# ແບບຟອມ 2

## ແບບຟອມນິຕິກຳເພື່ອສະເໜີລົງໃນຈົດໝາຍເຫດທາງລັດຖະການ
## ເພື່ອທາບທາມຄຳເຫັນທົ່ວໄປ

| **ອົງການສະເໜີ** | **ເລື່ອງ:** ຂໍລົງໃນຈົດໝາຍເຫດທາງລັດຖະການ |
|---|---|
| ຊື່ ກະຊວງ/ອົງການ: ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ<br>ຊື່ ພະນັກງານຮັບຜິດຊອບ: ທ່ານ ວັນຊະນະ ລັດມະນີ, ໂທ: 020 99894070<br>ທ່ານ ໄຊຊະນະ ຊາທິລາດ, ໂທ: 020 52790788<br>ອີ-ເມວ: vansana@mtc.gov.la<br>ວັນ, ເດືອນ, ປີ: 27 ເມສາ 2026 | |
| **ເນື້ອໃນ**<br><br>ວັນທີອະນຸມັດຮ່າງນິຕິກຳໂດຍຫົວໜ້າອົງການຈັດຕັ້ງທີ່ຮັບຜິດຊອບ (ມາດຕາ 36 ຂອງກົດໝາຍວ່າດ້ວຍການສ້າງນິຕິກຳ): 18 ເມສາ 2025<br><br>ຫົວຂໍ້ທີ່ສະເໜີມາຂອງຮ່າງນິຕິກຳ: ຮ່າງປັບປຸງກົດໝາຍວ່າດ້ວຍ ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ, ມີ 22 ໜ້າ<br>Law on Cyber crime (Admend)<br>( ຫົວຂໍ້ຂອງຮ່າງນິຕິກຳຕ້ອງກຳນົດຊື່ ເປັນພາສາລາວ ແລະ ພາສາອັງ ກິດ, ຈຳນວນໜ້າ) | **ເອກະສານທີ່ຮັບ**<br>**[ເປັນຮູບແບບອີເລັກໂຕຼນິກເທົ່ານັ້ນ]**<br><br>ຮ່າງນິຕິກຳ: ແມ່ນ / ບໍ່ແມ່ນ<br><br>ຄຳອະທິບາຍ: ມີ/ບໍ່ມີ<br><br>ຄຳເຫັນປະເມີນຜົນກະທົບ: ມີ/ບໍ່ມີ |
| **ທີ່ຢູ່ຊຶ່ງຈະໄດ້ສົ່ງຄຳເຫັນເຖິງ**<br>ທີ່ຢູ່ອີ-ເມວທີ່ນຳໃຊ້ປະຈຳຂອງຄະນະກຳມະການຮ່າງ:<br>Pisa@mtc.gov.la | **ຫົວໜ້າໜ່ວຍງານຈົດໝາຍເຫດທາງລັດຖະການ**<br>**ມີຄຳເຫັນສຸດທ້າຍ** |
| **ວັນທີທີ່ສະເໜີມາສຳລັບການພິມເຜີຍແຜ່**<br>ໂດຍທົ່ວໄປແລ້ວ,ຈົດໝາຍເຫດທາງລັດຖະການຈະພິມເຜີຍແຜ່ຮ່າງນິຕິກຳພາຍໃນກຳນົດເວລາ 10 ວັນລັດຖະການ. ຖ້າຫາກມີຄວາມຈຳເປັນ ເພື່ອພິມເຜີຍແຜ່ຮ່າງນິຕິກຳດັ່ງກ່າວຢ່າງຮີບດ່ວນ,ຈຶ່ງອະທິບາຍເຫດຜົນ ໂດຍສັງເຂບ ແລະ ວັນທີສະເໜີໃຫ້ມີການພິມເຜີຍແຜ່ສະເພາະ. | |
| **ລາຍເຊັນຫົວໜ້າຫ້ອງການຂອງອົງການທີ່ສະເໜີ ທາບທາມຮ່າງນິຕິກຳ**<br><br>ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຫ້ອງການ<br>ສົມອິບ ສີທາລາດ | |

# ຄຳຖາມເຈາະຈີ້ມ

1. ທາງດ້ານໂຄ່ງຮ່າງ ແລະ ເນື້ອໃນຂອງກົດໝາຍ ທ່ານເຫັນວ່າ ຄົບຖ້ວນ ເໝາະສົມ ສອດຄ່ອງ ແລ້ວບໍ່ ?
2. ມາດຕາ 8 ພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳທາງໄຊເບີ ທ່ານເຫັນວ່າ ຄົບຖ້ວນແລ້ວບໍ່ ? ທ່ານເຫັນວ່າ ຍັງມີອາຊະຍາກຳທາງໄຊເບີ ອື່ນອີກບໍ່ ທີ່ຕ້ອງໄດ້ຄຸ້ມຄອງ ?
3. ມາດຕາ 13 ການສ້າງຄວາມເສຍຫາຍໃນສື່ສັງຄົມອອນລາຍ ທ່ານເຫັນວ່າມີເນື້ອໃນ ຄົບຖ້ວນ ເໝາະສົມ ສອດຄ່ອງແລ້ວບໍ່ ?
4. ມາດຕາ 19 ການຫຼອກລວງທາງໄຊເບີ ທີ່ເປັນມາດຕາເພີ່ມໃໝ່ ທ່ານເຫັນວ່າມີເນື້ອໃນ ຄົບຖ້ວນເໝາະສົມ ແລ້ວບໍ່ ?
5. ມາດຕາ 21 ການກະທຳຜິດຕໍ່ແມ່ຍິງ ແລະ ເດັກຜ່ານໄຊເບີ ທີ່ເປັນມາດຕາເພີ່ມໃໝ່ ທ່ານເຫັນວ່າມີເນື້ອໃນ ຄົບຖ້ວນເໝາະສົມແລ້ວບໍ່ ?
6. ມາດຕາ 70 ມາດຕະການທາງອາຍາ ການກຳນົດໂທດດັ່ງກ່າວ ທ່ານເຫັນວ່າເໝາະສົມແລ້ວບໍ່ ?

# ສາລະບານ

**ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ**
**ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ**

ສະພາແຫ່ງຊາດ ເລກທີ /ສພຊ
ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ

# ກົດໝາຍ
# ວ່າດ້ວຍການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ

## ພາກທີ I
## ບົດບັນຍັດທົ່ວໄປ

**ມາດຕາ 1 (ປັບປຸງ) ຈຸດປະສົງ**

ກົດໝາຍສະບັບນີ້ ກຳນົດ ຫຼັກການ, ລະບຽບການ ແລະ ມາດຕະການ ກ່ຽວກັບການຄຸ້ມຄອງ, ຕິດຕາມ ກວດກາວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ເພື່ອເຮັດໃຫ້ວຽກງານດັ່ງກ່າວມີປະສິດທິຜົນ ແນໃສ່ຕ້ານ, ສະກັດກັ້ນ, ຈຳກັດ ແລະ ກຳຈັດ ອາຊະຍາກຳ, ປົກປ້ອງລະບົບ ຖານຂໍ້ມູນ, ລະບົບເຊີເວີ, ຂໍ້ມູນທາງ ລະບົບຄອມພິວເຕີ ຮັບປະກັນຄວາມໝັ້ນຄົງຂອງຊາດ, ຄວາມສະຫງົບ ແລະ ຄວາມເປັນລະບຽບຮຽບຮ້ອຍ ຂອງສັງຄົມ, ສາມາດເຊື່ອມໂຍງກັບພາກພື້ນ ແລະ ສາກົນປະກອບສ່ວນເຂົ້າໃນການປົກປັກຮັກສາ ແລະ ພັດທະນາເສດຖະກິດ-ສັງຄົມຂອງຊາດ ໃຫ້ຈະເລີນກ້າວໜ້າ ແລະ ຍືນຍົງ.

**ມາດຕາ 2 (ປັບປຸງ) ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ**

ອາຊະຍາກຳ ໄຊເບີ ແມ່ນ ການ ສ້າງຄວາມ ເສຍຫາຍໃຫ້ແກ່ ບຸກຄົນ, ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ ແລະ ສັງຄົມ ຕາມພຶດຕິກຳທີ່ໄດ້ກຳນົດໄວ້ໃນ ມາດຕາ 8 ຂອງກົດໝາຍສະບັບນີ້.

ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ແມ່ນ ການເຄື່ອນໄຫວຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທີ່ມີສິດ ແລະ ໜ້າທີ່ໂດຍກົງໃນການຊອກຮູ້ ແລະ ປະຕິບັດວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳ ໄຊເບີ ຕາມທີ່ໄດ້ກຳນົດ ໄວ້ໃນມາດຕາ 23 ແລະ 28 ຂອງກົດໝາຍສະບັບນີ້ ເພື່ອຈຳກັດ, ກຳຈັດ ແລະ ປາບປາມ ອາຊະຍາກຳທາງໄຊເບີ.

**ມາດຕາ 3 (ປັບປຸງ) ການອະທິບາຍຄຳສັບ**

ຄຳສັບທີ່ນຳໃຊ້ໃນກົດໝາຍສະບັບນີ້ ມີ ຄວາມໝາຍ ດັ່ງນີ້:

1. **ອາຊະຍາກຳ** ໝາຍເຖິງ ການກະທຳຜິດທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍອາຍາ ແລະ ກົດໝາຍອື່ນ ທີ່ກຳນົດໂທດທາງອາຍາ;

2. **ໄຊເບີ (Cyber)** ໝາຍເຖິງ ລະບົບເຕັກໂນໂລຊີການສື່ສານ ຂໍ້ມູນ ຂ່າວສານ ຊຶ່ງປະກອບດ້ວຍ ລະບົບຄອມພິວເຕີ, ເຄືອຂ່າຍຄອມພິວເຕີ, ໂຄງລ່າງພື້ນຖານດ້ານເຕັກໂນໂລຊີ ຂໍ້ມູນ ຂ່າວສານ, ລະບົບຄວບຄຸມ, ອຸປະກອນເຊື່ອມຕໍ່ ແລະ ກິດຈະກຳທາງອອນລາຍທັງໝົດ; (ເອົາມາຈາກົດໝາຍວ່າດ້ວຍ ຄວາມປອດໄພ

ໄຊເບີ)

3. **ລະບົບເຊີເວີ (Server System)** ໝາຍເຖິງ ລະບົບໃຫ້ບໍລິການຜ່ານລະບົບຄອມພິວເຕີ, ປະກອບ ດ້ວຍ ຖານຂໍ້ມູນເຊີເວີ (Database Server), ເວັບເຊີເວີ (Web Server), ເມວເຊີເວີ (Mail Server), ຟາຍ ເຊີເວີ (File Server) ແລະ ອື່ນໆ;

4. **ຂໍ້ມູນຄອມພິວເຕີ** ໝາຍເຖິງ ຂໍ້ມູນ, ຂໍ້ຄວາມ, ໂປຣແກຣມ ຫຼື ລະບົບຖານຂໍ້ມູນ, ຂໍ້ມູນສ່ວນບຸກຄົນ , ຂໍ້ມູນຈະລາຈອນທາງລະບົບຄອມພິວເຕີ ໃນຮູບແບບທີ່ສາມາດປະມວນຜົນ ແລະ ເຮັດໃຫ້ ລະບົບຄອມພິວ ເຕີເຮັດວຽກໄດ້;

5. **ລະບົບຖານຂໍ້ມູນ (Database System)** ໝາຍເຖິງ ລະບົບຂໍ້ມູນທີ່ເກັບຮັກສາໃນຮູບ ແບບເອເລັກ ໂຕຣນິກທີ່ສາມາດຄຸ້ມຄອງ, ປັບປຸງ ແລະ ນຳໃຊ້ໄດ້;

6. **ຂໍ້ມູນສ່ວນບຸກຄົນ** ໝາຍເຖິງ ຂໍ້ມູນທີ່ກ່ຽວຂ້ອງ ຫຼື ບົ່ງບອກເຖິງລັກສະນະ ຫຼື ຕົວຕົນ, ການເຄື່ອນ ໄຫວຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ໂດຍທາງກົງ ຫຼື ທາງອ້ອມ;

7. **ຂໍ້ມູນຈະລາຈອນທາງລະບົບຄອມພິວເຕີ** ໝາຍເຖິງ ຂໍ້ມູນຄອມພິວເຕີທີ່ກ່ຽວຂ້ອງກັບ ການສື່ສານ ຜ່ານລະບົບຄອມພິວເຕີ ຊຶ່ງຖືກສ້າງຂຶ້ນໂດຍລະບົບຄອມພິວເຕີທີ່ເປັນສ່ວນໜຶ່ງ ໃນຕ່ອງໂສ້ ຂອງການສື່ສານທີ່ ບົ່ງບອກເຖິງ ຜູ້ສົ່ງ, ຕົ້ນທາງ, ສົ່ງທາງ, ເສັ້ນທາງ, ປາຍທາງ, ວັນ, ເວລາ, ຂະໜາດ, ກຳນົດເວລາຂອງການສື່ສານ, ຊະນິດການບໍລິການ ແລະ ອື່ນໆ ທີ່ກ່ຽວຂ້ອງກັບການຕິດຕໍ່ສື່ສານຂອງລະ ບົບຄອມພິວເຕີນັ້ນ;

8. **ຜູ້ໃຫ້ບໍລິການ** ໝາຍເຖິງ ຜູ້ໃຫ້ບໍລິການດ້ານການສື່ສານຂໍ້ມູນຂ່າວສານ, ຜູ້ໃຫ້ບໍລິການທາງການເງິນ, ຜ່ານລະບົບຄອມ ພິວເຕີ ແລະ/ຫຼື ຜູ້ໃຫ້ບໍລິການເກັບຮັກສາຂໍ້ມູນຄອມພິວເຕີ; (ກວດຄືນ)

9. **ການປະມວນຂໍ້ມູນແບບອັດຕະໂນມັດ** ໝາຍເຖິງ ຂະບວນການ ຄຳນວນ, ວິເຄາະ, ສະຫຼຸບ, ແນະນຳ ວິທີການ ແລະ ປັບປຸງ ຂໍ້ມູນໃນລະບົບຄອມພິວເຕີ ໂດຍໂປຣແກຣມຄອມພິວເຕີໃດໜຶ່ງ ເພື່ອໃຫ້ໄດ້ຮັບຜົນ ຕາມຈຸດປະສົງຂອງຜູ້ນຳໃຊ້;

10. **ໂປຣແກຣມ** ໝາຍເຖິງ ລະບົບຄຳສັ່ງ ຫຼື ຊຸດຄຳສັ່ງ ທີ່ລະບົບຄອມພິວເຕີ ສາມາດປະຕິ ບັດໄດ້ ເພື່ອເຮັດໃຫ້ເກີດຜົນໄດ້ຮັບຕາມທີ່ໄດ້ກຳນົດໄວ້;

11. **ໄວຣັດ** ໝາຍເຖິງ ໂປຣແກຣມສະເພາະທີ່ສ້າງຂຶ້ນ ຊຶ່ງສາມາດແຜ່ກະຈາຍ, ສ້າງຄວາມເສຍຫາຍ ແລະ ທຳລາຍລະບົບຄອມພິວເຕີ, ເຄືອຂ່າຍຄອມພິວເຕີ ແລະ ຂໍ້ມູນຄອມພິວເຕີ;

12. **ໂປຣແກຣມປະສົງຮ້າຍ (Malicious Code)** ໝາຍເຖິງ ຊຸດຄຳສັ່ງຄອມພິວເຕີ ທີ່ສ້າງຂຶ້ນ ເພື່ອທຳ ລາຍລະບົບຄອມພິວເຕີ ຫຼື ລັກຂໍ້ມູນຄອມພິວເຕີ;

13. **ເວັບໄຊປອມ (Phishing)** ໝາຍເຖິງ ເວັບໄຊທີ່ສ້າງຂຶ້ນໃໝ່ ຊຶ່ງຄ້າຍຄືກັບເວັບໄຊເດີມ ເພື່ອຫຼອກ ລວງເອົາຂໍ້ມູນຜູ້ຊົມໃຊ້;

14. **ຊ່ອງໂຫວ່ຂອງລະບົບຄອມພິວເຕີ (Vulnerability)** ໝາຍເຖິງ ຂໍ້ບົກພ່ອງຂອງໂປຣ ແກຣມ ຫຼື ຊ່ອນແອ ທີ່ບໍ່ສົມບູນ ແລະ ບໍ່ໄດ້ຮັບການປັບປຸງ ເຮັດໃຫ້ຜູ້ປະສົງຮ້າຍສາມາດສວຍໃຊ້ ເພື່ອ ທຳລາຍລະບົບ, ລັກຂໍ້ມູນ, ປ່ຽນແປງຂໍ້ມູນ ແລະ ອື່ນໆ;

15. **ຂໍ້ມູນຜູ້ຊົມໃຊ້** ໝາຍເຖິງ ຂໍ້ມູນທີ່ນຳໄປສູ່ ຜູ້ຊົມໃຊ້ ເປັນຕົ້ນ ທີ່ຢູ່ໄປສະນີ, ທີ່ຢູ່ທາງເອເລັກ ໂຕຣນິກ, ທີ່ຢູ່ດ້ານພູມສັນຖານ, ເລກໝາຍອິນເຕີເນັດ, ເບີໂທລະສັບ ຫຼື ລະຫັດອື່ນ ທີ່ໃຊ້ເຂົ້າໃນລະ ບົບ ຄອມພິວເຕີ;

16. **ມາດຕະການປ້ອງກັນສະເພາະ** ໝາຍເຖິງ ການນຳໃຊ້ເຄື່ອງມື ແລະ/ຫຼື ໂປຣແກຣມຄອມ ພິວເຕີ ພິເສດ ເພື່ອຕ້ານ ແລະ ສະກັດກັ້ນການເຂົ້າເຖິງລະບົບຄອມພິວເຕີຂອງຜູ້ຊົມໃຊ້;

17. **ສື່ສັງຄົມອອນລາຍ** ໝາຍເຖິງ ການສື່ສານຜ່ານລະບົບເຄືອຂ່າຍອິນເຕີເນັດ ເພື່ອເຜີຍ ແຜ່ຂໍ້ມູນ ຂ່າວສານສູ່ສາທາລະນະ ດ້ວຍການນຳໃຊ້ວັດຖຸປະກອນຄອມພິວເຕີ ແລະ ອຸປະກອນສື່ສານ ອື່ນ;

18. **ພາບເຄື່ອນໄຫວ** ໝາຍເຖິງ ພາບທີ່ສ້າງຂຶ້ນ ຊຶ່ງມີການເໜັງຕີງຄ້າຍຄືກັບຕົວຈິງ ໂດຍຜ່ານອຸປະກອນເອເລັກໂຕຣນິກ ເຊັ່ນ ຮູບເງົາກະຕູນ.

19. **ບັນຊີຕົວແທນ (Proxy Account / Money Mule Account)** ໝາຍເຖິງ ບັນຊີເງິນຝາກທະນາຄານ, ບັນຊີກະເປົ໋າເງິນເອເລັກໂຕຣນິກ, ບັນຊີຊັບສິນດິຈິຕອນ ຫຼື ບັນຊີການເງິນອື່ນໆ ທີ່ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງໃດໜຶ່ງ ໄດ້ເປີດ ຫຼື ລົງທະບຽນນຳໃຊ້ ແລ້ວໄດ້ມອບສິດ, ສິ່ງມອບລະຫັດຜ່ານ, ຂໍ້ມູນການເຂົ້າເຖິງ ຫຼື ຍິນຍອມໃຫ້ບຸກຄົນອື່ນນຳໃຊ້, ຄຸ້ມຄອງ ຫຼື ຄວບຄຸມແທນຕົນເອງ ໂດຍມີຈຸດປະສົງເພື່ອປົກປິດຕົວຕົນ, ຮັບ, ໂອນ, ປ່ຽນແປງສະພາບ ຫຼື ຊຸກເຊື່ອງຊັບສິນ ແລະ ເງິນທຶນ ທີ່ໄດ້ມາຈາກການກະທຳຜິດ, ອາຊະຍາກຳທາງໄຊເບີ ຫຼື ເພື່ອອຳນວຍຄວາມສະດວກໃຫ້ແກ່ການຟອກເງິນ.

20. ສະກຸນເງິນດິຈິຕອນ **(Cryptocurrency)** ໝາຍເຖິງ ຂໍ້ມູນເອເລັກໂຕຣນິກ ຫຼື ຊັບສິນໃນຮູບແບບດິຈິຕອນ ທີ່ຖືກສ້າງຂຶ້ນເພື່ອໃຊ້ເປັນສື່ກາງໃນການແລກປ່ຽນ, ຕີມູນຄ່າ, ຊື້-ຂາຍ ຫຼື ຊຳລະສະສາງ ໂດຍນຳໃຊ້ເຕັກໂນໂລຊີການເຂົ້າລະຫັດ (Cryptography) ແລະ ລະບົບການບັນທຶກຂໍ້ມູນແບບກະຈາຍສູນ (ເຊັ່ນ: Blockchain) ເພື່ອຮັບປະກັນຄວາມປອດໄພຂອງການເຮັດທຸລະກຳ.

21. **ຂໍ້ມູນຊີວະມິຕິ (Biometric Data):** ຂໍ້ມູນລັກສະນະທາງກາຍະພາບ ຫຼື ພຶດຕິກຳສະເພາະຕົວຂອງບຸກຄົນ ທີ່ນຳໃຊ້ໃນລະບົບເຕັກໂນໂລຊີ ເພື່ອຢັ້ງຢືນ ຫຼື ລະບຸຕົວຕົນ ເຊັ່ນ: ລາຍນິ້ວມື, ໂຄງສ້າງໃບໜ້າ, ມ່ານຕາ ຫຼື ສຽງ.

22. **ກະແຈເຂົ້າລະຫັດ (Encryption Key):** ຊຸດຂໍ້ມູນ, ລະຫັດ ຫຼື ສູດຄຳນວນທາງຄະນິດສາດ ທີ່ໃຊ້ສຳລັບການເຂົ້າລະຫັດ (Encryption) ເພື່ອປົກປິດຂໍ້ມູນ ຫຼື ໃຊ້ສຳລັບຖອດລະຫັດ (Decryption) ເພື່ອອ່ານຂໍ້ມູນນັ້ນ.

23. **ລະບົບຄລາວ (Cloud System / Cloud Computing):** ການໃຫ້ບໍລິການຊັບພະຍາກອນດ້ານໄອທີ ເຊັ່ນ: ການຈັດເກັບຂໍ້ມູນ, ເຊີບເວີ, ຫຼື ຊອບແວ ຜ່ານລະບົບເຄືອຂ່າຍອິນເຕີເນັດ ເຊິ່ງຜູ້ໃຊ້ບໍ່ຈຳເປັນຕ້ອງມີເຄື່ອງເຊີບເວີຕັ້ງຢູ່ບ່ອນຂອງຕົນເອງ.

24. **ປັນຍາປະດິດ (AI - Artificial Intelligence):** ລະບົບຄອມພິວເຕີ ຫຼື ຊອບແວ ທີ່ຖືກພັດທະນາໃຫ້ມີຄວາມສາມາດໃນການປະມວນຜົນ, ການຮຽນຮູ້ ແລະ ການສ້າງຜົນຜະລິດຄ້າຍຄືກັບສະຕິປັນຍາຂອງມະນຸດ.

25. **ການສ້າງຂໍ້ມູນປອມທີ່ຄ້າຍຄືຄວາມຈິງ (Deepfake):** ການນຳໃຊ້ເຕັກໂນໂລຊີປັນຍາປະດິດ (AI) ໃນການຕັດຕໍ່, ດັດແປງ ຫຼື ສ້າງຮູບພາບ, ວິດີໂອ ຫຼື ສຽງຂອງບຸກຄົນໃດໜຶ່ງຂຶ້ນມາໃໝ່ ໃຫ້ມີຄວາມສົມຈິງຈົນຍາກທີ່ຈະແຍກແຍະ ເພື່ອຈຸດປະສົງສ້າງຄວາມເຂົ້າໃຈຜິດ ຫຼື ສ້າງຄວາມເສຍຫາຍ.

**ມາດຕາ 4 (ປັບປຸງ) ນະໂຍບາຍຂອງລັດ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ**

ລັດ ສົ່ງເສີມການນຳໃຊ້ໄຊເບີ ໃຫ້ມີຄວາມປອດໄພ, ສະດວກ, ວ່ອງໄວ ແລະ ຍຸຕິທຳ ພ້ອມທັງປົກປ້ອງສິດຜົນປະໂຫຍດອັນຊອບທຳ ຂອງຜູ້ໃຫ້ບໍລິການ, ຜູ້ໃຊ້ບໍລິການຜ່ານໄຊເບີ ຕາມກົດໝາຍ ແລະ ລະບຽບການ.

ລັດ ສ້າງເງື່ອນໄຂ ແລະ ອຳນວຍຄວາມສະດວກ ໃຫ້ແກ່ການຈັດຕັ້ງປະຕິບັດວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ດ້ວຍການ ສະໜອງງົບປະມານ, ສ້າງ, ປະກອບບຸກຄະລາກອນ, ພາຫະນະ, ອຸປະກອນ, ຄົ້ນຄວ້າ ນຳໃຊ້ເຕັກໂນໂລຊີທີ່ທັນສະໄໝ, ກໍ່ສ້າງພື້ນຖານໂຄງລ່າງ ເພື່ອເຮັດໃຫ້ວຽກງານດັ່ງກ່າວ ມີປະສິດທິພາບ ແລະ ປະສິດທິຜົນ.

ລັດ ຖືເອົາການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ເປັນວຽກຕົ້ນຕໍ ແລະ ເອົາການແກ້ໄຂບັນຫາເປັນວຽກສຳຄັນ.

ລັດ ຊຸກຍູ້ ແລະ ສົ່ງເສີມ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທັງພາຍໃນ ແລະ ຕ່າງປະເທດ ລົງທຶນ ເຂົ້າໃສ່ ການສ້າງ, ພັດທະນາເຕັກໂນໂລຊີ, ຜະລິດຕະພັນ ແລະ ການບໍລິການ ພ້ອມທັງເຂົ້າຮ່ວມໃນວຽກງານ ຕ້ານ ແລະ ສະກັດ ກັ້ນອາຊະຍາກຳໄຊເບີ.

**ມາດຕາ 5 (ປັບປຸງ) ຫຼັກການກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ**

ໃນວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ຕ້ອງຮັບປະກັນຫຼັກການ ດັ່ງນີ້:

1. ສອດຄ່ອງກັບ ແນວທາງນະໂຍບາຍ, ກົດໝາຍ, ແຜນຍຸດທະສາດ, ແຜນພັດທະນາ ເສດຖະ ກິດ-ສັງຄົມ ຂອງຊາດ;
2. ຮັບປະກັນຄວາມໝັ້ນຄົງ ຂອງຊາດ, ຄວາມສະຫງົບ, ຄວາມເປັນລະບຽບຮຽບຮ້ອຍຂອງສັງຄົມ, ວັດທະນະທຳ ແລະ ຮີດຄອງປະເພນີອັນດີງາມຂອງຊາດ;
3. ຮັກສາຄວາມລັບ ຂອງຊາດ, ຄວາມລັບທາງລັດຖະການ, ຂອງບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການ ຈັດ ຕັ້ງ;
4. ເປັນເອກະພາບ, ປອດໄພ, ສະດວກ, ວ່ອງໄວ, ທັນການ, ຍຸຕິທຳ, ເຂັ້ມງວດ, ໂປ່ງໃສ ແລະ ສາມາດ ກວດສອບໄດ້;
5. ປົກປ້ອງສິດ ແລະ ຜົນປະໂຫຍດອັນຊອບທຳຂອງຜູ້ໃຫ້ບໍລິການ, ຜູ້ໃຊ້ບໍລິການໄຊເບີ, ຂໍ້ມູນ ຄອມພິວເຕີ ຕາມກົດໝາຍ ແລະ ລະບຽບການ;
6. ຮັບປະກັນການມີສ່ວນຮ່ວມ ຂອງສັງຄົມ;
7. ສອດຄ່ອງກັບ ສົນທິສັນຍາ ທີ່ ສປປ ລາວ ເປັນພາຄີ ແລະ ສັນຍາສາກົນ ທີ່ກ່ຽວຂ້ອງ.

**ມາດຕາ 6 (ປັບປຸງ) ຂອບເຂດການນຳໃຊ້ກົດໝາຍ**

ກົດໝາຍສະບັບນີ້ ນຳໃຊ້ສຳລັບ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທັງພາຍໃນ ແລະ ຕ່າງປະເທດ ທີ່ເຄື່ອນໄຫວ ແລະ ພົວພັນກັບວຽກງານ ຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ຢູ່ ສປປ ລາວ.

**ມາດຕາ 7 (ປັບປຸງ) ການຮ່ວມມືສາກົນ**

ລັດ ພົວພັນ ຮ່ວມມື ກັບຕ່າງປະເທດ, ພາກພື້ນ ແລະ ສາກົນ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນ ອາຊະຍາກຳ ໄຊເບີ ດ້ວຍການແລກປ່ຽນບົດຮຽນ, ປະສົບ ການ, ຂໍ້ມູນຂ່າວສານ, ເຕັກນິກ, ເຕັກໂນໂລຊີ, ນະ ວັດຕະກຳ, ການຍົກລະດັບວິຊາສະເພາະ, ຄວາມຮູ້ ແລະ ຄວາມສາມາດຂອງບຸກຄະລາກອນ, ປະຕິບັດ ສົນທິສັນຍາ ທີ່ ສປປ ລາວ ເປັນພາຄີ ແລະ ສັນຍາສາກົນ ທີ່ກ່ຽວຂ້ອງ.

## ພາກທີ II
## ພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳໄຊເບີ

**ມາດຕາ 8 ພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳ ໄຊເບີ**

ພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳໄຊເບີ ມີ ດັ່ງນີ້:

1. ການເປີດເຜີຍມາດຕະການປ້ອງກັນການເຂົ້າເຖິງລະບົບຄອມພິວເຕີ
2. ການເຂົ້າເຖິງລະບົບຄອມພິວເຕີໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
3. ການຕັດຕໍ່ເນື້ອໃນ, ຮູບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
4. ການລັດເອົາຂໍ້ມູນໃນລະບົບຄອມພິວເຕີໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;

5. ການສ້າງຄວາມເສຍຫາຍຜ່ານສື່ສັງຄົມອອນລາຍ;
6. ການເຜີຍແຜ່ສິ່ງລາມົກຜ່ານໄຊເບີ;
7. ການລັບກອນລະບົບຄອມພິວເຕີ;
8. ການປອມແປງຂໍ້ມູນຄອມພິວເຕີ
9. ການທຳລາຍຂໍ້ມູນຄອມພິວເຕີ;
10. ການດຳເນີນກິດຈະການ ກ່ຽວກັບເຄື່ອງມືອາຊະຍາກຳໄຊເບີ;
11. ການຫຼອກລວງຜ່ານໄຊເບີ;
12. ການນຳໃຊ້ປັນຍາປະດິດ (AI) ໃນທາງທີ່ຜິດ;
13. ການສ້າງຄວາມເສຍຫາຍ ຕໍ່ແມ່ຍິງ ແລະ ເດັກ ຜ່ານໄຊເບີ;
14. ການຟອກເງິນທີ່ໄດ້ຈາກອາຊະຍາກຳໄຊເບີ;

**ມາດຕາ 9 (ປັບປຸງ) ການເປີດເຜີຍມາດຕະການປ້ອງກັນການເຂົ້າເຖິງລະບົບຄອມພິວເຕີ**

ການເປີດເຜີຍມາດຕະການປ້ອງກັນການເຂົ້າເຖິງລະບົບຄອມພິວເຕີແມ່ນ ການນຳເອົາຂໍ້ມູນທີ່ໃຊ້ສຳລັບການຢັ້ງຢືນຕົວຕົນ ເປັນຕົ້ນ ລະຫັດຜ່ານ (Password), ກະແຈເຂົ້າລະຫັດ (Encryption Key), ຂໍ້ມູນຊີວະມິຕິ (Biometric Data) ຫຼື ຂໍ້ມູນຊ່ອງໂຫວ່ຂອງລະບົບ (Vulnerabilities) ຫຼື ມາດຕະການປ້ອງກັນຄວາມປອດໄພສະເພາະອື່ນ ເພື່ອນຳໄປເປີດເຜີຍ, ສົ່ງຕໍ່, ແບ່ງປັນ, ຫຼື ຈຳໜ່າຍ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ຊຶ່ງສ້າງຄວາມສ່ຽງທີ່ກໍ່ໃຫ້ເກີດໄພຄຸກຄາມ ຫຼື ໄດ້ສ້າງຄວາມເສຍຫາຍຕົວຈິງ ໃຫ້ແກ່ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ.

**ມາດຕາ 10 (ປັບປຸງ) ການເຂົ້າເຖິງລະບົບຄອມພິວເຕີໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ**

ການເຂົ້າເຖິງລະບົບຄອມພິວເຕີ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ແມ່ນ ການກະທຳຂອງບຸກຄົນທີ່ໃຊ້ວິທີການ ຫຼື ອຸປະກອນໃດໜຶ່ງ ເພື່ອເຂົ້າເຖິງລະບົບຄອມພິວເຕີ, ລະບົບເຄືອຂ່າຍ, ຖານຂໍ້ມູນ ຂອງບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ໂດຍບໍ່ມີສິດ ຫຼື ເກີນຂອບເຂດສິດທີ່ໄດ້ຮັບອະນຸຍາດ.

**ມາດຕາ 11 (ປັບປຸງ) ການຕັດຕໍ່ເນື້ອໃນ, ຮູບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ**

ການຕັດຕໍ່ເນື້ອໃນ, ຮູບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ແມ່ນການນຳໃຊ້ເຕັກໂນໂລຊີ, ການນຳໃຊ້ເຄື່ອງມືທາງເອເລັກໂຕຣນິກ, ຊອບແວ ຫຼື ປັນຍາປະດິດ(AI) ເພື່ອສ້າງຂໍ້ມູນປອມທີ່ຄ້າຍຄວາມຈິງ ໂດຍເປັນການສ້າງຂຶ້ນໃໝ່, ເພີ່ມເຕີມ, ຕັດອອກ ຫຼື ດັດແປງຈາກຂໍ້ມູນຕົ້ນສະບັບ ເພື່ອເຜີຍແຜ່ຜ່ານໄຊເບີ ຊຶ່ງສ້າງຄວາມເສຍຫາຍໃຫ້ແກ່ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທີ່ກ່ຽວຂ້ອງ.

**ມາດຕາ 12 (ປັບປຸງ) ການລັດເອົາຂໍ້ມູນໃນລະບົບຄອມພິວເຕີໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ**

ການລັດເອົາຂໍ້ມູນໃນລະບົບຄອມພິວເຕີໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ແມ່ນການນຳໃຊ້ເຄື່ອງມືທາງດ້ານເອເລັກໂຕຣນິກ ຫຼື ຊອບແວ ເພື່ອລັກລອບເຂົ້າເຖິງ, ສຳເນົາ, ຖ່າຍໂອນ ຫຼື ດັກເອົາຂໍ້ມູນທີ່ກຳລັງ ຮັບ-ສົ່ງ ຫຼື ຂໍ້ມູນທີ່ຈັດເກັບໄວ້ໃນລະບົບຄອມພິວເຕີ, ເຄືອຂ່າຍ ແລະ ລະບົບຄລາວ (Cloud) ຂອງບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.

**ມາດຕາ 13 (ປັບປຸງ) ການສ້າງຄວາມເສຍຫາຍຜ່ານສື່ສັງຄົມອອນລາຍ**

ການສ້າງຄວາມເສຍຫາຍຜ່ານສື່ສັງຄົມອອນລາຍ ແມ່ນການນຳສະເໜີ, ເຜີຍແຜ່, ສົ່ງຕໍ່ ຂໍ້ມູນຂ່າວສານ ຫຼື ສະແດງຄວາມຄິດເຫັນສະໜັບສະໜຸນ ຜ່ານສື່ສັງຄົມອອນລາຍ ຊຶ່ງໄດ້ສ້າງຄວາມເສຍຫາຍຕໍ່ ບຸກຄົນ,

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຫຼື ມີຜົນກະທົບຕໍ່ຄວາມໝັ້ນຄົງຂອງຊາດ ແລະ ຄວາມເປັນລະບຽບ ຮຽບຮ້ອຍ ຂອງສັງຄົມ.

(ຂໍຄຳເຫັນຄືນ)

**ມາດຕາ 14 (ປັບປຸງ) ການເຜີຍແຜ່ສິ່ງລາມົກຜ່ານໄຊເບີ**

ການເຜີຍແຜ່ສິ່ງລາມົກຜ່ານໄຊເບີ ແມ່ນ ການ ຊື້-ຂາຍ, ການແຈກຢາຍ, ການສົ່ງຕໍ່, ການແນະນຳ ແລະ ການເຜີຍແຜ່ຂໍ້ມູນ ຮູບພາບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອ ກ່ຽວກັບອະໄວຍະວະເພດ, ການຮ່ວມເພດ ຫຼື ພຶດຕິກຳທາງເພດຂອງຄົນ ທີ່ຂັດກັບສິລະທຳ ແລະ ວັດທະນະທຳອັນດີງາມ ຜ່ານໄຊເບີ.

**ມາດຕາ 15 (ປັບປຸງ) ການລົບກວນລະບົບຄອມພິວເຕີ**

ການລົບກວນລະບົບຄອມພິວເຕີ ແມ່ນ ການກະທຳ ດັ່ງນີ້:

1. ການນຳໃຊ້ໂປຣແກຣມຄອມພິວເຕີ, ໄວຣັດ ມັລແວ (Malware), ໄວຣັດແລນຊຳແວ (Ransomware) ຫຼື ເຄື່ອງມືອື່ນ ເພື່ອຂັດຂວາງ, ທຳລາຍ ການປະຕິບັດງານຂອງລະບົບຄອມພິວເຕີ ຫຼື ເຂົ້າລະຫັດຂໍ້ມູນເພື່ອ ຮຽກຄ່າໄຖ່;
2. ສົ່ງຂໍ້ມູນເຂົ້າສູ່ລະບົບເຄືອຂ່າຍຄອມພິວເຕີ ໃນປະລິມານມະຫາສານໂດຍເຈດຕະນາ ເພື່ອໃຫ້ລະບົບນັ້ນບໍ່ ສາມາດໃຫ້ບໍລິການໄດ້;
3. ການສົ່ງຂໍ້ມູນລະບົບຄອມພິວເຕີ ຫຼື ຈົດໝາຍທາງເອເລັກໂຕຣນິກ ໂດຍມີການປົກປິດ ທີ່ຢູ່ ຫຼື ແຫຼ່ງທີ່ມາ ຂອງຜູ້ສົ່ງ ເພື່ອລົບກວນ, ສ້າງຄວາມເສຍຫາຍ.
4. ແຊກແຊງການເຮັດວຽກ, ປ່ຽນແປງຄຳສັ່ງ, ຊຸດຄຳສັ່ງ ຫຼື ການເຮັດວຽກຂອງອຸປະກອນເຄືອຂ່າຍຄອມພິວ ເຕີ ເພື່ອລົບກວນ ຫຼື ທຳລາຍການປະຕິບັດງານຂອງລະບົບຄອມພິວເຕີ.

**ມາດຕາ 16 (ປັບປຸງ) ການປອມແປງຂໍ້ມູນຄອມພິວເຕີ**

ການປອມແປງຂໍ້ມູນຄອມພິວເຕີ ແມ່ນ ການໃຊ້ຄອມພິວເຕີ ຫຼື ລະບົບຄອມພິວເຕີ ແລະ ອຸປະກອນເອ ເລັກໂຕຣນິກ ເພື່ອເຮັດໃຫ້ຂໍ້ມູນຄອມພິວເຕີ ຜິດຈາກຄວາມເປັນຈິງ ໂດຍມີຈຸດປະສົງນຳໄປອ້າງອີງ, ນຳໃຊ້ ຫຼື ເຮັດໃຫ້ ຫຼົງເຊື່ອວ່າຂໍ້ມູນນັ້ນເປັນຂໍ້ມູນທີ່ຖືກຕ້ອງ ແລະ ແທ້ຈິງ ດ້ວຍການກະທຳ ດັ່ງນີ້:

1. ການປ້ອນຂໍ້ມູນ, ການປ່ຽນແປງຂໍ້ມູນ, ການປອມທີ່ຢູ່ທາງເອເລັກໂຕຣນິກ ຫຼື ການລຶບຂໍ້ມູນໃນ ລະບົບຄອມພິວເຕີ ທີ່ສົ່ງຜົນໃຫ້ຂໍ້ມູນທາງລະບົບຄອມພິວເຕີໃດໜຶ່ງ ປ່ຽນແປງຈາກຂໍ້ມູນເດີມ ໂດຍເຈດຕະ ນາ;

2. ການປ້ອນ ແລະ ການປ່ຽນແປງ ຂໍ້ມູນທຸລະກຳທາງການເງິນ, ທາງການຄ້າ, ຄວາມລັບ ແລະ ຂໍ້ມູນ ອື່ນຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;

3. ການສ້າງ ເວັບໄຊປອມ, ສື່ສັງຄົມອອນລາຍ, ແອັບພລິເຄຊັນ ຫຼື ຂໍ້ຄວາມສັ້ນ (SMS) ເພື່ອຫຼອກ ລວງ, ການຫຼອກລວງໃຫ້ຜູ້ນຳໃຊ້ລະບົບຄອມພິວເຕີ ຫຼື ອິນເຕີເນັດ ປ້ອນຂໍ້ມູນບັນຊີເງິນຝາກ, ລະຫັດ ບັດເຄຣດິດ, ລະຫັດນຳໃຊ້ອິນເຕີເນັດ, ລະຫັດຜ່ານ ຫຼື ຂໍ້ມູນສ່ວນຕົວ;

**ມາດຕາ 17 (ປັບປຸງ) ການທຳລາຍຂໍ້ມູນຄອມພິວເຕີ**

ການທຳລາຍຂໍ້ມູນຄອມພິວເຕີ ແມ່ນ ການລຶບ, ການດັດແກ້, ການປ່ຽນແປງ ແລະ/ຫຼື ການເຮັດໃຫ້ຂໍ້ ມູນຄອມພິວເຕີ ຫຼື ຂໍ້ມູນໃນລະບົບຄອມພິວເຕີ ເສຍຫາຍ ແລະ ຜິດແປກ ຈາກຂໍ້ມູນເດີມ.

**ມາດຕາ 18 (ປັບປຸງ) ການດຳເນີນກິດຈະການ ກ່ຽວກັບເຄື່ອງມືອາຊະຍາກຳໄຊເບີ**

ການດຳເນີນກິດຈະການ ກ່ຽວກັບເຄື່ອງມືອາຊະຍາກຳໄຊເບີ ແມ່ນ ການກະທຳທີ່ມີເຈດຕະນາ ເພື່ອນຳໃຊ້ເຂົ້າໃນການກໍ່ອາຊະຍາກຳໄຊເບີ ດັ່ງນີ້:

1. ການສ້າງຊຸດຄຳສັ່ງ, ໂປຣແກຣມຄອມພິວເຕີໃໝ່ສະເພາະ, ການອອກແບບລະບົບ, ການປະກອບອຸປະກອນເອເລັກໂຕຣນິກ ເພື່ອໃຊ້ໃນການເຈາະລະບົບ, ລັກຂໍ້ມູນ, ທຳລາຍລະບົບຄອມພິວເຕີ ຫຼື ແຊກແຊງລະບົບການສື່ສານໂທລະຄົມມະນາຄົມ.

2. ການຜະລິດ, ການນຳເຂົ້າ, ການສົ່ງອອກ, ການຊື້-ຂາຍ, ການຈຳໜ່າຍ, ການແລກປ່ຽນເຄື່ອງມື, ໂປຣແກຣມປະສົງຮ້າຍ.

3. ການຜະລິດ, ການນຳເຂົ້າ, ການສົ່ງອອກ, ການຊື້-ຂາຍ, ການຈຳໜ່າຍ ອຸປະກອນຮັບ-ສົ່ງສັນຍານໂທລະຄົມມະນາຄົມ ແລະ ອິນເຕີເນັດ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.

4. ການມີໄວ້ໃນຄອບຄອງ, ການໂຄສະນາເຜີຍແຜ່, ການແນະນຳວິທີການນຳໃຊ້ເຄື່ອງມືໃນການກໍ່ອາຊະຍາກຳໄຊເບີ ໂດຍມີເຈດຕະນາເພື່ອໃຫ້ຕົນເອງ ຫຼື ຜູ້ອື່ນນຳໄປໃຊ້ໃນການກະທຳຜິດ ລວມທັງການປອມແປງສັນຍານເພື່ອສົ່ງຂໍ້ຄວາມຫຼອກລວງ.

5. ການໃຫ້ເຊົ່າລະບົບທີ່ນຳໃຊ້ເຂົ້າໃນການກໍ່ອາຊະຍາກຳໄຊເບີ.

6. ການເປີດສອນວິທີການນຳໃຊ້ເຄື່ອງມືເພື່ອໂຈມຕີລະບົບຄອມພິວເຕີ ແລະ ເຄືອຂ່າຍການສື່ສານ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.

7. ເປີດບັນຊີ, ຊື້-ຂາຍ ຫຼື ຍິນຍອມໃຫ້ບຸກຄົນອື່ນນຳໃຊ້ບັນຊີເງິນຝາກທະນາຄານຂອງຕົນ ເພື່ອນຳໃຊ້ເຂົ້າໃນການກະທຳຜິດອາຊະຍາກຳໄຊເບີ

8. ຂຶ້ນທະບຽນ, ຊື້-ຂາຍ ຫຼື ຍິນຍອມໃຫ້ບຸກຄົນອື່ນນຳໃຊ້ເລກໝາຍໂລກໝາຍລະສັບ ຂອງຕົນ ເພື່ອນຳໃຊ້ເຂົ້າໃນການກະທຳຜິດອາຊະຍາກຳໄຊເບີ

**ມາດຕາ 19 (ໃໝ່) ການຫຼອກລວງຜ່ານໄຊເບີ**

ການຫຼອກລວງຜ່ານໄຊເບີ ແມ່ນ ການກະທຳທີ່ເປັນການໃຊ້ເລ່ລ່ຽມ, ຕົວະຍົວະຫຼອກລວງ ຫຼື ຊັກຈູງໃຫ້ບຸກຄົນໃດໜຶ່ງປະຕິບັດຕາມ ຜ່ານໄຊເບີ ເພື່ອຈຸດປະສົງ ໃນການສໍ້ໂກງຊັບ ຂອງບຸກຄົນອື່ນ ຊຶ່ງມີການກະທຳ ດັ່ງນີ້:

1. ການຫຼອກລວງຜ່ານການຕິດຕໍ່ສື່ສານ ແມ່ນການຫຼອກລວງຜ່ານການໂທທາງສຽງ, ໂທທາງວີດີໂອ, ສົ່ງຂໍ້ຄວາມ, ສົ່ງລິ້ງປອມ, ແອບອ້າງຕົວຕົນ ຫຼື ຮູບແບບອື່ນ ໂດຍນຳໃຊ້ກົນອຸບາຍທາງເຕັກນິກ ເພື່ອຫຼອກລວງໃຫ້ຜູ້ອື່ນຫຼົງເຊື່ອ ແລະ ປະຕິບັດຕາມ ໃນການເຂົ້າເຖິງ ແລະ ໄດ້ມາຊຶ່ງຂໍ້ມູນສ່ວນບຸກຄົນ ຫຼື ຂໍ້ມູນທາງການເງິນ, ລວມເຖິງ ກະເປົ໋າເງິນເອເລັກໂຕຣນິກ, ຊັບສິນດິຈິຕອນ ຫຼື ວິທີການສ້າງແຮງຈູງໃຈໃຫ້ເສຍຊັບ;

2. ການຫຼອກລວງຜ່ານການໂຄສະນາ ລົງທຶນ, ຂາຍສິນຄ້າ ຫຼື ບໍລິການ ທີ່ບໍ່ມີຢູ່ຈິງ ຫຼື ບໍ່ຕົງກັບຄວາມຈິງ ເພື່ອຫຼອກລວງເອົາຊັບ, ຄ່າບໍລິການ ຫຼື ການຊຳລະຄ່າສິນຄ້າລ່ວງໜ້າ ຈາກຜູ້ບໍລິໂພກ.

3. ການຫຼອກລວງຜ່ານໄຊເບີອື່ນ ທີ່ຜິດກົດໝາຍ.

**ມາດຕາ 20 (ໃໝ່) ການນຳໃຊ້ປັນຍາປະດິດ (AI) ໃນທາງທີ່ຜິດ**

ການນຳໃຊ້ປັນຍາປະດິດ (AI) ໃນທາງທີ່ຜິດ ແມ່ນການນຳໃຊ້ເຕັກໂນໂລຊີປັນຍາປະດິດ (AI) ເພື່ອສ້າງ, ດັດແກ້ ຫຼື ປ່ຽນແປງ ພາບ, ສຽງ, ວິດີໂອ ຫຼື ຂໍ້ຄວາມ, ຂໍ້ມູນປອມ ໃຫ້ຜິດໄປຈາກຄວາມເປັນຈິງ ເພື່ອທຳການຫຼອກລວງຜ່ານໄຊເບີ ແລະ ສ້າງຄວາມເສຍຫາຍໃຫ້ແກ່ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ.

ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ຈະຖືກຖືວ່າກະທຳຜິດ ໃນກໍລະນີໃດໜຶ່ງ ດັ່ງນີ້:

1. ໃຊ້ ປັນຍາປະດິດ (AI) ຕັດຕໍ່ໃບໜ້າ, ຮ່າງກາຍ ຫຼື ສຽງ ຂອງບຸກຄົນອື່ນ ໃສ່ໃນເນື້ອຫາທີ່ລາມົກ ອານາຈານ ຫຼື ເນື້ອຫາທີ່ພາໃຫ້ເກີດຄວາມອັບອາຍ ແລະ ເສື່ອມເສຍຊື່ສຽງຢ່າງຮ້າຍແຮງ;

2. ນຳໃຊ້ ເຕັກໂນໂລຊີຂັ້ນສູງ ເພື່ອສ້າງຂໍ້ມູນປອມສະເໝືອນຈິງ (Deepfake) ສ້າງພາບ, ສຽງ ຫຼື ວິດີໂອ ເພື່ອແອບອ້າງເປັນບຸກຄົນອື່ນ, ພະນັກງານ ຫຼື ຜູ້ຕາງໜ້າອົງການຈັດຕັ້ງ ເພື່ອຕົວະຍົວະ, ຫຼອກລວງເອົາຊັບສິນ ຫຼື ຂໍ້ມູນສ່ວນບຸກຄົນ (Identity Theft);

3. ນຳໃຊ້ ເຕັກໂນໂລຊີຂັ້ນສູງ ທີ່ມີລັກສະນະຄືຄວາມຈິງ ເພື່ອເຜີຍແຜ່ຂ່າວປອມ (Fake News) ທີ່ມີຈຸດປະສົງສ້າງຄວາມປັ່ນປ່ວນ, ສ້າງຄວາມແຕກແຍກ ຫຼື ສົ່ງຜົນກະທົບຕໍ່ຄວາມສະຫງົບ ແລະ ຄວາມໝັ້ນຄົງ ຂອງຊາດ;

4. ສ້າງຫຼັກຖານປອມດ້ວຍ ປັນຍາປະດິດ (AI) ເພື່ອຫວັງຜົນໃນທາງຄະດີຄວາມ ຫຼື ເພື່ອໃສ່ຮ້າຍປ້າຍສີບຸກຄົນອື່ນໃນຂະບວນການກົດໝາຍ;

5. ຜູ້ສ້າງ ຫຼື ຜູ້ໃຫ້ບໍລິການທີ່ນຳໃຊ້ AI ທີ່ບໍ່ມີປ້າຍແຈ້ງເຕືອນໃຫ້ສັງຄົມຮັບຊາບເນື້ອຫານີ້ສ້າງຂຶ້ນດ້ວຍ AI

**ມາດຕາ 21 (ໃໝ່) ການກະທຳຜິດ ຕໍ່ແມ່ຍິງ ແລະ ເດັກ ຜ່ານໄຊເບີ**

ການກະທຳຜິດຕໍ່ ແມ່ຍິງ ແລະ ເດັກ ຜ່ານໄຊເບີ ມີດັ່ງນີ້:

1. ຜະລິດ, ສະເໜີໃຫ້, ຂາຍ, ຈຳໜ່າຍ, ສົ່ງ, ເຜີຍແຜ່ພາບ-ສຽງ, ວາງສະແດງ ຫຼື ເຮັດໃຫ້ມີຢູ່ ໃນຮູບແບບຂອງສິ່ງລາມົກອານາຈານ ຕໍ່ແມ່ຍິງ ແລະ ເດັກ ຫຼື ສື່ການຊຸດຮີດທາງເພດແມ່ຍິງ ແລະ ເດັກ;

2. ຊັກຊວນ, ການຈັດຫາ ຫຼື ການເຂົ້າເຖິງສິ່ງລາມົກອານາຈານ ຫຼື ການຊຸດຮີດທາງເພດ ຕໍ່ແມ່ຍິງ ແລະ ເດັກ;

3. ການຄອບຄອງສື່ລາມົກ ແມ່ຍິງ ແລະ ເດັກ ທີ່ຖືກບັນທຶກໄວ້ໃນລະບົບຄອມພິວເຕີ, ອຸປະກອນຈັດເກັບຂໍ້ມູນ ຫຼື ສື່ເອເລັກໂຕຣນິກໃດໜຶ່ງ;

4. ການສະໜັບສະໜູນສະໜອງທຶນ, ເຄື່ອງມື ຫຼື ອຳນວຍຄວາມສະດວກ ໃຫ້ແກ່ການກະທຳຜິດ ທີ່ລະບຸໄວ້ໃນຂໍ້ 1, 2 ແລະ 3 ຂອງມາດຕານີ້;

5. ຕິດຕໍ່ສື່ສານ, ຊັກຊວນ, ລໍ້ລວງ ຫຼື ໃຊ້ກົນອຸບາຍໃດໜຶ່ງ ເພື່ອຈຸດປະສົງໃນການກະທຳຜິດທາງເພດ ຫຼື ໃຊ້ຄວາມຮຸນແຮງ ຕໍ່ແມ່ຍິງ ແລະ ເດັກ;

6. ຕິດຕໍ່ສື່ສານ ຫຼື ເຜີຍແຜ່ຂໍ້ມູນຂ່າວສານ ທີ່ມີລັກສະນະ ເປັນການບັງຄັບ, ການຂົ່ມຂູ່ ຫຼື ການປະພຶດອື່ນໂດຍເຈດຕະນາ ທີ່ມີລັກສະນະໃຊ້ຄວາມຮຸນແຮງ ທີ່ແຕະຕ້ອງເຖິງ ສຸຂະພາບ, ຊີວິດ ຫຼື ຈິດໃຈ ຕໍ່ແມ່ຍິງ ແລະ ເດັກ;

7. ຕິດຕໍ່ສື່ສານ ຫຼື ເຜີຍແຜ່ຂໍ້ມູນຂ່າວສານ ທີ່ມີລັກສະນະ ເປັນການນິນທາ, ການໃສ່ຮ້າຍ, ການປ້ອຍດ່າ, ການເຍາະເຍີ້ຍສຽດສີ, ການໝິ່ນປະໝາດ ຫຼື ການປະພຶດອື່ນ ໂດຍເຈດຕະນາ ທີ່ເຮັດໃຫ້ເສື່ອມເສຍຊື່ສຽງ, ກຽດສັກສີ ຫຼື ຈິດໃຈ ຕໍ່ແມ່ຍິງ ແລະ ເດັກ;

8. ຕິດຕໍ່ສື່ສານ ຫຼື ເຜີຍແຜ່ຂໍ້ມູນຂ່າວສານ ທີ່ມີລັກສະນະ ເປັນການທຳລາມົກ, ການທຳອານາຈານ, ການເຜີຍແຜ່ສິ່ງລາມົກ, ການທຳມິດສະຈານ, ການບັງຄັບຮ່ວມເພດ, ການຮ່ວມເພດກັບເດັກ, ການຂົ່ມຂືນທຳຊຳເລົາ, ການບັງຄັບເປັນໂສເພນີ, ການຄ້າໂສເພນີ, ຫຼື ການລວງລະເມີດທາງເພດໃນຮູບແບບອື່ນ;

9. ຕິດຕໍ່ສື່ສານ ຫຼື ເຜີຍແຜ່ຂໍ້ມູນຂ່າວສານ ທີ່ມີລັກສະນະ ເປັນການຫຼອກລວງ ເພື່ອຈຸດປະສົງທາງການເງິນ, ຜົນປະໂຫຍດທາງວັດຖຸ ຫຼື ຂໍ້ມູນທາງການເງິນຂອງ ແມ່ຍິງ ແລະ ເດັກ.

10. ມີພຶດຕິກຳອື່ນທີ່ເປັນການກະທຳຜິດຕໍ່ ແມ່ຍິງ ແລະ ເດັກ ຜ່ານທາງໄຊເບີ.

**ມາດຕາ 22 (ໃໝ່) ການຟອກເງິນທີ່ໄດ້ຈາກອາຊະຍາກຳໄຊເບີ**

ການຟອກເງິນທີ່ໄດ້ຈາກອາຊະຍາກຳໄຊເບີ ແມ່ນ ການກະທຳໃດໜຶ່ງ ທີ່ມີເຈດຕະນາເພື່ອປົກປິດ, ເຊື່ອງອຳ, ຫັນປ່ຽນ ຫຼື ເຄື່ອນຍ້າຍ ເງິນ ຫຼື ຊັບສິນ ທີ່ໄດ້ມາຈາກການກໍ່ອາຊະຍາກຳທາງໄຊເບີ ເພື່ອໃຫ້ກາຍເປັນຊັບສິນທີ່ ຖືກຕ້ອງຕາມກົດໝາຍ ດ້ວຍຮູບແບບ ດັ່ງນີ້:

1. ການຮັບ, ຄອບຄອງ, ນຳໃຊ້, ຫັນປ່ຽນ ຫຼື ໂອນເງິນ ແລະ ຊັບສິນ ທີ່ຕົນເອງຮູ້ ຫຼື ຄວນຈະຮູ້ວ່າໄດ້ມາຈາກການກະທຳຜິດ ຕາມທີ່ໄດ້ລະບຸໄວ້ໃນ ມາດຕາ 9 ຫາ 15 ຂອງກົດໝາຍສະບັບນີ້;

2. ການປິດບັງ ຫຼື ເຊື່ອງອຳ ລັກສະນະທີ່ແທ້ຈິງ, ແຫຼ່ງທີ່ມາ, ທີ່ຕັ້ງ, ການຈຳໜ່າຍ, ການເຄື່ອນຍ້າຍ ຫຼື ສິດຄອບຄອງຊັບສິນ ໂດຍນຳໃຊ້ເຕັກໂນໂລຊີທາງການເງິນ, ສະກຸນເງິນດິຈິຕອນ (Cryptocurrency) ຫຼື ລະບົບການຊຳລະເງິນທາງເອເລັກໂຕຣນິກ.

3. ການນຳໃຊ້ ບັນຊີຕົວແທນ ເພື່ອຮັບເງິນທີ່ໄດ້ມາຈາກການສໍ້ໂກງ ຫຼື ການກະທຳຜິດທາງໄຊເບີ ເພື່ອຫຼີກເວັ້ນການກວດສອບຂອງເຈົ້າໜ້າທີ່.

4. ການໃຫ້ຄຳປຶກສາ, ການຈັດຫາວິທີການ ຫຼື ການສ້າງຊຸດຄຳສັ່ງ/ໂປຣແກຣມ ເພື່ອອຳນວຍຄວາມສະດວກໃນການຟອກເງິນທີ່ໄດ້ຈາກອາຊະຍາກຳທາງໄຊເບີ.

ຂະແໜງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ແລະ ທະນາຄານ ແຫ່ງ ສປປ ລາວ ປະສານກັບຂະແໜງການທີ່ກ່ຽວຂ້ອງ ເພື່ອຈັດຕັ້ງປະຕິບັດມາດຕະການຕ້ານການຟອກເງິນ ທີ່ໄດ້ຈາກອາຊະຍາກຳໄຊເບີ.

## ພາກທີ III
## ການເຄື່ອນໄຫວຕ້ານ ແລະ ສະກັດກັ້ນ ອາຊະຍາກຳໄຊເບີ
### ໝວດທີ 1
### ວຽກງານຕ້ານອາຊະຍາກຳໄຊເບີ

**ມາດຕາ 23 (ປັບປຸງ) ວຽກງານຕ້ານອາຊະຍາກຳໄຊເບີ**

ວຽກງານຕ້ານອາຊະຍາກຳໄຊເບີ ມີ ດັ່ງນີ້:

1. ການແຈ້ງເຕືອນ;
2. ການໃຫ້ຄຳປຶກສາ;
3. ການແຈ້ງເຫດສຸກເສີນ;
4. ການດຳເນີນການແກ້ໄຂ.

**ມາດຕາ 24 (ປັບປຸງ) ການແຈ້ງເຕືອນ**

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ສົມທົບກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ໃນການຕິດຕາມ, ວິເຄາະ ແລະ ແຈ້ງເຕືອນ ພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳໄຊເບີ ເກີດຂຶ້ນ ຫຼື ຄາດວ່າອາດຈະເກີດຂຶ້ນ, ລະບຸມາດຕະການປ້ອງກັນ ຫຼື ວິທີການແກ້ໄຂເບື້ອງຕົ້ນ ແລະ ສ້າງຄວາມຮັບຮູ້ ໃຫ້ແກ່ສັງຄົມຢ່າງທັນການ.

ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ແຈ້ງເຕືອນ ເມື່ອພົບເຫັນພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳທາງໄຊເບີ ຫຼື ຄວາມສ່ຽງທີ່ຈະສົ່ງຜົນກະທົບຕໍ່ສັງຄົມ ໂດຍຜ່ານຊ່ອງທາງຂອງຕົນ ແລະ ແຈ້ງໃຫ້ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຮັບຮູ້.

**ມາດຕາ 25 (ປັບປຸງ) ການໃຫ້ຄຳປຶກສາ**

ຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນຜູ້ໃຫ້ຄຳປຶກສາ, ແນະນຳ ວິທີການປ້ອງກັນ ແລະ ການແກ້ໄຂທາງດ້ານເຕັກນິກ ແກ່ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ເພື່ອຫຼຸດຜ່ອນການສູນເສຍຂໍ້ມູນ, ການລຶບກວນຂໍ້ມູນ, ບໍ່ໃຫ້ມີການຢຸດຕິການທຳງານຂອງລະບົບຄອມພິວເຕີ, ການກູ້ຄືນຂໍ້ມູນ ແລະ ລະບົບຄອມພິວເຕີທີ່ຖືກທຳລາຍໃຫ້ກັບຄືນສູ່ສະພາບປົກກະຕິ, ສະກັດກັ້ນ ການກະຈາຍໄວຣັດຄອມພິວເຕີ ແລະ ການເຂົ້າທຳລາຍຂໍ້ມູນໃນລະບົບຄອມພິວເຕີ.

**ມາດຕາ 26 (ປັບປຸງ) ການແຈ້ງເຫດສຸກເສີນ**

ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທັງພາຍໃນ ແລະ ຕ່າງປະເທດ ທີ່ດຳລົງຊີວິດ, ເຄື່ອນໄຫວ ຫຼື ນຳໃຊ້ລະບົບຄອມພິວເຕີ ແລະ/ຫຼື ຂໍ້ມູນຄອມພິວເຕີ ຢູ່ ສປປ ລາວ ຕ້ອງແຈ້ງເຫດສຸກເສີນ ກ່ຽວກັບອາຊະຍາກຳ ໄຊເບີ ທີ່ເກີດຂຶ້ນຕໍ່ຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຫຼື ເຈົ້າໜ້າທີ່ທີ່ກ່ຽວຂ້ອງ.

ການແຈ້ງເຫດສຸກເສີນ ສາມາດດຳເນີນດ້ວຍວິທີການ ດັ່ງນີ້:

1. ຄຳຮ້ອງຕາມແບບພິມ;
2. ໂທລະສັບ, ແຟັກ, ສາຍດ່ວນ;
3. ຈົດໝາຍເອເລັກໂຕຣນິກ;
4. ວິທີການອື່ນ.

**ມາດຕາ 27 (ປັບປຸງ) ການດຳເນີນການແກ້ໄຂ**

ພາຍຫຼັງໄດ້ຮັບການແຈ້ງເຫດສຸກເສີນທາງລະບົບຄອມພິວເຕີແລ້ວ ຂະແໜງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຕ້ອງຄົ້ນຄວ້າພິຈາລະນາ ແລະ ແຈ້ງຕອບພ້ອມທັງແນະນຳວິທີການແກ້ໄຂ ພາຍໃນກຳນົດເວລາ ຫ້າວັນລັດຖະການ.

ໃນກໍລະນີຈຳເປັນ ແລະ ຮີບດ່ວນ ຂະແໜງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຕ້ອງປະສານກັບຂະແໜງການທີ່ກ່ຽວຂ້ອງ ດຳເນີນການແກ້ໄຂທາງເຕັກນິກວິຊາການ ຕາມການແຈ້ງເຫດຂອງຜູ້ກ່ຽວຂ້ອງຢ່າງທັນການ.

ໃນກໍລະນີໄດ້ຮັບການແຈ້ງເຫດ ກ່ຽວກັບພຶດຕິກຳທີ່ໄດ້ກຳນົດໄວ້ໃນມາດຕາ 8 ຂອງ ກົດໝາຍສະບັບນີ້ ຊຶ່ງແຕະຕ້ອງເຖິງຄວາມໝັ້ນຄົງຂອງຊາດ ຫຼື ກຽດສັກສີຂອງບຸກຄົນໃດໜຶ່ງນັ້ນ ຂະແໜງການທີ່ກ່ຽວຂ້ອງ ທັງສູນກາງ ແລະ ທ້ອງຖິ່ນ ຕ້ອງຄົ້ນຄວ້າພິຈາລະນາຕອບໂຕ້ຕາມແຕ່ລະກໍລະນີ.

## ໝວດທີ 2
## ວຽກງານສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ

**ມາດຕາ 28 ວຽກງານສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີໄຊເບີ**

ວຽກງານສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ມີ ດັ່ງນີ້:

1. ການຈັດຕັ້ງໂຄສະນາເຜີຍແຜ່;
2. ການຝຶກອົບຮົມ;
3. ການໃຫ້ຄວາມຮູ້ກ່ຽວກັບຄວາມປອດໄພໄຊເບີ;
4. ການສ້າງກົດຈະກຳປ້ອງກັນຂໍ້ມູນ;
5. ການເຝົ້າລະວັງເຫດສຸກເສີນ;
6. ການເກັບກຳສະຖິຕິ.

**ມາດຕາ 29 (ປັບປຸງ) ການຈັດຕັ້ງໂຄສະນາເຜີຍແຜ່**

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນຜູ້ສ້າງປຶ້ມຄູ່ມື, ສະຕິກເກີ, ແຜ່ນໂຄສະນາ, ສື່ສິ່ງພິມ, ສື່ສັງຄົມອອນລາຍ ແລະ ສື່ດິຈິຕອນ ອື່ນໆ ກ່ຽວກັບການເຝົ້າລະວັງ, ປ້ອງກັນໄພ ໄຊເບີ, ປະສານສົມທົບກັບຂະແໜງການອື່ນ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນທີ່ກ່ຽວຂ້ອງ ໂຄສະນາເຜີຍແຜ່ ໃນຂອບເຂດທົ່ວປະເທດ.

**ມາດຕາ 30 (ປັບປຸງ) ການຝຶກອົບຮົມ**

ຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ປະສານສົມທົບກັບຂະແໜງການອື່ນ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນທີ່ກ່ຽວຂ້ອງ ຈັດຝຶກອົບຮົມໃຫ້ແກ່ພະນັກງານ, ເຈົ້າໜ້າທີ່ ທີ່ກ່ຽວຂ້ອງ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ລວມທັງວຽກງານສືບສວນ- ສອບສວນ.

**ມາດຕາ 31 (ປັບປຸງ) ການໃຫ້ຄວາມຮູ້ກ່ຽວກັບຄວາມປອດໄຊເບີ**

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນເຈົ້າການປະສານສົມທົບກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ກຳນົດມາດຕະການສະເພາະໃນການຮັກສາຄວາມປອດໄພໄຊເບີ ແລະ ໃຫ້ຄວາມຮູ້ກ່ຽວກັບມາດຕະການດັ່ງກ່າວແກ່ສັງຄົມ.

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນເຈົ້າການປະສານສົມທົບກັບ ກະຊວງສຶກສາທິການ ແລະ ກິລາ ນຳເອົາວິຊາຮຽນດ້ານຄວາມປອດໄພໄຊເບີ ບັນຈຸເຂົ້າ ໃນຫຼັກສູດ ການຮຽນ-ການສອນແຕ່ຊັ້ນມັດທະຍົມສຶກສາຕອນຕົ້ນຂຶ້ນໄປ.

**ມາດຕາ 32 (ປັບປຸງ) ການສ້າງກົດຈະກຳປ້ອງກັນຂໍ້ມູນ**

ຂະແໜງ ການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນເຈົ້າການສ້າງກົດຈະກຳໃຫ້ຄວາມຮູ້ໃນການປົກປ້ອງຂໍ້ມູນ ຢູ່ຕາມອົງການຈັດຕັ້ງຂອງລັດ, ເອກະຊົນ ແລະ ສະຖານການສຶກສາ ເພື່ອຮັບປະກັນຄວາມປອດໄພໄຊເບີ ແລະ ການປ້ອງກັນຂໍ້ມູນຄອມພິວເຕີ.

ອົງການຈັດຕັ້ງລັດ ແລະ ເອກະຊົນ ທີ່ນຳໃຊ້ລະບົບດິຈິຕອນ ຕ້ອງສ້າງລະບຽບການຄຸ້ມຄອງຂໍ້ມູນ ແລະ ແຜນຮັບມືກັບເຫດສຸກເສີນທາງໄຊເບີ ພ້ອມທັງສ້າງກົດຈະກຳປ້ອງກັນຂໍ້ມູນພາຍໃນເປັນແຕ່ລະໄລຍະ.

**ມາດຕາ 33 (ປັບປຸງ) ການເຝົ້າລະວັງເຫດສຸກເສີນ**

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນຜູ້ເຝົ້າລະວັງເຫດສຸກເສີນ ດ້ວຍການຕິດຕາມ, ກວດກາ, ແນະນຳ, ແຈ້ງເຕືອນ, ປ້ອງກັນ ແລະ ຕອບໂຕ້ໄພຄຸກຄາມທາງໄຊເບີ.

ບຸກຄົນ, ນິຕິກຳບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງຕິດຕາມການນຳໃຊ້ສື່ສັງຄົມອອນລາຍ ແລະ ມີມາດຕະການຕອບໂຕ້ ເມື່ອເຫັນວ່າ ມີແອບອ້າງ ການນຳໃຊ້ຂໍ້ມູນ, ການບໍລິການ, ຊື່ສຽງ ຂອງຕົນ ເພື່ອ ຕົວະຍົວະ, ຫຼອກຫຼວງ ຫຼື ກະທຳຜິດອື່ນ ຜ່ານທາງອິນເຕີເນັດ. ໂດຍອອກມາໃຫ້ຂໍ້ມູນຖືກຕ້ອງ ຢ່າງທັນການ ແລະ ພ້ອມແຈ້ງເຈົ້າໜ້າທີ່ກ່ຽວຂ້ອງດ່ວນ.

**ມາດຕາ 34 (ປັບປຸງ) ການເກັບກາຂໍ້ມູນ**

ຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ສົມທົບກັບ ຂະແໜງການປ້ອງກັນຄວາມສະຫງົບແລະຂະແໜງການທີ່ກ່ຽວຂ້ອງ ເກັບກຳ ຂໍ້ມູນ ແລະ ສ້າງຖານຂໍ້ມູນ ກ່ຽວກັບອາຊະຍາກຳ ໄຊເບີ ພ້ອມທັງສຶກສາຄົ້ນຄວ້າເປັນແຕ່ລະໄລຍະ ເພື່ອຊອກຮູ້ເງື່ອນໄຂ ແລະ ສາເຫດທີ່ພາໃຫ້ເກີດອາຊະຍາກຳ ໄຊເບີ.

ຜູ້ໃຫ້ບໍລິການ ທີ່ມີການເກັບຂໍ້ມູນຜູ້ໃຊ້ ຕ້ອງເກັບຂໍ້ມູນທີ່ບົ່ງບອກຕົວຕົນຂອງຜູ້ໃຊ້ໃຫ້ຖືກຕ້ອງ ແລະ ຄົບຖ້ວນມີ ແລະ ມີມາດຕະການດ້ານຄວາມປອດໄພ, ປ້ອງກັນການ ຮົ່ວໄຫຼ ຂອງຂໍ້ມູນ ອອກສູ່ສາທາລະນະ.

ຜູ້ໃຫ້ບໍລິການ ຕ້ອງຮັກສາຂໍ້ມູນຈະລາຈອນທາງລະບົບຄອມພິວເຕີ ຢ່າງໜ້ອຍ 90 ວັນ.

**ມາດຕາໃໝ່ 35 ການລະງັບການໃຫ້ບໍລິການ**

ຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ສົມທົບກັບ ພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ນຳໃຊ້ ມາດຕະການ ຈຳກັດ ຫຼື ລະງັບການບໍລິການ ທາງດ້ານໂທລະຄົມມະນາຄົມ, ອິນເຕີເນັດ ແລະ ການສື່ສານທັງໝົດ ຫຼື ບາງ ສ່ວນ ເມື່ອເຫັນວ່າອາຊະຍາກຳທາງໄຊເບີອາດຈະເກີດຂຶ້ນ ຫຼື ກຳລັງເກີດຂຶ້ນ ຢ່າງຮ້າຍແຮງ.

ຜູ້ໃຫ້ບໍລິການ ຕ້ອງລະງັບການເຂົ້າເຖິງບໍລິການຂອງຕົນ ບາງສ່ວນ ຫຼື ທັງໝົດ ເມື່ອມີການແຈ້ງຈາກຜູ້ ໃຊ້ບໍລິການຂອງຕົນ ຫຼື ເຈົ້າໜ້າທີ່ກ່ຽວຂ້ອງ ຜ່ານວິທີການທີ່ໄດ້ກຳນົດໄວ້ ຫຼື ພົບເຫັນມີການນຳໃຊ້ໃນການ ກະທຳຜິດທາງໄຊເບີ ພ້ອມທັງແຈ້ງພາກສ່ວນທີ່ກ່ຽວຂ້ອງໂດຍດ່ວນ.

## ໝວດທີ 3 (ປັບປຸງ)
## ໜ່ວຍງານຕ້ານ ແລະ ສະກັດກັ້ນ ອາຊະຍາກຳໄຊເບີ

**ມາດຕາ 36 (ປັບປຸງ) ໜ່ວຍງານຕ້ານ ແລະ ສະກັດກັ້ນ ອາຊະຍາກຳໄຊເບີ**

ໜ່ວຍງານຕ້ານ ແລະ ສະກັດກັ້ນ ອາຊະຍາກຳໄຊເບີ ແມ່ນໜ່ວຍງານທາງດ້ານວິຊາສະເພາະທີ່ມີພາລະບົດບາດ ໃນການຄຸ້ມຄອງ, ຕິດຕາມ, ກວດກາ. ໃຫ້ການສຶກສາ ແລະ ຄຳປຶກສາ, ແກ້ໄຂ ແລະ ສະກັດກັ້ນ ອາຊະຍາກຳທາງໄຊ ເບີ ໃນຂອບເຂດທົ່ວປະເທດ ໂດຍປະກອບ ສາມ ໜ່ວຍງານ ດັ່ງນີ້:

1. **ໜ່ວຍງານຕອບໂຕ້ເຫດການສຸກເສີນທາງໄຊເບີ (CERT)**
2. **ໜ່ວຍງານເຝົ້າລະວັງຄວາມປອດໄພທາງໄຊເບີ (SOC)**
3. **ໜ່ວຍງານຕ້ານການຕິວະຍິວະຫຼອກລວງທາງອອນລາຍ**

**ມາດຕາ 37 (ໃໝ່) ໜ່ວຍງານຕອບໂຕ້ເຫດການສຸກເສີນທາງໄຊເບີ (CERT)**

ໜ່ວຍງານຕອບໂຕ້ເຫດການສຸກເສີນທາງໄຊເບີ ມີໜ້າທີ່ເປັນຈຸດປະສານງານຫຼັກທັງພາຍໃນ ແລະ ຕ່າງປະເທດ ໃນການຮັບແຈ້ງເຫດ, ວິເຄາະ, ໃຫ້ຄຳແນະນຳ ແລະ ເຂົ້າຊ່ວຍເຫຼືອໃນການແກ້ໄຂເຫດການລະເມີດ ຄວາມປອດໄພທາງໄຊເບີ ຢ່າງທັນການ ເພື່ອຫຼຸດຜ່ອນຜົນກະທົບຕໍ່ລະບົບຂໍ້ມູນຂ່າວສານ ແລະ ໂຄງລ່າງພື້ນຖານທີ່ ສຳຄັນຂອງຊາດ;

**ມາດຕາ 38 (ໃໝ່) ໜ່ວຍງານເຝົ້າລະວັງຄວາມປອດໄພທາງໄຊເບີ (SOC)**

ໜ່ວຍງານເຝົ້າລະວັງຄວາມປອດໄພທາງໄຊເບີ ມີໜ້າທີ່ປະຕິບັດການເຝົ້າລະວັງ, ຕິດຕາມ ແລະ ກວດກາ ຄວາມຜິດປົກກະຕິຂອງລະບົບເຄືອຂ່າຍ ແລະ ຂໍ້ມູນຂ່າວສານ ແບບຕໍ່ເນື່ອງ ຕະຫຼອດຊາວສີ່ຊົ່ວໂມງ ເພື່ອຄົ້ນຫາ, ວິເຄາະໄພຄຸກຄາມ ແລະ ສະກັດກັ້ນການໂຈມຕີທາງໄຊເບີ ໃນທຸກຮູບແບບ ກ່ອນເກີດຄວາມເສຍຫາຍ;

**ມາດຕາ 39 (ໃໝ່) ໜ່ວຍງານຕ້ານການຕົວະຍົວະຫຼອກລວງທາງອອນລາຍ**

ໜ່ວຍງານຕ້ານການຕົວະຍົວະຫຼອກລວງທາງອອນລາຍ ມີໜ້າທີ່ ຕິດຕາມ, ເກັບກຳຂໍ້ມູນ ແລະ ປະສານສົມທົບກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ເພື່ອສະກັດກັ້ນ, ຈຳກັດ ແລະ ແກ້ໄຂ ບັນຫາການສໍ້ໂກງຊັບ, ການຕົວະຍົວະຫຼອກລວງຜ່ານສື່ສັງຄົມອອນລາຍ, ເວັບໄຊ ຫຼື ລະບົບໂທລະຄົມມະນາຄົມ ທີ່ເປັນອັນຕະລາຍຕໍ່ສັງຄົມ;

## ພາກທີ IV
## ການສືບສວນ-ສອບສວນຄະດີໄຊເບີ

**ມາດຕາ 40 ສາເຫດທີ່ພາໃຫ້ເປີດການສືບສວນ-ສອບສວນ**

ສາເຫດທີ່ພາໃຫ້ເປີດການສືບສວນ-ສອບສວນຄະດີໄຊເບີ ມີ ດັ່ງນີ້:

1. ມີການແຈ້ງຄວາມ, ການລາຍງານ, ການຮ້ອງຟ້ອງ ຂອງບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ກ່ຽວກັບພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳໄຊເບີ;
2. ມີການເຂົ້າມອບຕົວຂອງຜູ້ກະທຳຜິດ;
3. ພົບເຫັນຮ່ອງຮອຍ, ຂໍ້ມູນ, ຫຼັກຖານ ຂອງພຶດຕິກຳ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນມາດຕາ 8 ຂອງກົດໝາຍສະບັບນີ້.

**ມາດຕາ 41 ຂັ້ນຕອນການສືບສວນ-ສອບສວນຄະດີໄຊເບີ**

ໃນການສືບສວນ-ສອບສວນຄະດີໄຊເບີ ໃຫ້ປະຕິບັດ ດັ່ງນີ້:

1. ການແຈ້ງຄວາມ, ການລາຍງານ ຫຼື ການຮ້ອງຟ້ອງ;
2. ການເປີດການສືບສວນ-ສອບສວນ;
3. ການດຳເນີນການສືບສວນ-ສອບສວນ;
4. ການສະຫຼຸບການສືບສວນ-ສອບສວນ ແລະ ການປະກອບສຳນວນຄະດີ.

**ມາດຕາ 42 ການແຈ້ງຄວາມ, ການລາຍງານ ຫຼື ການຮ້ອງຟ້ອງ**

ການແຈ້ງຄວາມ, ການລາຍງານ ຫຼື ການຮ້ອງຟ້ອງ ກ່ຽວກັບການກະທຳຜິດໄຊເບີ ໃຫ້ແຈ້ງ ຫຼື ຍື່ນຕໍ່ອົງການສືບສວນ-ສອບສວນຂອງເຈົ້າໜ້າທີ່ຕຳຫຼວດ ຫຼື ອົງການໄອຍະການປະຊາຊົນ.

ອົງການສືບສວນ-ສອບສວນຂອງເຈົ້າໜ້າທີ່ຕຳຫຼວດ ຫຼື ອົງການໄອຍະການປະຊາຊົນ ຕ້ອງພິຈາລະນາການແຈ້ງຄວາມ, ການລາຍງານ ຫຼື ການຮ້ອງຟ້ອງ ບໍ່ໃຫ້ເກີນ ຫ້າວັນ ລັດຖະການ ນັບແຕ່ວັນໄດ້ຮັບການແຈ້ງຄວາມ, ການລາຍງານ ຫຼື ການຮ້ອງຟ້ອງ ເປັນຕົ້ນໄປ. ໃນກໍລະນີ ມີຄວາມຫຍຸ້ງຍາກສັບສົນ ການພິຈາລະນາດັ່ງກ່າວ ແມ່ນບໍ່ໃຫ້ເກີນ ສິບວັນ ລັດຖະການ.

**ມາດຕາ 43 ການເປີດການສືບສວນ-ສອບສວນ**

ໃນກໍລະນີ ທີ່ມີຂໍ້ມູນໜັກແໜ້ນ ກ່ຽວກັບການກະທຳຜິດໄຊເບີ ຫົວໜ້າອົງການສືບສວນ-ສອບສວນຂອງເຈົ້າໜ້າທີ່ຕຳຫຼວດ ຫຼື ຫົວໜ້າອົງການໄອຍະການປະຊາຊົນ ຕ້ອງອອກຄຳສັ່ງເປີດການສືບສວນ-ສອບສວນໃນຂອບເຂດສິດ ແລະ ໜ້າທີ່ ຂອງຕົນຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍວ່າດ້ວຍການດຳເນີນຄະດີອາຍາ.

ໃນກໍລະນີຈຳເປັນ, ຮີບດ່ວນ ແລະ ມີຂໍ້ມູນທີ່ຢັ້ງຢືນໄດ້ວ່າ ກຳລັງມີການກະກຽມ ຫຼື ກໍ່ອາຊະຍາກຳໄຊເບີ ຫົວໜ້າອົງການສືບສວນ-ສອບສວນຂອງເຈົ້າໜ້າທີ່ຕຳຫຼວດ ຫຼື ຫົວໜ້າອົງການໄອຍະການປະຊາຊົນ ຕ້ອງອອກຄຳສັ່ງໃຫ້ເກັບຮັກສາ ແລະ ປ້ອງກັນຂໍ້ມູນທາງຄອມພິວເຕີ ຫຼື ຂໍ້ມູນ ຈະລາຈອນທາງລະບົບຄອມພິວເຕີ.

ຜູ້ໃຫ້ບໍລິການ ຫຼື ພາກສ່ວນທີ່ຄຸ້ມຄອງຂໍ້ມູນ ມີພັນທະເກັບຮັກສາ ແລະ ປົກປ້ອງຂໍ້ມູນດັ່ງກ່າວ ໄວ້ເປັນຢ່າງດີ ຈົນກວ່າຈະສິ້ນສຸດການດຳເນີນຄະດີ ເພື່ອຮັບປະກັນບໍ່ໃຫ້ຂໍ້ມູນມີການປ່ຽນແປງ ຫຼື ເສຍຫາຍ.

**ມາດຕາ 44 ການດຳເນີນການສືບສວນ-ສອບສວນ**

ອົງການສືບສວນ-ສອບສວນຂອງເຈົ້າໜ້າທີ່ຕຳຫຼວດ ຫຼື ອົງການໄອຍະການປະຊາຊົນ ຕ້ອງປະສານສົມທົບກັບ ຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ແລະ ພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ເພື່ອດຳເນີນການຄົ້ນຫາຂໍ້ມູນຫຼັກຖານ ແລະ ທີ່ມາຂອງອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ເພື່ອເປັນບ່ອນອີງໃຫ້ແກ່ການສືບສວນ-ສອບສວນ.

ການດຳເນີນການສືບສວນ-ສອບສວນຄະດີທາງລະບົບຄອມພິວເຕີ ຕ້ອງນຳໃຊ້ວິທີການສືບ ສວນ-ສອບ ສວນ, ມາດຕະການສະກັດກັ້ນ ແລະ ກຳນົດເວລາໃນການສືບສວນ-ສອບສວນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດ ໝາຍວ່າດ້ວຍການດຳເນີນຄະດີອາຍາ.

**ມາດຕາ 45 ການສະຫຼຸບການສືບສວນ-ສອບສວນ ແລະ ການປະກອບສຳນວນຄະດີ**

ພາຍຫຼັງສິ້ນສຸດການສືບສວນ-ສອບສວນ ຂອງເຈົ້າໜ້າທີ່ຕຳຫຼວດ ຖ້າມີຂໍ້ມູນຫຼັກຖານທີ່ໜັກແໜ້ນວ່າການລະເມີດນັ້ນ ເປັນການກະທຳຜິດທາງລະບົບຄອມພິວເຕີ ອົງການສືບສວນ-ສອບສວນ ຕ້ອງສະຫຼຸບ ແລະ ປະກອບສຳນວນຄະດີສົ່ງໃຫ້ອົງການໄອຍະການປະຊາຊົນ ພິຈາລະນາສັ່ງຟ້ອງຂຶ້ນສານ.

ໃນກໍລະນີ ອົງການໄອຍະການປະຊາຊົນ ຫາກເປັນຜູ້ດຳເນີນການສືບສວນ-ສອບສວນ ກໍຕ້ອງ ສະຫຼຸບ, ປະກອບສຳນວນຄະດີ, ອອກຄຳສັ່ງຟ້ອງ ແລະ ຄຳຖະແຫຼງຂຶ້ນສານ ເພື່ອພິຈາລະນາຕັດສິນຄະດີ ຕາມກົດໝາຍ.

**ມາດຕາ 46 (ໃໝ່): ການຍຶດ, ການອາຍັດ, ການຮີບຊັບສິນ ການຄືນຊັບສິນ ທີ່ເກີດຈາກການກໍ່ອາຊະຍາກຳ**

ເຈົ້າໜ້າທີ່ສືບສວນ-ສອບສວນ ທີ່ກ່ຽວຂ້ອງ ມີສິດນຳໃຊ້ມາດຕະການ ຍຶດ ຫຼື ອາຍັດ ຊັບ ລວມທັງຊັບສິນດີຈີຕອນ ໃນກໍລະນີ ກວດພົບ, ພົບເຫັນ ຫຼື ສົງໄສວ່າເປັນພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳທາງໄຊເບີ ທີ່ລະບຸໄວ້ໃນ ມາດຕາ 8 ຂອງກົດໝາຍສະບັບນີ້.

ຊັບສິນທີ່ໄດ້ມາຈາກການກະທຳຜິດທາງລະບົບຄອມພິວເຕີ ໂດຍກົງ ຫຼື ທາງອ້ອມ ຕາມຄຳຕັດສິນຂອງສານ ຈະຖືກຮີບເປັນຂອງລັດ.

ກໍລະນີທີ່ມີຫຼັກຖານຢັ້ງຢືນວ່າ ຊັບ, ວັດຖຸສິ່ງຂອງ ທີ່ຍຶດ ຫຼື ອາຍັດ ຫາກເປັນກຳມະສິດທີ່ຖືກຕ້ອງຂອງຜູ້ຖືກເສຍຫາຍ ກໍ່ໃຫ້ສົ່ງຄືນຜູ້ກ່ຽວ.

ກໍລະນີຊັບສິນເປັນເງິນດີຈີຕອນ (Cryptocurrency), ການສົ່ງຄືນຊັບສົນຕ້ອງດຳເນີນຜ່ານຂະບວນການທີ່ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ວາງອອກ ເພື່ອຮັບປະກັນວ່າມູນຄ່າ ແລະ ຄວາມປອດໄພຂອງຊັບສິນຍັງຄົບຖ້ວນ.

## ພາກທີ V
## ການຮ່ວມມືສາກົນ ໃນການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ

### ມາດຕາ 47 ຫຼັກການພື້ນຖານໃນການຮ່ວມມືສາກົນ

ການຮ່ວມມືສາກົນໃນການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ລະຫວ່າງ ອົງການທີ່ມີສິດອຳນາດ ຂອງ ສປປ ລາວ ແລະ ຕ່າງປະເທດ ໃຫ້ປະຕິບັດຕາມຫຼັກການ ເຄົາລົບເອກະລາດ, ອຳນາດອະທິປະໄຕ ແລະ ຜົນແຜ່ນດິນອັນຄົບຖ້ວນຂອງກັນ, ບໍ່ແຊກແຊງວຽກງານພາຍໃນ ຂອງກັນ ແລະ ກັນ, ສະເໝີພາບ, ຕ່າງຝ່າຍ ຕ່າງມີຜົນປະໂຫຍດ ແລະ ສອດຄ່ອງ ກັບສັນຍາສາກົນ ແລະ ສົນທິສັນຍາ ທີ່ ສປປ ລາວ ເປັນພາຄີ.

### ມາດຕາ 48 ການຮ່ວມມືທາງດ້ານເຕັກນິກວິຊາການ

ການຮ່ວມມືສາກົນທາງດ້ານເຕັກນິກວິຊາການ ໃນວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ມີ ເນື້ອໃນຕົ້ນຕໍ ດັ່ງນີ້:

1. ການແລກປ່ຽນຂໍ້ມູນຂ່າວສານ ທາງດ້ານເຕັກນິກວິຊາການ ລວມທັງການຄົ້ນຄວ້າມາດຕະການ ກ່ຽວ ກັບການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ;
2. ການລະງັບ ຫຼື ແຈ້ງໃຫ້ຢຸດເຊົາ ການທຳລາຍທາງລະບົບຄອມພິວເຕີ;
3. ການປະສານກັບຜູ້ໃຫ້ບໍລິການຢູ່ຕ່າງປະເທດ ກ່ຽວກັບການນຳໃຊ້ສື່ສັງຄົມອອນລາຍ ທີ່ມີເນື້ອໃນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນມາດຕາ 13 ຂອງກົດໝາຍສະບັບນີ້;
4. ການໃຫ້ການຊ່ວຍເຫຼືອຊຶ່ງກັນ ແລະ ກັນໃນການເຝົ້າລະວັງ, ຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ໃນງານສຳຄັນ ເປັນຕົ້ນ ກອງປະຊຸມລະດັບຊາດ, ພາກພື້ນ ແລະ ສາກົນ ລວມທັງງານມະຫາກຳຕ່າງໆ.

### ມາດຕາ 49 ການຊ່ວຍເຫຼືອຊຶ່ງກັນ ແລະ ກັນ ທາງກົດໝາຍ

ການຊ່ວຍເຫຼືອຊຶ່ງກັນ ແລະ ກັນ ທາງກົດໝາຍ ດຳເນີນດ້ວຍການຮ້ອງຂໍໃຫ້ທຳການສືບສວນ- ສອບ ສວນ, ນຳໃຊ້ມາດຕະການສະກັດກັ້ນ, ອອກຄຳສັ່ງໃຫ້ເກັບຮັກສາ ແລະ ປ້ອງກັນຂໍ້ມູນໄຊເບີ ລວມທັງຂໍ້ມູນ ຈະລາຈອນທາງລະບົບຄອມພິວເຕີ, ການຊອກຄົ້ນ, ການບົ່ງຕົວ ແລະ ຊີ້ຕົວຜູ້ ກະທຳຜິດ, ການຍຶດ ຫຼື ການອາ ຍັດອຸປະກອນ ຫຼື ເຄື່ອງມືທີ່ໃຊ້ ແລະ ພົວພັນກັບການກະທຳຜິດ, ການຂໍ ຫຼັກຖານເພີ່ມເຕີມ ກ່ຽວກັບການ ກະທຳຜິດ ແລະ ການສົ່ງຜູ້ຮ້າຍຂ້າມແດນ.

ສຳລັບກົນໄກ ແລະ ຂັ້ນຕອນຂອງການຊ່ວຍເຫຼືອຊຶ່ງກັນ ແລະ ກັນ ທາງກົດໝາຍນັ້ນ ໃຫ້ປະຕິບັດ ຕາມ ກົດໝາຍ ແລະ ລະບຽບການທີ່ກ່ຽວຂ້ອງຂອງ ສປປ ລາວ, ສັນຍາສາກົນ ແລະ ສົນທິສັນຍາ ທີ່ ສປປ ລາວ ເປັນພາຄີ.

### ມາດຕາ 50 ເນື້ອໃນຂອງການຮ້ອງຂໍ ການຊ່ວຍເຫຼືອຊຶ່ງກັນ ແລະ ກັນ ທາງກົດໝາຍ

ການຮ້ອງຂໍ ການຊ່ວຍເຫຼືອຊຶ່ງກັນ ແລະ ກັນ ທາງກົດໝາຍ ມີ ເນື້ອໃນຕົ້ນຕໍ ດັ່ງນີ້:

1. ຈຸດປະສົງ, ຄວາມຈຳເປັນ ແລະ ສະພາບຄວາມເປັນຈິງໃນການຮ້ອງຂໍ;
2. ຂໍ້ມູນທີ່ສຳຄັນສຳລັບການຢັ້ງຢືນ, ການຕິດຕາມ ແລະ ການບົ່ງຕົວຜູ້ກະທຳຜິດເປັນອາຊະຍາກຳໄຊ ເບີ;
3. ການສະໜອງຫຍໍ້ ກ່ຽວກັບຂໍ້ມູນທາງລະບົບຄອມພິວເຕີ ຫຼື ຂໍ້ມູນຈະລາຈອນທາງລະບົບຄອມພິວເຕີ ທີ່ຕ້ອງການເກັບຮັກສາ ຫຼື ປ້ອງກັນສະເພາະ;
4. ບ່ອນອີງທາງດ້ານນິຕິກຳ ກ່ຽວກັບການກະທຳຂອງຜູ້ຖືກຫາ;

5. ອົງການ ຫຼື ເຈົ້າໜ້າທີ່ ທີ່ກ່ຽວຂ້ອງ ສາມາດຂໍຂໍ້ມູນເພີ່ມເຕີມຈາກປະເທດທີ່ຮ້ອງຂໍການ ຊ່ວຍເຫຼືອ ທາງກົດໝາຍ.

**ມາດຕາ 51 ການຮັກສາຄວາມລັບ**

ອົງການທີ່ມີສິດກ່ຽວຂ້ອງຂອງ ສປປ ລາວ ຕ້ອງຮັກສາຄວາມລັບ ຂອງປະເທດທີ່ຮ້ອງຂໍການຊ່ວຍເຫຼືອ ທາງກົດໝາຍ.

**ມາດຕາ 52 ການປະຕິເສດການຮ້ອງຂໍ**

ອົງການທີ່ມີສິດກ່ຽວຂ້ອງຂອງ ສປປ ລາວ ອາດປະຕິເສດການຮ້ອງຂໍໃນການຊ່ວຍເຫຼືອຊຶ່ງກັນ ແລະ ກັນ ທາງກົດໝາຍ ຖ້າການຮ້ອງຂໍນັ້ນຫາກຂັດກັບຫຼັກການພື້ນຖານ ໃນການຮ່ວມມືສາກົນຕາມທີ່ໄດ້ກຳນົດໄວ້ ໃນມາດຕາ 41 ຂອງກົດໝາຍສະບັບນີ້ ແລະ ກົດໝາຍອື່ນທີ່ກ່ຽວຂ້ອງຂອງ ສປປ ລາວ.

## ພາກທີ VI
## ຂໍ້ຫ້າມ

**ມາດຕາ 53 ຂໍ້ຫ້າມທົ່ວໄປ**

ຫ້າມ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ມີ ພຶດຕິກຳ ດັ່ງນີ້:

1. ມີພຶດຕິກຳຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນມາດຕາ 8 ຂອງກົດໝາຍສະບັບນີ້;
2. ໂຄສະນາທຳລາຍລະບອບການເມືອງ ເພື່ອສ້າງຄວາມປັ່ນປ່ວນໃນສັງຄົມ;
3. ທຳລາຍ ຫຼື ສ້າງຄວາມເສຍຫາຍໃຫ້ແກ່ອຸປະກອນເອເລັກໂຕຣນິກ, ຄອມພິວເຕີ ແລະ ສິ່ງອຳນວຍ ຄວາມສະດວກຕ່າງໆ ໃນການແລກປ່ຽນຂໍ້ມູນຂ່າວສານຜ່ານໄຊເບີ;
4. ສົມຮູ້ຮ່ວມຄິດກັບບຸກຄົນໃດໜຶ່ງ ເພື່ອເຜີຍແຜ່ສິ່ງລາມົກ ໂດຍຜ່ານສື່ສັງຄົມອອນລາຍ;
5. ທວງເອົາ, ຂໍເອົາ, ໃຫ້ ແລະ ຮັບສິນບົນ;
6. ມີພຶດຕິກຳອື່ນ ທີ່ເປັນການລະເມີດກົດໝາຍ ແລະ ລະບຽບການ.

**ມາດຕາ 54 ຂໍ້ຫ້າມສຳລັບຜູ້ໃຫ້ບໍລິການ**

ຫ້າມຜູ້ໃຫ້ບໍລິການ ມີ ພຶດຕິກຳ ດັ່ງນີ້:

1. ລຶບຂໍ້ມູນທີ່ຈະລາຈອນທາງລະບົບຄອມພິວເຕີ ກ່ອນ ເກົ້າສິບວັນ ໃນກໍລະນີເຊື່ອມຕໍ່ ແລະ ກ່ອນ ສາມຮ້ອຍຫົກສິບຫ້າວັນ ໃນກໍລະນີບໍ່ເຊື່ອມຕໍ່;
2. ລຶບຂໍ້ມູນຜູ້ຊົມໃຊ້ລະບົບຄອມພິວເຕີ ທີ່ສ້າງຄວາມເສຍຫາຍກ່ອນ ເກົ້າສິບວັນ;
3. ສະໜອງຂໍ້ມູນທີ່ບໍ່ຖືກຕ້ອງ ໃຫ້ເຈົ້າໜ້າທີ່ ແລະ ພະນັກງານທີ່ກ່ຽວຂ້ອງ;
4. ເປີດເຜີຍຂໍ້ມູນຂອງຜູ້ໃຊ້ບໍລິການ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
5. ສ້າງເງື່ອນໄຂ ຫຼື ອຳນວຍຄວາມສະດວກໃຫ້ແກ່ການເຄື່ອນໄຫວກໍ່ອາຊະຍາກຳໄຊເບີ;
6. ມີພຶດຕິກຳອື່ນ ທີ່ເປັນການລະເມີດກົດໝາຍ ແລະ ລະບຽບການ.

**ມາດຕາ 55 ຂໍ້ຫ້າມສຳລັບເຈົ້າໜ້າທີ່ ແລະ ພະນັກງານທີ່ກ່ຽວຂ້ອງ**

ຫ້າມເຈົ້າໜ້າທີ່ ແລະ ພະນັກງານທີ່ກ່ຽວຂ້ອງ ມີ ພຶດຕິກຳ ດັ່ງນີ້:

1. ເປີດເຜີຍຄວາມລັບຂອງ ລັດ, ທາງລັດຖະການ, ຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ຜ່ານໄຊເບີ;

2. ເປີດເຜີຍລະຫັດເຂົ້າເຖິງລະບົບຄອມພິວເຕີ ແລະ ມາດຕະການປ້ອງກັນສະເພາະຂອງ ຂະແໜງການຕົນ;

3. ສົ່ງມອບ ຂໍ້ມູນ, ຂໍ້ມູນຈະລາຈອນໄຊເບີ ຫຼື ຂໍ້ມູນຂອງຜູ້ໃຊ້ບໍລິການໃຫ້ແກ່ບຸກຄົນອື່ນ ຍົກເວັ້ນ ການສົ່ງມອບ ເພື່ອປະໂຫຍດໃນການດຳເນີນຄະດີ ເຊັ່ນ ການປະຕິບັດຄຳສັ່ງ ຫຼື ກໍລະນີໄດ້ຮັບອະນຸຍາດ ຈາກອົງການດຳເນີນຄະດີ;

4. ກີດໜ່ວງ, ຖ່ວງດຶງ ແລະ ປອມແປງເອກະສານ ກ່ຽວກັບຂໍ້ມູນທີ່ເປັນການກະທຳຜິດໄຊເບີ;

5. ສວຍໃຊ້ໜ້າທີ່ຕຳແໜ່ງ ເພື່ອຜົນປະໂຫຍດ ສ່ວນຕົວ, ຄອບຄົວ ແລະ ພັກພວກ;

6. ປະລະໜ້າທີ່ຄວາມຮັບຜິດຊອບທີ່ການຈັດຕັ້ງມອບໝາຍໃຫ້;

7. ມີພຶດຕິກຳອື່ນ ທີ່ເປັນການລະເມີດກົດໝາຍ ແລະ ລະບຽບການ.

# ພາກທີ VII
# ການຄຸ້ມຄອງ ແລະ ການກວດກາ ວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ

## ໝວດທີ 1
## ການຄຸ້ມຄອງ ວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ

**ມາດຕາ 56 (ປັບປຸງ) ອົງການຄຸ້ມຄອງ ວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ**

ລັດຖະບານ ຄຸ້ມຄອງວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີຢ່າງລວມສູນ ແລະ ເປັນເອກະພາບໃນຂອບເຂດທົ່ວປະເທດ ໂດຍມອບໃຫ້ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນຜູ້ຮັບຜິດຊອບໂດຍກົງ ແລະ ເປັນເຈົ້າການປະສານສົມທົບກັບ ກະຊວງ ປ້ອງກັນປະເທດ, ກະຊວງປ້ອງກັນຄວາມສະຫງົບ, ທະນາຄານແຫ່ງ ສປປ ລາວ, ຜູ້ໃຫ້ບໍລິການ ໂທລະຄົມມະນາຄົມ ແລະ ອິນເຕີເນັດ, ກະຊວງ, ອົງການ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນທີ່ກ່ຽວຂ້ອງ.

ອົງການຄຸ້ມຄອງວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ປະກອບດ້ວຍ:

1. ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ;

2. ພະແນກເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ນະຄອນຫຼວງ, ແຂວງ;

3. ຫ້ອງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເມືອງ, ນະຄອນ.

**ມາດຕາ 57 ສິດ ແລະ ໜ້າທີ່ ຂອງ ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ**

ໃນການຄຸ້ມຄອງວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ມີ ສິດ ແລະ ໜ້າທີ່ ດັ່ງນີ້:

1. ຄົ້ນຄວ້າ, ສ້າງແຜນຍຸດທະສາດ, ນະໂຍບາຍ, ກົດໝາຍ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ເພື່ອສະເໜີລັດຖະບານພິຈາລະນາ;

2. ໂຄສະນາ, ເຜີຍແຜ່ກົດໝາຍ ແລະ ລະບຽບການ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ໃນຂອບເຂດທົ່ວປະເທດ;

3. ຊີ້ນຳການສ້າງ, ຝຶກອົບຮົມ, ຍົກລະດັບ ແລະ ພັດທະນາບຸກຄະລາກອນ ກ່ຽວກັບຄວາມປອດໄພໄຊເບີ;

4. ຊີ້ນຳການເຝົ້າລະວັງ, ຕິດຕາມ, ກວດກາ, ແນະນຳ, ແຈ້ງເຕືອນ ແລະ ຕອບໂຕ້ເຫດສຸກ ເສີນທາງ ລະບົບຄອມພິວເຕີ;

5. ປະສານສົມທົບກັບກະຊວງ, ອົງການອື່ນທີ່ກ່ຽວຂ້ອງ ໃນການເຄື່ອນໄຫວຕ້ານ ແລະ ສະກັດກັ້ນອາ ຊະຍາກຳໄຊເບີ ;

6. ພົວພັນ, ຮ່ວມມືກັບຕ່າງປະເທດ, ພາກພື້ນ ແລະ ສາກົນ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາ ຊະຍາກຳໄຊເບີ ;

7. ສະຫຼຸບ ແລະ ລາຍງານການເຄື່ອນໄຫວວຽກງານຂອງຕົນ ຕໍ່ລັດຖະບານຢ່າງເປັນປົກກະຕິ;

8. ນຳໃຊ້ສິດ ແລະ ປະຕິບັດໜ້າທີ່ອື່ນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ ແລະ ລະບຽບການ.

**ມາດຕາ 58 ສິດ ແລະ ໜ້າທີ່ ຂອງພະແນກເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ນະຄອນຫຼວງ, ແຂວງ**

ໃນການຄຸ້ມຄອງວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ພະແນກ ເຕັກໂນໂລຊີ ແລະ ການ ສື່ສານ ນະຄອນຫຼວງ, ແຂວງ ມີ ສິດ ແລະ ໜ້າທີ່ ຕາມຂອບເຂດ ຄວາມຮັບຜິດຊອບຂອງຕົນ ດັ່ງນີ້:

1. ໂຄສະນາ ເຜີຍແຜ່ ແຜນຍຸດທະສາດ, ນະໂຍບາຍ, ກົດໝາຍ, ລະບຽບການ ກ່ຽວກັບ ວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳ ໄຊເບີ ແລ້ວຈັດຕັ້ງປະຕິບັດ;

2. ຂຶ້ນແຜນ ສ້າງ, ຝຶກອົບຮົມ, ຍົກລະດັບ ແລະ ພັດທະນາ ບຸກຄະລາກອນ ກ່ຽວກັບວຽກ ງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳ ໄຊເບີ ແລ້ວສະເໜີຕໍ່ຂັ້ນເທິງ;

3. ຮັບແຈ້ງເຫດສຸກເສີນ ທາງລະບົບຄອມພິວເຕີ ແລ້ວລາຍງານ ຕໍ່ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກ ເສີນທາງຄອມພິວເຕີ;

4. ແຈ້ງຄວາມ, ລາຍງານການກະທຳຜິດທາງລະບົບຄອມພິວເຕີ ຕໍ່ອົງການສືບສວນ- ສອບສວນ ແລະ ອົງການໄອຍະການປະຊາຊົນ ແຂວງ, ນະຄອນ;

5. ປະສານສົມທົບ ແລະ ໃຫ້ການຮ່ວມມືກັບອົງການສືບສວນ-ສອບສວນ ແລະ ອົງການໄອຍະການ ປະຊາຊົນ ແຂວງ, ນະຄອນ ໃນການດຳເນີນຄະດີໄຊເບີ;

6. ແຈ້ງໃຫ້ຜູ້ໃຫ້ບໍລິການ, ຜູ້ຮັກສາຂໍ້ມູນ ອຳນວຍຄວາມສະດວກ ແລະ ສະໜອງຂໍ້ມູນ ກ່ຽວກັບການ ກະທຳຜິດໄຊເບີ;

7. ປະສານສົມທົບກັບພະແນກການອື່ນທີ່ກ່ຽວຂ້ອງ ໃນການເຄື່ອນໄຫວຕ້ານ ແລະ ສະກັດກັ້ນອາຊະ ຍາກຳໄຊເບີ;

8. ປະສານງານ, ຮ່ວມມືກັບ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີຂອງ ກະຊວງ ເຕັກໂນໂລຊີ ແລະ ການສື່ສານ;

9. ເກັບກຳສະຖິຕິ ກ່ຽວກັບອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ;

10. ປະສານງານ, ພົວພັນ, ຮ່ວມມືກັບຕ່າງປະເທດ, ພາກພື້ນ ແລະ ສາກົນ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ຕາມການມອບໝາຍ;

11. ສະຫຼຸບ ແລະ ລາຍງານການເຄື່ອນໄຫວວຽກງານຂອງຕົນ ຕໍ່ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ແລະ ອົງການປົກຄອງແຂວງ, ນະຄອນ ຢ່າງເປັນປົກກະຕິ;

12. ນຳໃຊ້ສິດ ແລະ ປະຕິບັດໜ້າທີ່ອື່ນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ ແລະ ລະບຽບການ.

**ມາດຕາ 59 ສິດ ແລະ ໜ້າທີ່ ຂອງ ຫ້ອງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເມືອງ, ນະຄອນ**

ໃນການຄຸ້ມຄອງວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ຫ້ອງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເມືອງ, ນະຄອນ ມີ ສິດ ແລະ ໜ້າທີ່ ຕາມຂອບ ເຂດຄວາມຮັບຜິດຊອບຂອງຕົນ ດັ່ງນີ້:

1. ເຜີຍແຜ່ ແຜນຍຸດທະສາດ, ນະໂຍບາຍ, ກົດໝາຍ, ລະບຽບການ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ແລ້ວຈັດຕັ້ງປະຕິບັດ;

2. ຂຶ້ນແຜນ ສ້າງ, ຝຶກອົບຮົມ, ຍົກລະດັບ ແລະ ພັດທະນາ ບຸກຄະລາກອນ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ແລ້ວສະເໜີຕໍ່ຂັ້ນເທິງຖັດຕົນ;

3. ຮັບແຈ້ງເຫດສຸກເສີນ ທາງລະບົບຄອມພິວເຕີ ແລ້ວລາຍງານ ຕໍ່ພະແນກ ເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ນະຄອນຫຼວງ, ແຂວງ ເພື່ອນຳສະເໜີ ຕໍ່ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂ ເຫດສຸກເສີນທາງຄອມພິວເຕີ;

4. ແຈ້ງຄວາມ, ລາຍງານການກະທຳຜິດທາງລະບົບຄອມພິວເຕີ ຕໍ່ອົງການສືບສວນ-ສອບສວນ ຫຼື ອົງການໄອຍະການປະຊາຊົນເຂດ;

5. ປະສານສົມທົບ ແລະ ໃຫ້ການຮ່ວມມືກັບອົງການສືບສວນ-ສອບສວນ ຫຼື ອົງການໄອຍະການ ປະຊາຊົນເຂດໃນການດຳເນີນຄະດີທາງລະບົບຄອມພິວເຕີ;

6. ປະສານສົມທົບກັບຫ້ອງການອື່ນທີ່ກ່ຽວຂ້ອງ ໃນການເຄື່ອນໄຫວຕ້ານ ແລະ ສະກັດກັ້ນ ອາຊະຍາ ກຳທາງລະບົບຄອມພິວເຕີ;

7. ເກັບກຳສະຖິຕິ ກ່ຽວກັບອາຊະຍາກຳອາຊະຍາກຳໄຊເບີ;

8. ສະຫຼຸບ ແລະ ລາຍງານການເຄື່ອນໄຫວວຽກງານຂອງຕົນ ຕໍ່ພະແນກ ເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ນະຄອນຫຼວງ, ແຂວງ ແລະ ອົງການປົກຄອງເມືອງ, ເທດສະບານ ຢ່າງເປັນປົກກະຕິ;

9. ນຳໃຊ້ສິດ ແລະ ປະຕິບັດໜ້າທີ່ອື່ນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ ແລະ ລະບຽບການ.

**ມາດຕາ 60 (ປັບປຸງ) ສິດ ແລະ ໜ້າທີ່ຂອງ ກະຊວງ, ອົງການ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ທີ່ກ່ຽວຂ້ອງ**

ກະຊວງ, ອົງການ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ທີ່ກ່ຽວຂ້ອງ ມີ ສິດ ແລະ ໜ້າທີ່ ໃນການຄຸ້ມຄອງ, ຕິດຕາມ, ຮ່ວມມື ແລະ ປະສານສົມທົບກັບ ຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ, ຂະແໜງການປ້ອງກັນຊາດ-ປ້ອງກັນຄວາມສະຫງົບ ຂັ້ນຂອງຕົນ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນ ອາຊະຍາກຳໄຊເບີ ຕາມພາລະບົດບາດ ແລະ ຂອບເຂດຄວາມຮັບຜິດຊອບຂອງຕົນ.

## ໝວດທີ 2
## ການກວດກາ ວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ

**ມາດຕາ 61 (ປັບປຸງ) ອົງການກວດກາ ວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກາໄຊເບີ**

ອົງການກວດກາວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ປະກອບດ້ວຍ:

1. ອົງການກວດກາພາຍໃນ ຊຶ່ງແມ່ນ ອົງການດຽວກັນກັບ ອົງການຄຸ້ມຄອງວຽກງານຕ້ານ ແລະ ສະກັດ ກັ້ນອາຊະຍາກຳໄຊເບີ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນມາດຕາ 57 ຂອງກົດໝາຍ ສະບັບນີ້;

2. ອົງການກວດກາພາຍນອກ ຊຶ່ງແມ່ນ ສະພາແຫ່ງຊາດ, ສະພາປະຊາຊົນຂັ້ນແຂວງ, ອົງການກວດກາ ລັດແຕ່ລະຂັ້ນ, ອົງການກວດສອບແຫ່ງລັດ, ແນວລາວສ້າງຊາດ, ສະຫະພັນນັກຮົບເກົ່າລາວ, ອົງການຈັດຕັ້ງ ມະຫາຊົນ ແລະ ສື່ມວນຊົນ.

**ມາດຕາ 62 ເນື້ອໃນການກວດກາ**

ເນື້ອໃນການກວດກາວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ມີດັ່ງນີ້:

1. ການປະຕິບັດ ແຜນຍຸດທະສາດ, ນະໂຍບາຍ, ກົດໝາຍ ແລະ ລະບຽບການ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ;

2. ການຈັດຕັ້ງ ແລະ ການເຄື່ອນໄຫວວຽກງານຂອງອົງການຄຸ້ມຄອງວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ;

3. ການປະຕິບັດສັນຍາສາກົນ ແລະ ສົນທິສັນຍາ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳໄຊເບີ ທີ່ ສປປ ລາວ ເປັນພາຄີ.

**ມາດຕາ 63 ຮູບການການກວດກາ**

ການກວດກາວຽກງານຄວາມປອດໄພໄຊເບີ ດຳເນີນດ້ວຍ ສາມຮູບການ ດັ່ງນີ້:

1. ການກວດກາຕາມແຜນປົກກະຕິ ຊຶ່ງແມ່ນ ການກວດກາທີ່ດຳເນີນຕາມແຜນການ ຢ່າງເປັນປະຈຳ ແລະ ມີກຳນົດເວລາອັນແນ່ນອນ;

2. ການກວດກາໂດຍມີການແຈ້ງໃຫ້ຮູ້ລ່ວງໜ້າ ຊຶ່ງແມ່ນ ການກວດການອກແຜນການ ເມື່ອເຫັນວ່າມີຄວາມຈຳເປັນ ຈຶ່ງຕ້ອງແຈ້ງໃຫ້ຜູ້ຖືກກວດກາຮູ້ກ່ອນລ່ວງໜ້າ;

3. ການກວດກາແບບກະທັນຫັນ ຊຶ່ງແມ່ນ ການກວດກາແບບຮີບດ່ວນ ໂດຍບໍ່ໄດ້ແຈ້ງໃຫ້ຜູ້ຖືກກວດກາ ຮູ້ກ່ອນລ່ວງໜ້າ.

ໃນການກວດກາວຽກງານຄວາມປອດໄພໄຊເບີ ຕ້ອງປະຕິບັດຕາມກົດໝາຍ ຢ່າງເຂັ້ມງວດ.

## ພາກທີ VIII
## ນະໂຍບາຍຕໍ່ຜູ້ມີຜົນງານ ແລະ ມາດຕະການຕໍ່ລະເມີດ

**ມາດຕາ 64 ນະໂຍບາຍຕໍ່ຜູ້ມີຜົນງານ**

ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ທີ່ມີຜົນງານດີເດັ່ນໃນການຈັດຕັ້ງປະຕິບັດກົດໝາຍສະບັບນີ້ ເປັນຕົ້ນ ການລາຍງານ, ການໃຫ້ຄວາມຮ່ວມມື, ການສະໜອງຂໍ້ມູນ ກ່ຽວກັບພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳໄຊເບີ ຈະໄດ້ຮັບການຍ້ອງຍໍ ແລະ ນະໂຍບາຍອື່ນ ຕາມລະບຽບການ.

**ມາດຕາ 65 ມາດຕະການຕໍ່ຜູ້ລະເມີດ**

ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ທີ່ລະເມີດກົດໝາຍສະບັບນີ້ ຈະຖືກ ສຶກສາອົບຮົມ, ກ່າວເຕືອນ, ລົງວິໄນ, ປັບໃໝ, ໃຊ້ແທນຄ່າເສຍຫາຍທາງແພ່ງທີ່ຕົນໄດ້ກໍ່ຂຶ້ນ ຫຼື ຖືກລົງໂທດທາງອາຍາ ຕາມກົດໝາຍ.

**ມາດຕາ 66 ມາດຕະການສຶກສາອົບຮົມ**

ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ທີ່ລະເມີດກົດໝາຍສະບັບນີ້ ຊຶ່ງເປັນການລະເມີດຄັ້ງທຳອິດ ແລະ ກໍ່ຄວາມເສຍຫາຍບໍ່ຫຼວງຫຼາຍ ຈະຖືກສຶກສາອົບຮົມ ແລະ ກ່າວເຕືອນ.

**ມາດຕາ 67 ມາດຕະການທາງວິໄນ**

ເຈົ້າໜ້າທີ່ ແລະ ພະນັກງານທີ່ກ່ຽວຂ້ອງ ທີ່ລະເມີດກົດໝາຍສະບັບນີ້ ຊຶ່ງບໍ່ເປັນການກະທຳຜິດ ທາງອາຍາ ຈະຖືກລົງວິໄນຕາມແຕ່ລະກໍລະນີ ດັ່ງນີ້:

1. ຕິຕຽນ, ກ່າວເຕືອນ ຄວາມຜິດຕາມລະບຽບການ ພ້ອມທັງບັນທຶກໄວ້ໃນປະຫວັດຂອງຜູ້ກ່ຽວ;

2. ໂຈະການເລື່ອນຊັ້ນ, ຂັ້ນເງິນເດືອນ ແລະ ການຍ້ອງຍໍ;

3. ປົດຕຳແໜ່ງ ຫຼື ຍົກຍ້າຍໄປຮັບໜ້າທີ່ອື່ນທີ່ມີຕຳແໜ່ງຕ່ຳກວ່າ;

4. ໃຫ້ອອກຈາກລັດຖະການ ໂດຍບໍ່ໄດ້ຮັບນະໂຍບາຍໃດໆ.

5. ຜູ້ຖືກລົງວິໄນ ຕ້ອງສົ່ງຄືນຊັບສິນທີ່ຕົນໄດ້ມາຈາກການປະຕິບັດໜ້າທີ່ຂອງຕົນທີ່ບໍ່ຖືກຕ້ອງນັ້ນ ໃຫ້ການຈັດຕັ້ງຢ່າງຄົບຖ້ວນ.

**ມາດຕາ 68 ມາດຕະການປັບໃໝ**

ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ທີ່ລະເມີດກົດໝາຍສະບັບນີ້ ຈະຖືກປັບໃໝ ໃນກໍລະນີ ດັ່ງນີ້:

1. ສະໜອງຂໍ້ມູນທີ່ບໍ່ຖືກຕ້ອງ ໃຫ້ເຈົ້າໜ້າທີ່ ແລະ ພະນັກງານທີ່ກ່ຽວຂ້ອງ ຊຶ່ງບໍ່ສ້າງຄວາມເສຍຫາຍໃຫ້ແກ່ຜູ້ໃດໜຶ່ງ;

2. ບໍ່ສະໜອງຂໍ້ມູນຕາມກຳນົດເວລາທີ່ເຈົ້າໜ້າທີ່ ຫຼື ພະນັກງານທີ່ກ່ຽວຂ້ອງແຈ້ງໃຫ້;

3. ລຶບຂໍ້ມູນໃນລະບົບຄອມພິວເຕີ ຫຼື ຂໍ້ມູນຄອມພິວເຕີຂອງຜູ້ອື່ນທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດຈາກຜູ້ກ່ຽວ;

4. ກໍລະນີອື່ນ ທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ ແລະ ລະບຽບການກ່ຽວກັບການລະເມີດທາງບໍລິຫານ.

ອັດຕາປັບໃໝ ແຕ່ລະກໍລະນີ ໄດ້ກຳນົດໄວ້ໃນລະບຽບການຕ່າງຫາກ.

**ມາດຕາ 69 ມາດຕະການທາງແພ່ງ**

ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ທີ່ລະເມີດກົດໝາຍສະບັບນີ້ ຊຶ່ງໄດ້ກໍ່ຄວາມເສຍຫາຍແກ່ ຜູ້ອື່ນ ຕ້ອງໃຊ້ແທນຄ່າເສຍຫາຍທີ່ຕົນໄດ້ກໍ່ຂຶ້ນ.

**ມາດຕາ 70 (ປັບປຸງ) ມາດຕະການທາງອາຍາ**

ບຸກຄົນທີ່ໄດ້ກະທຳຜິດໃນສະຖານ ຕໍ່ລົງໄປນີ້ ຈະຖືກລົງໂທດ ດັ່ງນີ້:

1. ການເປີດເຜີຍມາດຕະການປ້ອງກັນການເຂົ້າເຖິງໄຊເບີ: ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 3 ເດືອນ ຫາ 1 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 10,000,000 ກີບ ຫາ 30,000,000 ກີບ.

2. ການເຂົ້າເຖິງໄຊເບີໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ: ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 6 ເດືອນ ຫາ 2 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 20,000,000 ກີບ ຫາ 50,000,000 ກີບ.

3. ການດັດຕໍ່ເນື້ອໃນ, ຮູບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວີດີໂອ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ (ລວມເຖິງ Deepfake): ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 1 ປີ ຫາ 3 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 30,000,000 ກີບ ຫາ 100,000,000 ກີບ.

4. ການລັດເອົາຂໍ້ມູນໃນໄຊເບີ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ: ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 1 ປີ ຫາ 5 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 50,000,000 ກີບ ຫາ 200,000,000 ກີບ.

5. ການສ້າງຄວາມເສຍຫາຍຜ່ານສື່ສັງຄົມອອນລາຍ: ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 1 ປີ ຫາ 5 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 50,000,000 ກີບ ຫາ 200,000,000 ກີບ.

6. ການເຜີຍແຜ່ສິ່ງລາມົກຜ່ານລະບົບໄຊເບີ: ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 2 ປີ ຫາ 7 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 50,000,000 ກີບ ຫາ 300,000,000 ກີບ.

7. ການລົບກວນລະບົບໄຊເບີ: ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 2 ປີ ຫາ 7 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 50,000,000 ກີບ ຫາ 300,000,000 ກີບ.

8. ການປອມແປງຂໍ້ມູນໄຊເບີ: ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 2 ປີ ຫາ 7 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 50,000,000 ກີບ ຫາ 300,000,000 ກີບ.

9. ການທຳລາຍຂໍ້ມູນຄອມພິວເຕີ: ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 3 ປີ ຫາ 10 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 100,000,000 ກີບ ຫາ 500,000,000 ກີບ.

10. ການດຳເນີນກິດຈະການ ກ່ຽວກັບເຄື່ອງມືອາຊະຍາກຳທາງລະບົບໄຊເບີ: ຈະຖືກລົງໂທດຕັດອິດສະລະພາບແຕ່ 5 ປີ ຫາ 10 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 150,000,000 ກີບ ຫາ 500,000,000 ກີບ (ພ້ອມທັງຍຶດເຄື່ອງມືທີ່ໃຊ້ໃນການກະທຳຜິດ).

11. ການຫຼອກລວງຜ່ານໄຊເບີ ຈະຖືກຕັດອິດສະລະພາບແຕ່ 3 ຫາ 7 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 10,000,000 ກີບ ຫາ 50,000,000 ກີບ;

12. ການນຳໃຊ້ປັນຍາປະດິດ (AI) ໃນທາງທີ່ຜິດຈະຖືກຕັດອິດສະລະພາບແຕ່ 5 ປີ ຫາ 10 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 50,000,000 ກີບ ຫາ 100,000,000 ກີບ;

13. ການສ້າງຄວາມເສຍຫາຍ ຕໍ່ແມ່ຍິງ ແລະ ເດັກ ຜ່ານໄຊເບີ ຈະຖືກຕັດອິດສະລະພາບແຕ່ 3 ປີ ຫາ 5 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 10,000,000 ກີບ ຫາ 30,000,000 ກີບ;

14. ການຟອກເງິນທີ່ໄດ້ຈາກອາຊະຍາກຳໄຊເບີ ຈະຖືກຕັດອິດສະລະພາບແຕ່ 3 ປີ ຫາ 7 ປີ ແລະ ຈະຖືກປັບໃໝແຕ່ 300,000,000 ກີບ ຫາ 500,000,000 ກີບ;

(ຂໍຄຳເຫັນຈາກພາກສ່ວນທີ່ກ່ຽວຂ້ອງຄືນ)

## ພາກທີ IX
## ບົດບັນຍັດສຸດທ້າຍ

**ມາດຕາ 71 ການຈັດຕັ້ງປະຕິບັດ**

ລັດຖະບານ ແຫ່ງ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ ເປັນຜູ້ຈັດຕັ້ງປະຕິບັດກົດໝາຍສະບັບນີ້.

**ມາດຕາ 72 ຜົນສັກສິດ**

ກົດໝາຍສະບັບນີ້ ມີຜົນສັກສິດ ນັບແຕ່ວັນທີ ..... ພາຍຫຼັງປະທານປະເທດ ແຫ່ງ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ ອອກລັດຖະດຳລັດປະກາດໃຊ້ ແລະ ໄດ້ລົງຈົດໝາຍເຫດທາງລັດຖະການເປັນຕົ້ນໄປ.

**ປະທານສະພາແຫ່ງຊາດ**