations of the respective Party that takes part in the relevant cooperation activities or during implementation of classified contracts to which this Agreement shall be applied.

10. "Competent Authority" means the State agency according to the national laws and regulations of the respective Party performing the State policy for the protection of classified information, as well as supervising the implementation of this Agreement.

11. "Contractor" means an individual or a legal entity within its jurisdiction possessing the legal capability to undertake the classified contracts.

12. "Classified contract" means an agreement in writing between the users of the Parties in relating to the generation, use, access, storage or transmission of classified information.

13. "Need-to-know" principle" means the access to classified information only shall be provided to an individual or a legal entity in connection with official duties and for the performance of a specific official task.

14. "The third Party" means any individual, legal entity, State or an international organization, which is not a Party to sign this Agreement or classified contract.

15. "Declassification of Information" means the removal of the security classification level.

16. "Breach of security" means an action or inaction contrary to the national laws and regulations of the respective Party, which results or may result in the unauthorized access, disclosure, loss, destruction, illegal misappropriation or any form damaging to exchanged classified information.

17. "Force Majeure" means extraordinary events or circumstances which happen beyond the control of one of the parties, making the party's performance of its obligations under the agreement impossible or impracticable.

Article 3

Security Classification Levels

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the national laws and regulations of the respective Party:

For the Socialist Republic of Viet Nam	For the Lao People's Democratic Republic	Equivalent in English
TUYỆT MẬT	ລັບທີ່ສຸດ	TOP SECRET
TỐI MẬT	ລັບສະເພາະ	SECRET
MẬT	ລັບ	CONFIDENTIAL

Article 4

Competent Authorities

1. The competent authorities of the Parties are:

For the Socialist Republic of Viet Nam: Ministry of Public Security.

For the Lao People's Democratic Republic: Ministry of Public Security.

2. The Parties shall notify each other through diplomatic channels of any change of their competent authorities.

3. The competent authorities shall inform each other of its applicable laws regulating the protection of classified information.

4. In order to ensure the close co-operation during the implementation of this Agreement, the competent authorities may hold consultations at request made by each Party.

5. In order to achieve and maintain comparable standards of security, the competent authorities shall, on request, provide each other with information about the security standards, procedures and practices for protection of classified information applied by the respective Party.

6. The competent authorities of the Parties may conclude the administrative documents in relation with the implementation of this Agreement.

7. The competent authorities of the Parties shall ensure to comply with this Agreement strictly, applicable to all State agencies, legal entities, individuals participating in the cooperation between the two countries or implementing the contracts under the scope of this Agreement.

Article 5

Transmission of Classified Information

1. Classified information shall be transmitted by means of diplomatic channel or by mutual consent in accordance with the national laws and regulations of the respective Party. The Receiving Party shall confirm with the Originating Party in writing upon the receipt of classified information.

2. Classified information at the top secret level as stated in Article 3 shall be only transmitted via diplomatic channel.

3. In case of transferring a large consignment containing classified material information, the competent authorities shall mutually agree upon and approve the means of transportation, the route and other security measures.

4. In case one of the Parties has a ground that the implementation of the request to transmit Classified Information shall damage national sovereignty and security or disobey each Party's national laws and regulations as well as international obligations, it can deny the request of Transmission of Classified Information and notify to the request Party in writing the reason for denial.

Article 6

Measures for Protection of Classified Information

1. In accordance with their national laws and regulations, the Parties shall take all appropriate measures for protection of classified information which is provided under this Agreement. Such exchanged classified information shall be protected with the corresponding security classification level of the Receiving Party.

2. The Parties shall in due time inform each other about any changes in the national laws and regulations affecting the protection of classified information. In such cases, the Parties shall inform each other in order to discuss possible amendments to this Agreement. Meanwhile, the classified information shall be protected pursuant to the provisions of the Agreement, unless otherwise agreed in writing.

3. No individual shall be entitled to access classified information solely by virtue of his or her rank, official position. Access to classified information shall be limited only to individuals, legal entities in accordance with the "need to know" principle as stated in Article 2. The access to classified information must comply with the national laws and regulations of the respective Party.

4. The Originating Party is obligated:

a) To ensure the classified information shall be marked at a security classification level in accordance with the national laws and regulations of the respective Party.

(b) To notify the Receiving Party of any condition of issuance or limitation to the usage of the classified information originated by it and about the next change on classification.

5. The Receiving Party is obligated:

a) Not to disclose classified information to any third Party without the prior written consent of the Originating Party;

b) To ensure the classified information shall be marked at a security classification level equivalent to that provided by the Originating Party;

c) Not to use classified information for other purposes than those provided for;

d) To ensure the protection of classified information with the terms of duration as provided the Originating Party, unless otherwise requested in writing by the Originating Party.

Article 7

Translation, Reproduction and Destruction of Classified Information

1. Classified documents marked at TUYÊN MẬT/ລັບທီສຸດ/TOP SECRET security classification level shall only be reproduced with the written approval of the Originating Party.

2. All translations of classified information shall be made in accordance with the national laws and regulations of the respective Party. Such translation shall bear the same marking made by the Originating Party and be placed under the same protection as the original information.

3. When classified material is reproduced, all original security markings thereon shall also be reproduced. The procedure for reproduction of classified material shall be implemented in accordance with the laws and regulations of the respective Party. The reproduced classified material shall be placed under the same control as the original classified material. The number of copies shall be limited to that required for official purposes.

4. Classified material shall be destroyed or modified insofar as to prevent its reconstruction in whole or in part.

5. The Originating Party may prohibit the creation of copies, alterations or destruction of classified information by giving it an appropriate marking or by attaching a subsequent written notice. If the destruction of the classified material is prohibited, this material and the reproduced classified material shall be returned to the Originating Party.

6. Classified material of TUYÊN MẬT/ ລັບທັສຸດ/ TOP SECRET security classification level shall not be destroyed and shall be returned to the the Originating Party.

7. In case of force majeure situation, which makes it impossible to protect and return the provided classified material under this Agreement, the classified material shall be destroyed immediately. The Receiving Party shall notify the Originating Party about the destruction of the classified material as soon as possible.

Article 8

Classified Contracts

1. Classified contract shall be concluded and implemented in accordance with the national laws and regulations of the respective Party.

2. Each the signed classified contract under the provisions of this Agreement should be attached an annex including such information as follows:

- a) The instruction of classification and the list of classified information;
- b) The procedures for notifying any changes on the security classification level of the classified information;
- c) The channels to be used for communication;
- d) The procedures for transmission;
- e) The possible relevant authorities are responsible for the coordination in the protection of the classified information under the classified contracts;

f) The basic information about the possible individual, legal entity to be accessed the classified information and its function, responsibility;

3. The contractors' obligation to protect the classified information shall, in all cases, refer, at least, to the following:

a) Disclosure of the classified information only to individual, legal entity who takes part in the activities of classified contract and in accordance with "need-to-know" principle;

b) Making arrangement for the means to be used for the transmission of the classified material;

c) Ensuring the security classified level of the provided classified information to be unchanged unless authorized in writing by the Originating Party;

d) The notification about the changes that may arise in respect of classified information either because of changes in its security classification level or because protection is no longer necessary;

e) The announcement about the procedure for the approval of visits, access or inspection by personnel of one Party to facilities of the other Party which are covered by the contract;

f) The announcement in due time to the contractors of any actual, attempted or suspected unauthorized access to classified information of the contract;

g) Usage of the classified information under the classified contract only for the purposes related to the subject matter of the contract or the purposes for which it is provided and within any limitations stated by the Originating Party;

h) Strict adherence to the procedures for destruction of the classified material;

i) Supply of Classified information under the classified contract only to any third Party with the written consent of the Originating Party.

4. The measures required for the protection of classified information as well as the procedure for assessment and indemnification for possible losses caused to the contractors by unauthorized access to classified information shall be specified in more details in the respective classified contract.

Article 9

Breach of Security

1. In case of a breach of security, the competent authority in whose State a breach of security occurred shall inform the competent authority of the other Party as soon as possible and shall conduct the appropriate investigation. The other Party should, if so requested, cooperate in the investigation process.

2. In case of a breach of security occurs in a third country, the Competent Authority of the Originating Party shall take the actions referred to in paragraph 1 of this Article, when possible.

3. In any case, the competent authority of the Party in which the breach of security happened shall inform the other Party of the outcome of the investigation and of the reasons, extent of damage caused, and solutions for recovery.

4. The competent authority of the Party in which the breach of security happened shall take all appropriate measures under its national laws and regulations so as to limit the consequences of a breach of security and to prevent a recurrence.

Article 10

Visits

1. Experts of the Parties may hold regular meetings to discuss the procedures for protection of classified information.

2. The visitors shall be authorized by the sending Party to access to the classified information or to premises where classified information is originated, handled or stored and shall have prior written consent of the host Party.

3. Visiting procedures shall be agreed between the Parties.

4. The requesting Party shall provide by written the following information:

- a) Name of the visitor, date of birth, passport number;
- b) Nationality of the visitor;
- c) Title of the visitor and name of the agency represented by his/her;
- d) Purpose, proposed working program and planned date of the visit;

e) Names of agencies and facilities requested to be visited;
f) The visitors shall be required for written confirmation from the sending Party for accessing to the classified information or to premises where classified information is originated, handled or stored, scope, content of the accessed classified information in accordance with the national laws and regulations of the respective Party.

g) The classified information to be requested for having access by the visitors and the necessary time for this. The host Party shall inform about the security classification level of the information.

5. The Parties may agree to establish lists of authorized persons to make recurring visits. These lists shall be valid for an initial period of twelve months. Once those lists have been approved by the Parties, the terms of the specific visits shall be directly arranged with the appropriate authorities of the organizations to be visited by those persons, in accordance with the terms and conditions agreed upon.

6. Each Party shall guarantee the protection of personal data of the visitors, according to the respective national laws and regulations.

7. Each Party shall have the right to change the list of visitors and inform its reasons to the other Party.

Article 11

Expenses

Each Party shall bear the expenses incurred in the course of application and implementation of this Agreement under the regulations and laws of the respective Party.

Article 12

Final Provisions

1. This Agreement shall enter into force on the thirtieth day (30th) from the date of exchanging diplomatic notifications by the Parties to inform each other of the fulfillment of all internal legal procedures necessary for its entry into force.

2. This Agreement may be amended on the basis of mutual written consent by both Parties via diplomatic channel. Any amendment document and supplementary document shall constitute an integral part of this Agreement, and shall have equal legal validity as this Agreement. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

3. Each Party may terminate this Agreement by written notice forwarded to the other Party via diplomatic channel. The termination shall enter into force 180 days after the date of receipt of the last notification. Notwithstanding the termination of this Agreement, all provided classified information shall continue to be protected in accordance with the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

4. Any dispute regarding the interpretation or application of this Agreement shall be resolved amicably by consultation between the Parties without recourse to the jurisdiction of the third Party.

This Agreement is signed at Vientiane Capital, Lao PDR on the 29th of September 2023 in two original copies, each in the Vietnamese, Lao and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English version text shall prevail.

**FOR THE GOVERNMENT OF
THE SOCIALIST REPUBLIC OF
VIET NAM**



**General TO LAM
Minister of Public Security**

**FOR THE GOVERNMENT OF
THE LAO PEOPLE'S
DEMOCRATIC REPUBLIC**



**General Vilay LAKHAMPHONG
Deputy Prime Minister
and Minister of Public Security**

ສິນທິສັນຍາ

ວ່າດ້ວຍການຮັກສາ ແລະ ແລກປ່ຽນຂໍ້ມູນລັບ

ລະຫວ່າງ

ລັດຖະບານ ແຫ່ງ ສາທາລະນະລັດ ສັງຄົມນິຍົມຫວຽດນາມ

ແລະ

ລັດຖະບານ ແຫ່ງ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ

ສິນທິສັນຍາ
ວ່າດ້ວຍການຮັກສາ ແລະ ແລກປ່ຽນຂໍ້ມູນລັບ
ລະຫວ່າງ
ລັດຖະບານ ແຫ່ງ ສາທາລະນະລັດ ສັງຄົມນິຍົມຫວຽດນາມ
ແລະ
ລັດຖະບານ ແຫ່ງ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ

ລັດຖະບານແຫ່ງ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ ແລະ ສາທາລະນະລັດ ສັງຄົມນິຍົມ ຫວຽດນາມ (ຫຼັງຈາກນີ້ເອີ້ນລວມກັນວ່າ “ຄູ່ພາຄີ”);

ໂດຍເຫັນດີ ໃນການເປີດກວ້າງ ແລະ ຮັດແໜ້ນການຮ່ວມມືທາງດ້ານການເມືອງ, ເສດຖະກິດ ແລະ ການຈັດຕັ້ງເຈລະຈາ ກ່ຽວກັບບັນຫາທີ່ພົວພັນເຖິງການເມືອງ ແລະ ຄວາມສະຫງົບ;

ໂດຍຮັບຮູ້ເຖິງບົດບາດຄວາມສໍາຄັນ ຂອງການຮ່ວມມືທັງສອງຝ່າຍ ເພື່ອສັນຕິພາບ, ຄວາມໝັ້ນຄົງ ແລະ ການພັດທະນາ;

ໂດຍຮັບຮູ້ວ່າ ການຮ່ວມມືທີ່ດີ ເພື່ອເພີ່ມທະວີສາຍພົວພັນມິດຕະພາບ, ຄວາມສາມັກຄີແບບພິເສດ ແລະ ການຮ່ວມມືຮອບດ້ານລະຫວ່າງສອງລັດ ຊຶ່ງສາມາດກໍານົດໃຫ້ມີການຮຽກຮ້ອງການແລກປ່ຽນຂໍ້ມູນລັບເຊິ່ງ ກັນ ແລະ ກັນ;

ບົນພື້ນຖານຫຼັກການ ການເຄົາລົບເອກະລາດ, ອະທິປະໄຕ ແລະ ຜືນແຜ່ນດິນອັນຄົບຖ້ວນ, ບໍ່ແຊກ ແຊງກິດຈະການພາຍໃນຂອງກັນ ແລະ ກັນ, ສະເໝີພາບ ແລະ ຕ່າງຝ່າຍຕ່າງໄດ້ຮັບຜົນປະໂຫຍດ ຕາມການ ກໍານົດຂອງນິຕິກຳສາກົນ, ກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ;

ໂດຍປາຖະໜາ ສ້າງບັນດາລະບຽບການ ກ່ຽວກັບການຮັກສາຂໍ້ມູນລັບ ເພື່ອນໍາໃຊ້ເຂົ້າໃນສັນຍາຮ່ວມ ມືອື່ນໆໃນອານາຄົດ ແລະ ບັນດາສັນຍາລັບທີ່ຈະໄດ້ຈັດຕັ້ງປະຕິບັດລະຫວ່າງຄູ່ພາຄີ ທີ່ປະກອບມີ ຫຼື ພົວພັນ ເຖິງຂໍ້ມູນລັບ;

ໄດ້ຕົກລົງກັນດັ່ງນີ້:

ມາດຕາ 1
ຂອບເຂດການນໍາໃຊ້ແລະ ຈຸດປະສົງ

1. ສິນທິສັນຍາສະບັບນີ້ ໄດ້ກໍານົດຫຼັກການ ກ່ຽວກັບການຮັກສາ ແລະ ແລກປ່ຽນຂໍ້ມູນລັບລະຫວ່າງຄູ່ ພາຄີ, ໂດຍນໍາໃຊ້ກັບບັນດາອົງການຈັດຕັ້ງລັດ, ນິຕິບຸກຄົນ ແລະ ບຸກຄົນ ຂອງຄູ່ພາຄີທີ່ເຂົ້າຮ່ວມໃນການຮ່ວມມື ລະຫວ່າງສອງລັດ ຫຼື ການປະຕິບັດບັນດາສັນຍາທີ່ຢູ່ໃນຂອບເຂດຂອງສິນທິສັນຍາສະບັບນີ້ ໃນທຸກການເຄື່ອນໄຫວ ວຽກງານການຮ່ວມມືໃນການຮັກສາ ແລະ ແລກປ່ຽນຂໍ້ມູນລັບ.

2. ໃນຂົງເຂດການທະຫານ, ວຽກງານປ້ອງກັນຊາດ ແລະ ກົດລັບ ແມ່ນບໍ່ຢູ່ພາຍໃຕ້ຂອບເຂດຂອງສິນທິສັນຍາສະບັບນີ້.

3. ຈຸດປະສົງຂອງສິນທິສັນຍາສະບັບນີ້ເພື່ອຮັບປະກັນໄດ້ວຽກງານຮັກສາ ແລະ ແລກປ່ຽນຂໍ້ມູນລັບໃນໄລຍະການຮ່ວມມືຂອງຄູ່ພາຄີ.

ມາດຕາ 2

ອະທິບາຍຄຳສັບ

ຄຳສັບທີ່ນຳໃຊ້ໃນສິນທິສັນຍາສະບັບນີ້ ມີຄວາມໝາຍດັ່ງນີ້:

1. “ຂໍ້ມູນລັບ” ໝາຍເຖິງ ທຸກຂໍ້ມູນທີ່ຈັດຢູ່ໃນ ລັກສະນະ, ປະເພດ ຫຼື ຮູບແບບສິ່ງຂ່າວໃດໆກໍຕາມທີ່ໄດ້ສ້າງຂຶ້ນ ແລະ ໄດ້ຢັ້ງຢືນລະດັບຄວາມລັບ, ເພື່ອຜົນປະໂຫຍດຂອງຄວາມໝັ້ນຄົງຂອງຊາດ ແລະ ສອດຄ່ອງກັບກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ ເພື່ອໃຫ້ໄດ້ຮັບການປ້ອງກັນ ການສູນຫາຍ, ການລ່ວງລະເມີດ, ການເຂົ້າເຖິງແບບຜິດກົດໝາຍ, ການເປີດເຜີຍ, ທຳລາຍ ຫຼື ຮູບແບບອື່ນໆທີ່ກໍ່ໃຫ້ເກີດຄວາມເສຍຫາຍຕໍ່ຂໍ້ມູນລັບ.

2. “ເອກະສານລັບ” ໝາຍເຖິງ ເອກະສານທຸກຮູບແບບທີ່ບັນທຶກຂໍ້ມູນລັບ ຊຶ່ງບໍ່ລວມເຖິງຈຸດພິເສດຂອງຂໍ້ມູນລັບ ຫຼື ວິທີການບັນທຶກ.

3. “ວັດຖຸລັບ” ໝາຍເຖິງ ທຸກເອກະສານລັບ ຫຼື ອຸປະກອນເຕັກນິກ, ເຄື່ອງມື, ການຕິດຕັ້ງ, ເຄື່ອງຈັກ ຫຼື ອາວຸດທີ່ໄດ້ຜະລິດ ຫຼື ກຳລັງຢູ່ໃນຂັ້ນຕອນຜະລິດ, ກໍຄືບັນດາສ່ວນປະກອບໄດ້ນຳໃຊ້ເຂົ້າໃນການຜະລິດ ທີ່ລວມມີຂໍ້ມູນລັບ.

4. “ການເຂົ້າເຖິງຂໍ້ມູນລັບໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ” ໝາຍເຖິງ ການທີ່ບຸກຄົນ ຫຼື ນິຕິບຸກຄົນ ເຂົ້າເຖິງຂໍ້ມູນລັບ ໂດຍບໍ່ຖືກຕ້ອງຕາມກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ ແລະ ຂໍ້ກຳນົດພາຍໃຕ້ສິນທິສັນຍາສະບັບນີ້.

5. “ລະດັບຄວາມລັບ” ໝາຍເຖິງ ລະດັບ ຂອງຄວາມລັບ ຕາມທີ່ໄດ້ກຳນົດໃນກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີທີ່ເຫັນວ່າມີຄວາມສຳຄັນຂອງຂໍ້ມູນລັບ, ໂດຍໃຫ້ສອດຄ່ອງກັບມາດຕະການຄວາມປອດໄພສະເພາະທີ່ພົວພັນເຖິງການສ້າງ, ການເຂົ້າເຖິງ, ການດັດແກ້, ການເກັບຮັກສາສຳເນົາ ແລະ ການສະໜອງຂໍ້ມູນລັບດັ່ງກ່າວ.

6. “ເຄື່ອງໝາຍລັບ” ໝາຍເຖິງ ເຄື່ອງໝາຍທີ່ໄດ້ປະທັບໃສ່ວັດຖຸລັບ ທີ່ສະແດງໃຫ້ເຫັນເຖິງລະດັບຄວາມລັບ.

7. “ພາຄີຝ່າຍສິ່ງ” ໝາຍເຖິງ ລັດທີ່ສິ່ງຂໍ້ມູນລັບ.

8. “ພາຄີຝ່າຍຮັບ” ໝາຍເຖິງ ລັດທີ່ໄດ້ຮັບຂໍ້ມູນລັບ.

9. “ຜູ້ນຳໃຊ້” ໝາຍເຖິງ ບຸກຄົນ ຫຼື ນິຕິບຸກຄົນທີ່ໄດ້ຮັບອະນຸຍາດເຂົ້າເຖິງຂໍ້ມູນລັບ ຕາມກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ ທີ່ເຂົ້າຮ່ວມໃນບັນດາການເຄື່ອນໄຫວພົວພັນຮ່ວມມື ຫຼື ເຂົ້າຮ່ວມໃນການຈັດຕັ້ງປະຕິບັດ ບັນດາສັນຍາລັບ ທີ່ສິນທິສັນຍາສະບັບນີ້ຈະໄດ້ຖືກນຳໃຊ້.

10. “ອົງການທີ່ມີສິດອຳນາດ” ໝາຍເຖິງ ອົງການຈັດຕັ້ງລັດ ທີ່ໄດ້ກຳນົດໄວ້ຕາມກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ ເພື່ອຈັດຕັ້ງປະຕິບັດນະໂຍບາຍທັງໝົດຂອງລັດ ແນໃສ່ເພື່ອຮັກສາຂໍ້ມູນລັບ, ກໍ່ຄືການດຳເນີນການກວດກາການຜັນຂະຫຍາຍສິນທິສັນຍາສະບັບນີ້.

11. “ພາຄີຝ່າຍເຊັນສັນຍາ” ໝາຍເຖິງ ບຸກຄົນ ຫຼື ນິຕິບຸກຄົນທີ່ມີສິດອຳນາດຂອງພາຄີຝ່າຍໃດຝ່າຍໜຶ່ງ ມີສິດທາງດ້ານກົດໝາຍໃນການລົງນາມບັນດາສັນຍາ.

12. “ສັນຍາລັບ” ໝາຍເຖິງ ການຕົກລົງເຫັນດີເປັນລາຍລັກອັກສອນ ລະຫວ່າງ ຜູ້ນຳໃຊ້ຂອງຄູ່ພາຄີທີ່ພົວພັນເຖິງການສ້າງ, ການນຳໃຊ້, ການເຂົ້າເຖິງ, ການເກັບສຳເນົາ ຫຼື ການສະໜອງຂໍ້ມູນລັບ.

13. “ຫຼັກການ “ຈຳເປັນຕ້ອງຮູ້” ໝາຍເຖິງ ຫຼັກການທີ່ມີສິດເຂົ້າເຖິງຂໍ້ມູນລັບ ທີ່ໄດ້ມອບໝາຍໃຫ້ບຸກຄົນ ຫຼື ນິຕິບຸກຄົນ ທີ່ພົວພັນເຖິງໜ້າທີ່ຫຼັກສະເພາະ ແລະ ເພື່ອການປະຕິບັດໜ້າທີ່ຫຼັກສະເພາະອັນໃດໜຶ່ງ.

14. “ຝ່າຍທີ່ສາມ” ໝາຍເຖິງ ບຸກຄົນ, ນິຕິບຸກຄົນ, ອົງການຈັດຕັ້ງລັດ ຫຼື ອົງການຈັດຕັ້ງສາກົນໃດໜຶ່ງ ທີ່ບໍ່ແມ່ນຝ່າຍໃດໜຶ່ງ ໃນການລົງນາມສິນທິສັນຍາສະບັບນີ້ ຫຼື ລົງນາມສັນຍາລັບ.

15. “ຖອນລະຫັດລັບ” ແມ່ນການລົບລ້າງລະດັບຄວາມລັບ.

16. “ການລະເມີດຄວາມປອດໄພ” ແມ່ນການກະທຳ ຫຼື ບໍ່ກະທຳໃດໜຶ່ງ ທີ່ຜິດຕໍ່ກັບລະບຽບກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ, ທີ່ນຳໄປສູ່ ຫຼື ອາດຈະນຳໄປສູ່ ການເຂົ້າເຖິງຂໍ້ມູນແບບຜິດກົດໝາຍ, ເປີດເຜີຍ, ສູນເສຍ, ທຳລາຍ, ການຄອບຄອງແບບຜິດກົດໝາຍ ຫຼື ຮຸບແບບໃດກໍ່ຕາມ ທີ່ສາມາດກໍ່ໃຫ້ເກີດຄວາມເສຍຫາຍຂອງຂໍ້ມູນລັບໃນການແລກປ່ຽນ.

17. “ເຫດສຸດວິໄສ” ໝາຍເຖິງ ເຫດການ ຫຼື ສະພາບການທີ່ບໍ່ຄາດຄິດ ຊຶ່ງເປັນສາເຫດທີ່ເຮັດໃຫ້ພາຄີອີກຝ່າຍໜຶ່ງບໍ່ສາມາດຄວບຄຸມສະຖານະການໄດ້, ເຮັດໃຫ້ພາຄີຝ່າຍໜຶ່ງບໍ່ສາມາດປະຕິບັດ ຫຼື ປະຕິບັດບໍ່ໄດ້ເລີຍຕາມພັນທະຂອງຕົນພາຍໃຕ້ສິນທິສັນຍາສະບັບນີ້.

ມາດຕາ 3

ລະດັບຄວາມລັບ

ຄູ່ພາຄີເຫັນດີເປັນເອກະພາບວ່າລະດັບຄວາມລັບຕໍ່ໄປນີ້ແມ່ນມີຄວາມກ່ຽວຂ້ອງແລະ ສອດຄ່ອງກັບບັນດາລະດັບຄວາມລັບຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ:

ສຳລັບ ສປປ ລາວ	ສຳລັບສສ ຫວຽດນາມ	ພາສາອັງກິດ
ລັບທີ່ສຸດ	TUYỆT MẬT	TOP SECRET
ລັບສະເພາະ	TỐI MẬT	SECRET
ລັບ	MẬT	CONFIDENTIAL

ມາດຕາ 4
ອົງການທີ່ມີສິດອຳນາດ

1. ອົງການທີ່ມີສິດອຳນາດຂອງຄູ່ພາຄືແມ່ນ:
 - ສຳລັບ ສາທາລະນະລັດ ສັງຄົມນິຍົມຫວຽດນາມ: ກະຊວງປ້ອງກັນຄວາມສະຫງົບ.
 - ສຳລັບ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ: ກະຊວງປ້ອງກັນຄວາມສະຫງົບ.
2. ຄູ່ພາຄືຈະຕ້ອງແຈ້ງໃຫ້ກັນຊາບໂດຍຜ່ານຊ່ອງທາງການທູດກ່ຽວກັບການປ່ຽນແປງຕໍ່ກັບອົງການທີ່ມີສິດອຳນາດ.
3. ອົງການທີ່ມີສິດອຳນາດຈະຕ້ອງແຈ້ງໃຫ້ຄູ່ພາຄືຊາບກ່ຽວກັບການນຳໃຊ້ກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຕົນ ທີ່ກຳນົດເຖິງການຮັກສາຂໍ້ມູນລັບ.
4. ເພື່ອຮັບປະກັນໃຫ້ແກ່ການຮ່ວມມືທີ່ແໜ້ນແຟ້ນໃນໄລຍະການປະຕິບັດສົນທິສັນຍາສະບັບນີ້, ບັນດາອົງການທີ່ມີສິດອຳນາດສາມາດຈັດຕັ້ງການປຶກສາຫາລືຕາມການສະເໜີຂອງຄູ່ພາຄືໃດໜຶ່ງ.
5. ເພື່ອບັນລຸຈຸດປະສົງແລະຮັກສາໄດ້ມາດຕະຖານຄວາມປອດໄພທີ່ເທົ່າທຽມກັນ, ບັນດາອົງການທີ່ມີສິດອຳນາດຈະຕ້ອງສະໜອງຂໍ້ມູນເຊິ່ງກັນແລະກັນຕາມການສະເໜີກ່ຽວກັບມາດຖານຄວາມປອດໄພ, ຂັ້ນຕອນແລະ ການປະຕິບັດ ຕໍ່ກັບວຽກງານການຮັກສາຂໍ້ມູນລັບທີ່ໄດ້ນຳໃຊ້ໃຫ້ຄູ່ພາຄື.
6. ອົງການທີ່ມີສິດອຳນາດຂອງຄູ່ພາຄືສາມາດເຊັນເອກະສານທາງດ້ານບໍລິຫານທີ່ພົວພັນເຖິງການຈັດຕັ້ງປະຕິບັດສົນທິສັນຍາສະບັບນີ້.
7. ອົງການທີ່ມີສິດອຳນາດຂອງຄູ່ພາຄື ຈະຕ້ອງຮັບປະກັນການຈັດຕັ້ງປະຕິບັດສົນທິສັນຍາສະບັບນີ້ຢ່າງເຂັ້ມງວດກັບບັນດາອົງການຈັດຕັ້ງລັດ, ນິຕິບຸກຄົນ, ບຸກຄົນ ທີ່ເຂົ້າຮ່ວມໃນການຮ່ວມມື ລະຫວ່າງສອງລັດ ຫຼື ປະຕິບັດບັນດາສັນຍາທີ່ຢູ່ໃນຂອບເຂດຂອງສົນທິສັນຍາສະບັບນີ້.

ມາດຕາ 5
ການສົ່ງຂໍ້ມູນລັບ

1. ຂໍ້ມູນລັບຈະຖືກສົ່ງຜ່ານຊ່ອງທາງການທູດ ຫຼື ຊ່ອງທາງອື່ນຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄື ແລະຕ້ອງໄດ້ຮັບການເຫັນດີຂອງທັງສອງຝ່າຍ. ເມື່ອພາຄືຝ່າຍຮັບໄດ້ຮັບຂໍ້ມູນລັບແລ້ວຈະຕ້ອງແຈ້ງເປັນລາຍລັກອັກສອນໃຫ້ພາຄືຝ່າຍສົ່ງຊາບ.
2. ສຳລັບຂໍ້ມູນທີ່ໄດ້ຈັດຢູ່ໃນປະເພດ ລັບທີ່ສຸດຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນມາດຕາ 3 ຈະຕ້ອງສົ່ງຜ່ານຊ່ອງທາງການທູດເທົ່ານັ້ນ.

3. ໃນກໍລະນີ ສິ່ງມອບພັດສະດຸຂະໜາດໃຫຍ່ ທີ່ບັນຈຸວັດຖຸລັບ, ອົງການທີ່ມີສິດອຳນາດຈະຕ້ອງເຫັນດີ ເປັນເອກະພາບກັນໃນການອະນຸມັດກ່ຽວກັບພາຫະນະການຂົນສົ່ງ, ເສັ້ນທາງແລະ ມາດຕະການດ້ານຄວາມ ປອດໄພອື່ນໆ.

4. ໃນກໍລະນີພາຄີຝ່າຍໃດໜຶ່ງ ມີບ່ອນອື່ງ ໃນການຈັດຕັ້ງປະຕິບັດຕາມຄໍາຮ້ອງຂໍໃນການສົ່ງຂໍ້ມູນລັບທີ່ອາດຈະ ສ້າງຄວາມເສຍຫາຍ ໃຫ້ແກ່ອະທິປະໄຕ ແລະ ຄວາມສະຫງົບພາຍໃນ ຫຼື ຂັດຕໍ່ກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງແຕ່ ລະຝ່າຍ ລວມທັງພັນທະສາກົນ ແມ່ນສາມາດປະຕິເສດຕໍ່ຄໍາຮ້ອງຂໍການສົ່ງຂໍ້ມູນລັບ ແລະ ແຈ້ງໃຫ້ຝ່າຍຮ້ອງຂໍຊາບ ເປັນລາຍລັກອັກສອນ ກ່ຽວກັບເຫດຜົນໃນການປະຕິເສດ.

ມາດຕາ 6

ມາດຕະການຮັກສາຂໍ້ມູນລັບ

1. ສອດຄ່ອງກັບກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ, ຄູ່ພາຄີຈະຕ້ອງຜັນຂະຫຍາຍນຳໃຊ້ທຸກມາດ ຕະການທີ່ສອດຄ່ອງເພື່ອຮັກສາຂໍ້ມູນລັບທີ່ໄດ້ຖືກສົ່ງຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນສົນທິສັນຍາສະບັບນີ້. ຂໍ້ມູນລັບທີ່ ໄດ້ຖືກສົ່ງນັ້ນຈະຕ້ອງໄດ້ຮັບການຮັກສາຄືກັນກັບລະດັບຄວາມລັບຂອງພາຄີຝ່າຍຮັບ.

2. ຄູ່ພາຄີຈະຕ້ອງແຈ້ງໃຫ້ກັນຊາບຢ່າງທັນການກ່ຽວກັບການປ່ຽນແປງກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງ ຕົນທີ່ມີຜົນກະທົບຕໍ່ກັບວຽກງານການຮັກສາຂໍ້ມູນລັບ. ໃນກໍລະນີດັ່ງກ່າວຄູ່ພາຄີຈະຕ້ອງແຈ້ງໃຫ້ກັນຊາບ ເພື່ອ ປຶກສາຫາລືເຖິງຄວາມເປັນໄປໄດ້ ໃນການດັດແກ້ສົນທິສັນຍາສະບັບນີ້. ໃນຊ່ວງໄລຍະນັ້ນ, ຂໍ້ມູນລັບຈະຕ້ອງໄດ້ ຮັບການເກັບຮັກສາໄວ້ ຕາມຂໍ້ກຳນົດຂອງສົນທິສັນຍາສັນຍາສະບັບນີ້, ຈົນກວ່າຈະມີການຕົກລົງເຫັນດີເປັນລາຍ ລັກອັກສອນ.

3. ຫ້າມບຸກຄົນໃດ ສວຍໃຊ້ໜ້າທີ່ຕໍາແໜ່ງ ໃນການເຂົ້າເຖິງຂໍ້ມູນລັບ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ, ການເຂົ້າ ເຖິງຂໍ້ມູນລັບໄດ້ຈຳກັດສະເພາະບຸກຄົນ, ນິຕິບຸກຄົນ ໃຫ້ສອດຄ່ອງກັບ ຫຼັກການ “ຈຳເປັນຕ້ອງຮູ້” ຕາມທີ່ໄດ້ກຳ ນົດໄວ້ໃນມາດຕາ 2. ການອະນຸຍາດໃຫ້ເຂົ້າເຖິງຂໍ້ມູນລັບຕ້ອງປະຕິບັດຕາມກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງ ຄູ່ພາຄີ.

4. ພາຄີຝ່າຍສົ່ງມີພັນທະປະຕິບັດດັ່ງນີ້:

ກ. ຮັບປະກັນຂໍ້ມູນລັບ ຕ້ອງປະທັບຕາ ເຄື່ອງໝາຍລັບ ໃຫ້ສອດຄ່ອງຕາມກົດໝາຍ ແລະ ນິຕິກຳພາຍ ໃນ ຂອງພາຄີຝ່າຍສົ່ງກຳນົດ.

ຂ. ແຈ້ງໃຫ້ພາຄີຝ່າຍຮັບ ຊາບ ກ່ຽວກັບທຸກເງື່ອນໄຂ ໃນການສົ່ງ ຫຼື ຂອບເຂດຈຳກັດ ໃນການນຳໃຊ້ຂໍ້ ມູນລັບ ທີ່ສົ່ງໃຫ້ ແລະ ທຸກການປ່ຽນແປງ ໃນການຈັດປະເພດຮັກສາຂໍ້ມູນລັບ.

5. ພາຄີຝ່າຍຮັບມີພັນທະປະຕິບັດດັ່ງນີ້:

ກ. ຫ້າມເປີດເຜີຍ, ສົ່ງຂໍ້ມູນທີ່ເປັນຄວາມລັບໃຫ້ແກ່ຝ່າຍທີ່ສາມໂດຍທີ່ບໍ່ໄດ້ຮັບການເຫັນດີທີ່ເປັນລາຍ ລັກອັກສອນກ່ອນລ່ວງໜ້າຈາກພາຄີຝ່າຍທີ່ສົ່ງຂໍ້ມູນ.

ຂ. ຮັບປະກັນຂໍ້ມູນລັບ ຕ້ອງປະທັບຕາເຄື່ອງໝາຍລັບ ໃຫ້ຄືກັນກັບເຄື່ອງໝາຍລັບ ທີ່ພາຄີຝ່າຍສົ່ງເປັນຜູ້ກຳນົດ.

ຄ. ຫ້າມນຳໃຊ້ຂໍ້ມູນລັບເພື່ອຈຸດປະສົງອື່ນ ນອກຈາກຈຸດປະສົງທີ່ໄດ້ກຳນົດໄວ້ແລ້ວ.

ງ. ຮັບປະກັນໃນການຮັກສາຂໍ້ມູນລັບ ຕໍ່ກັບໄລຍະເວລາທີ່ພາຄີຝ່າຍສົ່ງເປັນຜູ້ກຳນົດ, ຍົກເວັ້ນໃນກໍລະນີທີ່ມີຄຳຮ້ອງຂໍອື່ນ ເປັນລາຍລັກອັກສອນຈາກພາຄີຝ່າຍສົ່ງ.

ມາດຕາ 7

ການແປ, ສຳເນົາ ແລະ ທຳລາຍຂໍ້ມູນລັບ

1. ວັດຖຸລັບທີ່ໄດ້ປະທັບເຄື່ອງໝາຍ TUYỆT MẬT/ ລັບທີ່ສຸດ/TOP SECRET ຈະສຳເນົາໄດ້ກໍ່ຕໍ່ເມື່ອມີການເຫັນດີ ໂດຍການຢັ້ງຢືນເປັນລາຍລັກອັກສອນຈາກພາຄີຝ່າຍສົ່ງ.

2. ການແປຂໍ້ມູນລັບ ຕ້ອງປະຕິບັດຕາມກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ. ສະບັບທີ່ຖືກແປນັ້ນ ພາຄີຝ່າຍຮັບຕ້ອງໄດ້ປະທັບຕາເຄື່ອງໝາຍລັບ ຄືກັນກັບເຄື່ອງໝາຍລັບຂອງພາຄີຝ່າຍສົ່ງກຳນົດ ແລະ ຕ້ອງໄດ້ເກັບຮັກສາໄວ້ຄືກັບສະບັບຕົ້ນ.

3. ເມື່ອວັດຖຸລັບໄດ້ຮັບການສຳເນົາ, ບັນດາເຄື່ອງໝາຍລັບທັງໝົດຈະຕ້ອງຖືກສຳເນົາ. ຂັ້ນຕອນການສຳເນົາວັດຖຸລັບຈະຕ້ອງປະຕິບັດຕາມກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ. ການສຳເນົາວັດຖຸລັບຈະຕ້ອງປະຕິບັດຄືກັນກັບສະບັບຕົ້ນ. ການສຳເນົາຕ້ອງມີຈຳນວນຈຳກັດ ຕາມຈຸດປະສົງຂອງວຽກງານທາງການ.

4. ວັດຖຸລັບຈະຖືກທຳລາຍ ຫຼື ດັດແກ້ ເພື່ອປ້ອງກັນການນຳມາເຮັດຄືນໃໝ່ ທັງໝົດ ຫຼື ບາງສ່ວນ.

5. ພາຄີຝ່າຍສົ່ງສາມາດລະບຸຈະແຈ້ງ ກ່ຽວກັບການຫ້າມໃນການສຳເນົາ, ປ່ຽນແປງ ຫຼື ທຳລາຍວັດຖຸລັບ ໂດຍການປະທັບຕາເຄື່ອງໝາຍໃສ່ວັດຖຸລັບ ໃນບ່ອນທີ່ເໝາະສົມ ຫຼື ສົ່ງເປັນໜັງສືແຈ້ງມາພາຍຫຼັງ. ຖ້າໃນກໍລະນີວັດຖຸລັບຖືກກຳນົດ ຫ້າມທຳລາຍວັດຖຸລັບດັ່ງກ່າວ ແລະ ວັດຖຸລັບທີ່ໄດ້ສຳເນົາ ຈະຕ້ອງຖືກສົ່ງກັບຄືນໃຫ້ພາຄີຝ່າຍສົ່ງ.

6. ວັດຖຸລັບ TUYỆT MẬT / ລັບທີ່ສຸດ/TOP SECRET ແມ່ນບໍ່ອະນຸຍາດໃຫ້ທຳລາຍ ແລະ ຕ້ອງໄດ້ສົ່ງຄືນໃຫ້ພາຄີຝ່າຍສົ່ງ.

7. ໃນກໍລະນີທີ່ມີເຫດຈຳເປັນ ທີ່ບໍ່ສາມາດເກັບຮັກສາ ແລະ ສົ່ງຄືນວັດຖຸລັບທີ່ໄດ້ຮັບນັ້ນ ຕາມທີ່ໄດ້ກຳໄວ້ໃນສັນຍາສະບັບນີ້, ຂໍ້ມູນລັບຕ້ອງຖືກທຳລາຍໃນທັນທີ. ພາຄີຝ່າຍຮັບຕ້ອງແຈ້ງໃຫ້ພາຄີຝ່າຍສົ່ງຊາບ ກ່ຽວກັບການທຳລາຍວັດຖຸລັບດັ່ງກ່າວໃນທັນທີ.

ມາດຕາ 8

ສັນຍາລັບ

1. ສັນຍາລັບຈະຕ້ອງລົງນາມ ແລະ ຈັດຕັ້ງປະຕິບັດໃຫ້ສອດຄ່ອງກັບກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ.

2. ທຸກສັນຍາລັບທີ່ໄດ້ລົງນາມ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນສັນຍາສະບັບນີ້ຕ້ອງມີເອກະສານຊ້ອນທ້າຍ ຄັດຕິດ ຊຶ່ງມີເນື້ອໃນຂໍ້ມູນດັ່ງນີ້:

ກ. ຄຳແນະນຳການຈັດປະເພດ ແລະ ບັນຊີລາຍການຂອງຂໍ້ມູນລັບ;

ຂ. ບັນດາຂັ້ນຕອນໃນການແຈ້ງ ຕໍ່ກັບການປ່ຽນແປງໃດໜຶ່ງ ກ່ຽວກັບລະດັບການຮັກສາຂອງຂໍ້ມູນລັບ;

ຄ. ຊ່ອງທາງການຕິດຕໍ່;

ງ. ຂັ້ນຕອນການຂົນສົ່ງ;

ຈ. ບັນດາອົງການທີ່ມີໜ້າທີ່ຮັບຜິດຊອບ ກ່ຽວກັບການປະສານໃນການຮັກສາຂໍ້ມູນລັບທີ່ໄດ້ກຳນົດໄວ້ ໃນສັນຍາລັບ;

ສ. ຂໍ້ມູນພື້ນຖານຂອງບຸກຄົນ, ນິຕິບຸກຄົນທີ່ກ່ຽວຂ້ອງ ທີ່ຈະເຂົ້າເຖິງຂໍ້ມູນລັບ ແລະ ບົດບາດໜ້າທີ່, ໜ້າທີ່ຮັບຜິດຊອບ ຂອງບັນດານິຕິບຸກຄົນດັ່ງກ່າວ;

3. ພັນທະໃນການຮັກສາຂໍ້ມູນລັບຂອງທັງສອງຝ່າຍທີ່ລົງນາມໃນສັນຍາລັບໃນທຸກກໍລະນີ ຢ່າງໜ້ອຍຕ້ອງ ມີພື້ນຖານດັ່ງນີ້:

ກ. ເປີດເຜີຍລາຍລະອຽດຂອງຂໍ້ມູນລັບໃຫ້ບຸກຄົນ, ນິຕິບຸກຄົນ ທີ່ເຂົ້າຮ່ວມໃນການຈັດຕັ້ງປະຕິບັດ ສັນຍາລັບ ແລະ ໃຫ້ສອດຄ່ອງກັບຫຼັກການ “ຈຳເປັນຕ້ອງຮູ້”;

ຂ. ຈັດພາຫະນະທີ່ນຳໃຊ້ໃນການຂົນສົ່ງວັດຖຸລັບ;

ຄ. ຮັບປະກັນລະດັບຄວາມລັບຂອງຂໍ້ມູນລັບທີ່ໄດ້ສົ່ງນັ້ນ ບໍ່ໃຫ້ຖືກປ່ຽນແປງ, ຍົກເວັ້ນໄດ້ຮັບ ອະນຸຍາດຈາກພາຄີຝ່າຍສົ່ງເປັນລາຍລັກອັກສອນ;

ງ. ແຈ້ງກ່ຽວກັບການປ່ຽນແປງທີ່ເກີດຂຶ້ນ ທີ່ພົວພັນເຖິງຂໍ້ມູນລັບ ເຮັດໃຫ້ມີການປ່ຽນແປງຂອງລະດັບ ຄວາມລັບ ຫຼື ບໍ່ຈຳເປັນຕ້ອງມີການຮັກສາຂໍ້ມູນລັບຕໍ່ໄປອີກ;

ຈ. ແຈ້ງກ່ຽວກັບຂັ້ນຕອນການອະນຸມັດໃນການຢັ້ງຢືນຢາມ, ເຂົ້າເຖິງ ຫຼື ກວດກາ ໂດຍເຈົ້າໜ້າທີ່ຂອງ ຝ່າຍໜຶ່ງກັບບັນດາພາກສ່ວນທີ່ກ່ຽວຂ້ອງຂອງອີກຝ່າຍ ເພື່ອອຳນວຍຄວາມສະດວກຕາມທີ່ໄດ້ລະບຸໄວ້ໃນສັນຍາ ລັບ;

ສ. ແຈ້ງໃຫ້ຝ່າຍລົງນາມສັນຍາຊາບຢ່າງທັນການກ່ຽວກັບທຸກການເຂົ້າເຖິງຂໍ້ມູນລັບ, ການພະຍາຍາມ ລັກລອບເຂົ້າເຖິງ ຫຼື ກໍລະນີສົງໄສມີການເຂົ້າເຖິງຂໍ້ມູນລັບຂອງສັນຍາ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;

ຊ. ນຳໃຊ້ຂໍ້ມູນລັບໃນສັນຍາລັບເພື່ອຈຸດປະສົງທີ່ພົວພັນເຖິງເນື້ອໃນຂອງສັນຍາລັບເທົ່ານັ້ນ ຫຼື ຂໍ້ມູນລັບ ທີ່ສົ່ງໃຫ້ນັ້ນ ໄດ້ກຳນົດຂອບເຂດຈຳກັດ ທີ່ກຳນົດໂດຍພາຄີຝ່າຍສົ່ງ;

ຍ. ປະຕິບັດຂັ້ນຕອນໃນການທຳລາຍວັດຖຸລັບຢ່າງເຂັ້ມງວດ;

ດ. ສະໜອງຂໍ້ມູນລັບໃນສັນຍາລັບ ໃຫ້ຝ່າຍທີສາມ ຖ້າມີການເຫັນດີເປັນເອກະພາບທີ່ເປັນລາຍລັກ ອັກສອນຂອງພາຄີຝ່າຍສົ່ງ.

4. ບັນດາມາດຕະການທີ່ຈຳເປັນສຳລັບການຮັກສາຂໍ້ມູນລັບ ກໍຄືລະບຽບຂັ້ນຕອນເພື່ອຕິລາຄາ ແລະ ຮັບຮູ້ ເຖິງຄວາມເປັນໄປໄດ້ ຂອງການສູນເສຍທີ່ອາດຈະເກີດຂຶ້ນ ໃນການລົງນາມສັນຍາລັບຂອງທັງສອງຝ່າຍ ໂດຍ ການເຂົ້າເຖິງຂໍ້ມູນລັບທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດຈະໄດ້ກຳນົດລະອຽດໃນສັນຍາລັບທີ່ກ່ຽວຂ້ອງ.

ມາດຕາ 9

ການລະເມີດຄວາມປອດໄພ

1. ໃນກໍລະນີທີ່ມີການລະເມີດດ້ານຄວາມປອດໄພ, ອົງການທີ່ມີສິດອຳນາດຂອງຝ່າຍໃດໜຶ່ງທີ່ເກີດມີການ ລະເມີດຄວາມປອດໄພນັ້ນ ຕ້ອງແຈ້ງໃຫ້ອົງການທີ່ມີສິດອຳນາດຂອງອີກຝ່າຍຊາບຢ່າງທັນການແລະ ດຳເນີນ ການສືບສວນ-ສອບສວນຢ່າງເໝາະສົມ. ພາຄີອີກຝ່າຍຈະຕ້ອງຮ່ວມມືໃນການສືບສວນ-ສອບສວນນັ້ນ, ຖ້າໄດ້ ຮັບການຮ້ອງຂໍ.

2. ໃນກໍລະນີທີ່ມີການລະເມີດດ້ານຄວາມປອດໄພ ທີ່ເກີດຂຶ້ນຢູ່ລັດທີ່ສາມ, ອົງການທີ່ມີສິດອຳນາດຂອງ ພາຄີຝ່າຍສິ່ງຈະປະຕິບັດຕາມຮູບການ ຕາມທີ່ໄດ້ກຳນົດຢູ່ໃນ ຂໍ້ 1 ຂອງມາດຕານີ້.

3. ໃນທຸກໆກໍລະນີ, ອົງການທີ່ມີສິດອຳນາດຂອງຝ່າຍທີ່ເກີດມີການລະເມີດດ້ານຄວາມປອດໄພນັ້ນຕ້ອງ ແຈ້ງໃຫ້ອີກຝ່າຍຊາບກ່ຽວກັບຜົນຂອງການສືບສວນ-ສອບສວນ, ສາເຫດ, ລະດັບຄວາມເສຍຫາຍທີ່ເກີດຂຶ້ນ ແລະ ວິທີການແກ້ໄຂ.

4. ອົງການທີ່ມີສິດອຳນາດຂອງຝ່າຍໃດໜຶ່ງທີ່ເກີດມີການລະເມີດດ້ານຄວາມປອດໄພນັ້ນ ຕ້ອງປະຕິບັດທຸກ ມາດຕະການ ທີ່ສອດຄ່ອງກັບກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຕົນ ເພື່ອຈຳກັດຜົນເສຍຫາຍຂອງການລະເມີດ ດ້ານຄວາມປອດໄພ ແລະ ເພື່ອປ້ອງກັນການລະເມີດຕື່ມອີກ.

ມາດຕາ 10

ການຢັ້ງຢືນຢາມ

1. ບັນດາຜູ້ຊ່ຽວຊານຂອງຄູ່ພາຄີ ສາມາດຈັດຕັ້ງການພົບປະເປັນແຕ່ລະໄລຍະເພື່ອແລກປ່ຽນກ່ຽວກັບບັນ ດາລະບຽບຂັ້ນຕອນ ໃນການຮັກສາຂໍ້ມູນລັບ.

2. ບັນດາບຸກຄົນທີ່ເດີນທາງມາຢັ້ງຢືນຢາມ ຕ້ອງໄດ້ຮັບອະນຸຍາດໂດຍພາຄີຝ່າຍສິ່ງ ໃນການເຂົ້າເຖິງຂໍ້ມູນລັບ ຫຼື ເຂົ້າເຖິງອົງການທີ່ ສ້າງ, ແກ້ໄຂ ຫຼື ເກັບຮັກສາ ຂໍ້ມູນລັບ ແລະ ຕ້ອງໄດ້ຮັບອະນຸຍາດເປັນລາຍລັກອັກສອນ ຈາກພາຄີທີ່ຮັບ.

3. ບັນດາຂັ້ນຕອນໃນການຢັ້ງຢືນຢາມ ຕ້ອງໄດ້ຮັບຄວາມເປັນເອກະພາບລະຫວ່າງຄູ່ພາຄີ.

4. ຝ່າຍເດີນທາງມາຢັ້ງຢືນຢາມ ຕ້ອງສະໜອງບັນດາເອກະສານທີ່ມີຂໍ້ມູນ ດັ່ງນີ້:

- ກ) ຊື່ ແລະ ນາມສະກຸນ, ວັນເດືອນປີເກີດ, ເລກທີໜັງສືຜ່ານແດນ ຂອງບຸກຄົນທີ່ມາຢັ້ງຢືນຢາມ;
- ຂ) ສັນຊາດຂອງບຸກຄົນທີ່ມາຢັ້ງຢືນຢາມ;

ຄ) ໜ້າທີ່ດຳແໜ່ງຂອງບຸກຄົນທີ່ມາຢ້ຽມຢາມ ແລະ ຊື່ອົງການທີ່ບຸກຄົນດັ່ງກ່າວຕາງໜ້າ;

ງ) ຈຸດປະສົງ, ແຜນຄາດກະການເຮັດວຽກ ແລະ ໄລຍະເວລາຂອງການມາຢ້ຽມຢາມ;

ຈ) ຊື່ສຳນັກງານອົງການ ແລະ ສະຖານທີ່ທີ່ຈະໄປຢ້ຽມຢາມ;

ສ) ສອດຄ່ອງກັບກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ, ບຸກຄົນທີ່ມາຢ້ຽມຢາມ ຕ້ອງໄດ້ຮັບການຢັ້ງຢືນເປັນລາຍລັກອັກສອນຈາກຝ່າຍສົ່ງ ໃນການອະນຸຍາດໃຫ້ເຂົ້າເຖິງຂໍ້ມູນລັບ ຫຼື ການເຂົ້າເຖິງອົງການທີ່ ສ້າງ, ແກ້ໄຂ ຫຼື ເກັບຮັກສາ ຂໍ້ມູນລັບ, ຂອບເຂດ, ເນື້ອໃນ ຂອງບັນດາຂໍ້ມູນລັບ ທີ່ໄດ້ຮັບອະນຸຍາດເຂົ້າເຖິງ.

ຊ) ຂໍ້ມູນລັບທີ່ບຸກຄົນມາຢ້ຽມຢາມຕ້ອງການເຂົ້າເຖິງ ແລະ ໄລຍະເວລາ ກ່ຽວກັບການເຂົ້າເຖິງຂໍ້ມູນດັ່ງກ່າວ. ພາຄີຝ່າຍຮັບຈະຕ້ອງແຈ້ງ ກ່ຽວກັບລະດັບຄວາມລັບ ເພື່ອຮັບປະກັນໃນດ້ານຄວາມປອດໄພຂອງຂໍ້ມູນ.

5. ຄູ່ພາຄີ ສາມາດຕົກລົງກັນ ເພື່ອນຳເອົາບັນຊີລາຍຊື່ບັນດາບຸກຄົນທີ່ໄດ້ຖືກມອບສິດເພື່ອກະກຽມຄວາມພ້ອມໃນການມາຢ້ຽມຢາມຂອງແຕ່ລະໄລຍະ, ບັນດາລາຍຊື່ນັ້ນ ມີຜົນນຳໃຊ້ໄດ້ພາຍໃນ 12 ເດືອນ. ເມື່ອບັນດາລາຍຊື່ນັ້ນໄດ້ຮັບອະນຸມັດຈາກຄູ່ພາຄີແລ້ວ, ໄລຍະເວລາຂອງການມາຢ້ຽມຢາມຕົວຈິງນັ້ນ ຈະໄດ້ມີການກະກຽມກັບເຈົ້າໜ້າທີ່ທີ່ຮັບຜິດຊອບຂອງບັນດາການຈັດຕັ້ງ ທີ່ບຸກຄົນດັ່ງກ່າວຈະມາຢ້ຽມຢາມ ໃຫ້ແທດເໝາະກັບເວລາ ແລະ ເງື່ອນໄຂທີ່ໄດ້ຕົກລົງເປັນເອກະພາບກັນ.

6. ຄູ່ພາຄີຈະຕ້ອງຮັບປະກັນໃນການຮັກສາຂໍ້ມູນສ່ວນຕົວຂອງບຸກຄົນທີ່ມາຢ້ຽມຢາມ, ໃຫ້ສອດຄ່ອງກັບກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ.

7. ຄູ່ພາຄີມີສິດທີ່ຈະປ່ຽນແປງບັນຊີລາຍຊື່ບັນດາບຸກຄົນທີ່ຈະມາຢ້ຽມຢາມ ແລະ ແຈ້ງເຫດຜົນໃຫ້ອົກຝ່າຍຊາບ.

ມາດຕາ 11

ຄ່າໃຊ້ຈ່າຍ

ຄູ່ພາຄີຈະຕ້ອງໄດ້ຮັບຜິດຊອບຄ່າໃຊ້ຈ່າຍຂອງຕົນທີ່ເກີດຂຶ້ນ ໃນການນຳໃຊ້ແລະ ຈັດຕັ້ງປະຕິບັດຂອງສົນທິສັນຍາສະບັບນີ້ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ ແລະ ນິຕິກຳພາຍໃນຂອງຄູ່ພາຄີ.

ມາດຕາ 12

ບົດບັນຍັດສຸດທ້າຍ

1. ສົນທິສັນຍາສະບັບນີ້ ຈະມີຜົນບັງຄັບໃຊ້ພາຍຫຼັງ 30 ວັນ ຫຼັງຈາກທີ່ສອງຝ່າຍໄດ້ແລກປ່ຽນສານທາງການທຸດເພື່ອແຈ້ງໃຫ້ກັນຊາບ ກ່ຽວກັບການສຳເລັດບັນດາຂັ້ນຕອນພາຍໃນທີ່ຈຳເປັນເພື່ອໃຫ້ສົນທິສັນຍາມີຜົນສັກສິດ.

2. ສົນທິສັນຍາສະບັບນີ້ ອາດຈະໄດ້ຮັບການປັບປຸງບົນພື້ນຖານການຕົກລົງເຫັນດີເປັນລາຍລັກອັກສອນຂອງທັງສອງຝ່າຍໂດຍຜ່ານຊ່ອງທາງການທຸດ. ເອກະສານສະບັບປັບປຸງ, ເພີ່ມຕື່ມຂອງສົນທິສັນຍາ ແມ່ນສ່ວນໜຶ່ງຂອງ

ສິນທິສັນຍາ ແລະ ມີຜົນບັງຄັບໃຊ້ຄືກັນກັບສະບັບຕົ້ນ. ການປັບປຸງດັ່ງກ່າວຈະມີຜົນບັງຄັບໃຊ້ຕາມທີ່ໄດ້ລະບຸໄວ້ໃນຂໍ້ 1 ຂອງມາດຕານີ້.

3. ຄູ່ພາຄີສາມາດຍົກເລີກສິນທິສັນຍາດ້ວຍການແຈ້ງເປັນລາຍລັກອັກສອນໃຫ້ອີກຝ່າຍຊາບໂດຍຜ່ານຊ່ອງທາງການທຸດ. ການຍົກເລີກສິນທິສັນຍາຈະມີຜົນບັງຄັບໃຊ້ພາຍຫຼັງ 180 ວັນນັບແຕ່ວັນທີ່ໄດ້ຮັບໜັງສືແຈ້ງ. ເຖິງວ່າສິນທິສັນຍາສະບັບນີ້ຈະສິ້ນສຸດລົງ, ທຸກຂໍ້ມູນລັບທີ່ໄດ້ສົ່ງຕາມສິນທິສັນຍາສະບັບນີ້ຈະຍັງສືບຕໍ່ໄດ້ຮັບການຮັກສາຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນສິນທິສັນຍາສະບັບນີ້ ຈົນກວ່າພາຄີຝ່າຍລິ້ງຈະແຈ້ງໃຫ້ຍົກເວັ້ນໃນການຮັກສາຂໍ້ມູນລັບໃຫ້ພາຄີຝ່າຍຮັບຊາບ.

4. ບັນດາຄຳເຫັນທີ່ບໍ່ເຫັນພ້ອມກົງກັນ ທີ່ພົວພັນເຖິງການອະທິບາຍຫຼືການນຳໃຊ້ສິນທິສັນຍາສະບັບນີ້ຈະໄດ້ຮັບການແກ້ໄຂດ້ວຍວິທີການເຫັນດີເຫັນພ້ອມ ໂດຍຜ່ານການປຶກສາຫາລືລະຫວ່າງຄູ່ພາຄີ, ໂດຍບໍ່ອີງໃສ່ການພິຈາລະນາຕັດສິນຈາກຝ່າຍທີສາມ.

ສິນທິສັນຍາສະບັບນີ້ ລົງນາມທີ່ນະຄອນຫຼວງວຽງຈັນ, ສປປ ລາວ, ວັນທີ 29 ກັນຍາ 2023, ເປັນ 02 ສະບັບຕົ້ນ, ພາສາລາວ, ພາສາຫວຽດ ແລະ ພາສາອັງກິດ, ເອກະສານທຸກສະບັບລ້ວນແຕ່ມີຄຸນຄ່າເທົ່າທຽມກັນ. ໃນກໍລະນີທີ່ມີການຕີຄວາມໝາຍແຕກຕ່າງກັນ ໃຫ້ໃຊ້ສະບັບພາສາອັງກິດເປັນບ່ອນອີງ.

ຕາງໜ້າລັດຖະບານ

ແຫ່ງ

ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ



ຟິນເອກ ໂຕເລີມ

ລັດຖະມົນຕີກະຊວງປ້ອງກັນຄວາມສະຫງົບ

ຕາງໜ້າລັດຖະບານ

ແຫ່ງ

ສາທາລະນະລັດ ສັງຄົມນິຍົມຫວຽດນາມ



ຟິນເອກ ວິໄລ ຫຼ້າຄຳຟອງ

ຮອງ ນາຍົກລັດຖະມົນຕີ

ລັດຖະມົນຕີກະຊວງປ້ອງກັນຄວາມສະຫງົບ