ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ
ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ

ປະທານປະເທດ ເລກທີ 144 /ປປທ

ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ 06 ສິງຫາ 2025

ລັດຖະດຳລັດ

ກ່ຽວກັບການປະກາດໃຊ້ກົດໝາຍວ່າດ້ວຍຄວາມປອດໄພໄຊເບີ

- ອີງຕາມ ມາດຕາ 68 ຂໍ້ 1 ຂອງລັດຖະທຳມະນຸນ ແຫ່ງ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນ ລາວ ສະບັບເລກທີ 77/ສພຊ, ລົງວັນທີ 20 ເດືອນມີນາ ປີ 2025;
- ອີງຕາມ ມະຕິກອງປະຊຸມສະພາແຫ່ງຊາດ ກ່ຽວກັບການຮັບຮອງເອົາກົດໝາຍວ່າດ້ວຍຄວາມປອດໄພ ໄຊເບີ ສະບັບເລກທີ 163/ສພຊ, ລົງວັນທີ 25 ມິຖຸນາ 2025;
- ອີງຕາມ ໜັງສືສະເໜີຂອງຄະນະປະຈຳສະພາແຫ່ງຊາດ ສະບັບເລກທີ 41/ຄປຈ, ລົງວັນທີ 23 ກໍລະກົດ 2025.

ປະທານປະເທດ

ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ ອອກລັດຖະດຳລັດ:

ມາດຕາ 1 ປະກາດໃຊ້ກົດໝາຍວ່າດ້ວຍຄວາມປອດໄພໄຊເບີ.

ມາດຕາ 2 ລັດຖະດຳລັດສະບັບນີ້ ມີຜົນສັກສິດ ນັບແຕ່ວັນລົງລາຍເຊັນ ເປັນຕົ້ນໄປ.

ປະທານປະເທດ ແຫ່ງ ສປປ ລາວ

ທອງລຸນ ສີສຸລິດ

ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ

ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ

ສະພາແຫ່ງຊາດ

ເລກທີ 163 / ສພຊ

ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ 25 / 06 / 25

ມະຕິ
ຂອງກອງປະຊຸມສະພາແຫ່ງຊາດ
ກ່ຽວກັບການຮັບຮອງເອົາກົດໝາຍວ່າດ້ວຍຄວາມປອດໄພໄຊເບີ

- ອີງຕາມລັດຖະທຳມະນູນ ແຫ່ງ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ ສະບັບເລກທີ 77 /ສພຊ, ລົງວັນທີ 20 ເດືອນມີນາ ປີ 2025 ມາດຕາ 54 ຂໍ້ 1;
- ອີງຕາມກົດໝາຍວ່າດ້ວຍສະພາແຫ່ງຊາດ ສະບັບເລກທີ 56 /ສພຊ, ລົງວັນທີ 28 ມິຖຸນາ 2024 ມາດຕາ 11 ຂໍ້ 1.

ພາຍຫຼັງກອງປະຊຸມສະໄໝສາມັນ ເທື່ອທີ 9 ຂອງສະພາແຫ່ງຊາດ ຊຸດທີ IX ໄດ້ຄົ້ນຄວ້າພິຈາລະນາຢ່າງກວ້າງຂວາງ ແລະ ເລິກເຊິ່ງ ກ່ຽວກັບເນື້ອໃນຂອງກົດໝາຍວ່າດ້ວຍຄວາມປອດໄພໄຊເບີ ໃນວາລະຂອງກອງປະຊຸມຄັ້ງວັນທີ 23 ມິຖຸນາ 2025 ແລະ ຖືກພິຈາລະນາຮັບຮອງເອົາໃນວາລະຕອນບ່າຍ ຂອງວັນທີ 25 ມິຖຸນາ 2025.

ກອງປະຊຸມສະພາແຫ່ງຊາດ ຕົກລົງ:

ມາດຕາ 1 ຮັບຮອງເອົາກົດໝາຍວ່າດ້ວຍຄວາມປອດໄພໄຊເບີ ດ້ວຍຄະແນນສຽງຫຼາຍກວ່າເຄິ່ງໜຶ່ງ ຂອງຈຳນວນສະມາຊິກສະພາແຫ່ງຊາດ ທີ່ເຂົ້າຮ່ວມກອງປະຊຸມ.

ມາດຕາ 2 ມະຕິສະບັບນີ້ ມີຜົນສັກສິດນັບແຕ່ວັນລົງລາຍເຊັນ ເປັນຕົ້ນໄປ.

ປະທານສະພາແຫ່ງຊາດ

ປອ ໄຊສົມພອນ ພົມວິຫານ

ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ
ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ

ສະພາແຫ່ງຊາດ

ເລກທີ 87 /ສພຊ
ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ 25 ມິຖຸນາ 2025

ກົດໝາຍ
ວ່າດ້ວຍຄວາມປອດໄພໄຊເບີ

ພາກທີ I
ບົດບັນຍັດທົ່ວໄປ

ມາດຕາ 1 ຈຸດປະສົງ

ກົດໝາຍສະບັບນີ້ ກຳນົດ ຫຼັກການ, ລະບຽບການ ແລະ ມາດຕະການ ກ່ຽວກັບການຄຸ້ມຄອງ ແລະ ການຕິດຕາມ ກວດກາ ວຽກງານຄວາມປອດໄພໄຊເບີ ເພື່ອເຮັດໃຫ້ວຽກງານດັ່ງກ່າວ ມີປະສິດທິພາບ ແລະ ປະສິດທິຜົນ ແນໃສ່ປ້ອງກັນ ຄວາມໝັ້ນຄົງຂອງຊາດ, ຄວາມສະຫງົບ, ຄວາມເປັນລະບຽບຮຽບຮ້ອຍຂອງສັງຄົມ, ຄວາມປອດໄພທາງດ້ານ ຂໍ້ມູນ ຂ່າວສານ, ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ, ປົກປ້ອງ ສິດ ແລະ ຜົນປະໂຫຍດຂອງລັດ, ການຈັດຕັ້ງ ແລະ ບຸກຄົນ, ສາມາດເຊື່ອມໂຍງກັບພາກພື້ນ ແລະ ສາກົນ ປະກອບສ່ວນ ເຂົ້າໃນການປົກປັກຮັກສາ ແລະ ສ້າງສາປະເທດຊາດ.

ມາດຕາ 2 ຄວາມປອດໄພໄຊເບີ

ຄວາມປອດໄພໄຊເບີ ແມ່ນ ການປ້ອງກັນ ລະບົບເຕັກໂນໂລຊີການສື່ສານ ຂໍ້ມູນ ຂ່າວສານ ຈາກການໂຈມຕີທາງໄຊເບີ ຫຼື ຄວາມເສຍຫາຍຈາກໄພຄຸກຄາມທາງໄຊເບີ ລວມທັງການຮັກສາຄວາມຖືກຕ້ອງຂອງ ລະບົບ, ເຄືອຂ່າຍ ແລະ ການຮັບປະກັນຄວາມພ້ອມໃນການໃຊ້ງານຂອງລະບົບດັ່ງກ່າວ.

ມາດຕາ 3 ການອະທິບາຍຄຳສັບ

ຄຳສັບທີ່ນຳໃຊ້ໃນກົດໝາຍສະບັບນີ້ ມີຄວາມໝາຍ ດັ່ງນີ້:

1. ໄຊເບີ (Cyber) ໝາຍເຖິງ ລະບົບເຕັກໂນໂລຊີການສື່ສານ ຂໍ້ມູນ ຂ່າວສານ ຊຶ່ງປະກອບດ້ວຍ ເຄືອຂ່າຍຄອມພິວເຕີ, ໂຄງລ່າງພື້ນຖານດ້ານເຕັກໂນໂລຊີ ຂໍ້ມູນ ຂ່າວສານ, ລະບົບຄວບຄຸມ, ອຸປະກອນເຊື່ອມຕໍ່ ແລະ ກິດຈະກຳທາງອອນລາຍທັງໝົດ;

2. ໜ່ວຍງານໂຄງລ່າງພື້ນຖານຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ (Critical Information Infrastracture - CII) ໝາຍເຖິງ ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ ຫຼື ອົງການທີ່ເປັນເຈົ້າຂອງ, ດຳເນີນການ ຫຼື ບໍລິຫານລະບົບທີ່ສຳຄັນຕໍ່ຊາດ ຊຶ່ງການຢຸດສະງັກ ຫຼື ທຳລາຍໜ່ວຍງານເຫຼົ່ານີ້ ຈະສົ່ງຜົນກະທົບຮ້າຍແຮງຕໍ່ຄວາມ

ໝັ້ນຄົງ, ເສດຖະກິດ-ສັງຄົມຂອງ ສປປ ລາວ;

3. ໜ່ວຍງານຕອບໂຕ້ເຫດສຸກເສີນທາງຄອມພິວເຕີ (CERT) ໝາຍເຖິງ ທີມຊ່ຽວຊານທີ່ຮັບຜິດຊອບຈັດການ ແລະ ປ້ອງກັນເຫດການດ້ານຄວາມປອດໄພໄຊເບີ;

4. ໄພຄຸກຄາມທາງໄຊເບີ (Cyber threat) ໝາຍເຖິງ ໄພອັນຕະລາຍ ຫຼື ຄວາມສ່ຽງ ທີ່ອາດເກີດຂຶ້ນກັບລະບົບ, ເຄືອຂ່າຍ ຫຼື ຂໍ້ມູນ ໃນໂລກໄຊເບີ ເປັນຕົ້ນ ການໂຈມຕີທາງໄຊເບີ, ມອນແວ ຫຼື ການລະເມີດຂໍ້ມູນສ່ວນຕົວ;

5. ໂລກໄຊເບີ (Cyberspace) ໝາຍເຖິງ ສະພາບແວດລ້ອມດິຈິຕອນ ຊຶ່ງປະກອບດ້ວຍ ລະບົບ, ເຄືອຂ່າຍ, ຂໍ້ມູນເອເລັກໂຕຣນິກ ແລະ ການໂຕ້ຕອບ ລະຫວ່າງຜູ້ໃຊ້ງານທັງໝົດ ທີ່ເຊື່ອມຕໍ່ຜ່ານເຕັກໂນໂລຊີການສື່ສານ;

6. ການໂຈມຕີທາງໄຊເບີ (Cyber attack) ໝາຍເຖິງ ການກະທຳໃດໜຶ່ງ ທີ່ມີເຈດຕະນາທຳລາຍ, ຂັດຂວາງ ຫຼື ເຂົ້າເຖິງ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ຕໍ່ລະບົບ, ເຄືອຂ່າຍ ຫຼື ຂໍ້ມູນ ເປັນຕົ້ນ ການໂຈມຕີແບບດີດອດ, ການເຈາະລະບົບ, ຊ່ອງໂຫວ່ຂອງລະບົບຄອມພິວເຕີ;

7. ໄຟວໍ (Firewall) ໝາຍເຖິງ ລະບົບຮັກສາຄວາມປອດໄພເຄືອຂ່າຍທີ່ຕິດຕາມ ແລະ ຄວບຄຸມການຈະລາຈອນຂໍ້ມູນເຂົ້າ-ອອກ, ປ້ອງກັນການເຂົ້າເຖິງທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດ ແລະ ໄພຄຸກຄາມທາງອິນເຕີເນັດ;

8. ການໂຈມຕີແບບດີດອດ (Distributed Denial of Service attack - DDoS) ໝາຍເຖິງ ການໂຈມຕີທາງໄຊເບີ ທີ່ໃຊ້ຄວບຄຸມອຸປະກອນຈຳນວນຫຼາຍ ໃນການຮ້ອງຂໍຂໍ້ມູນຈຳນວນຫຼາຍ ໄປຫາລະບົບເປົ້າໝາຍ, ເຮັດໃຫ້ລະບົບນັ້ນລົ້ມເຫຼວ ຫຼື ບໍ່ສາມາດໃຫ້ບໍລິການໄດ້ປົກກະຕິ;

9. ຄລາວ (Cloud) ໝາຍເຖິງ ລະບົບການເກັບຮັກສາ ແລະ ປະມວນຂໍ້ມູນທີ່ໃຊ້ຊັບພະຍາກອນຄອມພິວເຕີທາງໄກຜ່ານອິນເຕີເນັດ;

10. ຮາດດິດ (Hard disk) ໝາຍເຖິງ ອຸປະກອນເອເລັກໂຕຣນິກ ເພື່ອເກັບຂໍ້ມູນ ພາຍໃນຄອມພິວເຕີ, ໃຊ້ສຳລັບບັນທຶກ ແລະ ເກັບຮັກສາຂໍ້ມູນ ໃນປະລິມານຫຼາຍ;

11. ຂໍ້ມູນສ່ວນບຸກຄົນ (Personal data) ໝາຍເຖິງ ຂໍ້ມູນໃດໜຶ່ງ ທີ່ສາມາດນຳໃຊ້ເພື່ອລະບຸຕົວຕົນຂອງບຸກຄົນໄດ້ ບໍ່ວ່າທາງກົງ ຫຼື ທາງອ້ອມ;

12. ມອນແວ (Malware) ໝາຍເຖິງ ຊອບແວທີ່ຖືກອອກແບບມາເພື່ອ ທຳລາຍ, ກໍ່ກວນ ການເຮັດວຽກຂອງລະບົບຄອມພິວເຕີ ຫຼື ລັກຂໍ້ມູນ;

13. ແຣນຊຳແວ (Ransomware) ໝາຍເຖິງ ມອນແວປະເພດໜຶ່ງທີ່ເຂົ້າລະຫັດໄຟລ ຂອງຜູ້ຖືກຕົວະຍົວະຫຼອກລວງ ແລະ ຮຽກຄ່າໄຖ່ ເພື່ອແລກກັບການຖອດລະຫັດເອກະສານ;

14. ຊ່ອງໂຫວ່ຂອງລະບົບຄອມພິວເຕີ (Vulnerability) ໝາຍເຖິງ ຂໍ້ບົກພ່ອງຂອງໂປຣແກຣມ ຫຼື ຊອບແວ ທີ່ບໍ່ສົມບູນ ແລະ/ຫຼື ບໍ່ໄດ້ຮັບການປັບປຸງ ເຮັດໃຫ້ຜູ້ປະສົງຮ້າຍສາມາດສວຍໃຊ້ ເພື່ອທຳລາຍລະບົບ, ລັກຂໍ້ມູນ, ປ່ຽນແປງຂໍ້ມູນ ແລະ ອື່ນໆ;

15. ເຄືອຂ່າຍ (Network) ໝາຍເຖິງ ລະບົບເຊື່ອມຕໍ່ອຸປະກອນ ຄອມພິວເຕີ ແລະ ເອເລັກໂຕຣນິກທີ່ສາມາດແລກປ່ຽນ ຂໍ້ມູນ ຂ່າວສານ ໄດ້;

16. ຖານຂໍ້ມູນ (Database) ໝາຍເຖິງ ລະບົບເກັບຮັກສາ ແລະ ຈັດການຂໍ້ມູນທີ່ສາມາດຄົ້ນຫາ ແລະ ເຂົ້າເຖິງໄດ້ຢ່າງເປັນລະບົບ;

17. ລະບົບຄວບຄຸມ (Control System) ໝາຍເຖິງ ລະບົບທີ່ໃຊ້ໃນການ ຄວບຄຸມ, ຕິດຕາມ ແລະ ຈັດການພຶດຕິກຳຂອງອຸປະກອນ, ເຄື່ອງຈັກ ຫຼື ຂະບວນການຕ່າງໆ ໃຫ້ເຮັດວຽກອັດຕະໂນມັດ ເປັນຕົ້ນ ລະບົບຄວບຄຸມອຸດສາຫະກຳ, ລະບົບປັບອາກາດ, ລະບົບຄວບຄຸມການບິນຂອງເຮືອບິນ;

18. ປັນຍາປະດິດ (Artificial Intelligence - AI) ໝາຍເຖິງ ເຕັກໂນໂລຊີທີ່ເຮັດໃຫ້ເຄື່ອງຈັກ ສາມາດຄິດ, ຮຽນຮູ້ ແລະ ຕັດສິນໃຈໄດ້ຄືກັບມະນຸດ;

19. ການສົ່ງເສີມການພັດທະນາລະບົບນິເວດດິຈິຕອນທີ່ປອດໄພ (Secure Digital Ecosystem) ໝາຍເຖິງ ການສ້າງສະພາບແວດລ້ອມດິຈິຕອນທີ່ປອດໄພ ແລະ ເຊື່ອຖືໄດ້ ຊຶ່ງປະກອບດ້ວຍ ການພັດທະນາໂຄງລ່າງພື້ນຖານເຕັກໂນໂລຊີທີ່ປອດໄພ, ປົກປ້ອງຂໍ້ມູນສ່ວນຕົວ, ພັດທະນາບຸກຄະລາກອນ, ສ້າງນິຕິກຳທີ່ເໝາະສົມ ແລະ ເຊື່ອມໂຍງສາກົນຢ່າງປອດໄພ ເພື່ອສົ່ງເສີມເສດຖະກິດດິຈິຕອນ;

20. ຜູ້ໃຫ້ບໍລິການພາຍນອກ (Third-party Service Provider) ໝາຍເຖິງ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ພາຍນອກທີ່ໃຫ້ບໍລິການດ້ານເຕັກໂນໂລຊີ ຂໍ້ມູນ ຂ່າວສານ, ການບໍລິການຄລາວ, ການບຳລຸງຮັກສາລະບົບ ຫຼື ການບໍລິການຄວາມປອດໄພໄຊເບີອື່ນ ທີ່ອາດເຂົ້າເຖິງ ຫຼື ປະມວນຜົນຂໍ້ມູນຂອງໜ່ວຍງານ.

ມາດຕາ 4 ນະໂຍບາຍຂອງລັດ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ

ລັດ ຖືເອົາຄວາມປອດໄພໄຊເບີ ເປັນບຸລິມະສິດ ໃນວຽກງານປ້ອງກັນຊາດ-ປ້ອງກັນຄວາມສະຫງົບ, ການພັດທະນາເສດຖະກິດ-ສັງຄົມ, ວິທະຍາສາດ, ເຕັກໂນໂລຊີ ແລະ ການຕ່າງປະເທດ.

ລັດ ຖືສຳຄັນວຽກງານຄວາມປອດໄພໄຊເບີ ດ້ວຍການສະໜອງ ງົບປະມານ, ວັດຖຸປະກອນທີ່ຈຳເປັນ, ສ້າງໂຄງລ່າງພື້ນຖານ, ພັດທະນາ, ບຳລຸງ ແລະ ປະກອບຊັບພະຍາກອນມະນຸດ ທີ່ເປັນມືອາຊີບ, ຄົ້ນຄວ້ານຳໃຊ້ເຕັກໂນໂລຊີທີ່ທັນສະໄໝ ເພື່ອເຮັດໃຫ້ວຽກງານດັ່ງກ່າວ ມີປະສິດທິພາບ ແລະ ປະສິດທິຜົນ.

ລັດ ສົ່ງເສີມ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທັງພາຍໃນ ແລະ ຕ່າງປະເທດ ໃຫ້ມີການຮ່ວມມື ແລະ ມີສ່ວນຮ່ວມໃນການປ້ອງກັນຄວາມປອດໄພໄຊເບີ ທີ່ເປັນອັນຕະລາຍຕໍ່ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ແລະ ຄວາມເປັນລະບຽບຮຽບຮ້ອຍຂອງສັງຄົມ.

ລັດ ຊຸກຍູ້ ແລະ ສົ່ງເສີມ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ໃຫ້ມີການຄົ້ນຄວ້າ, ການລົງທຶນ, ການພັດທະນາເຕັກໂນໂລຊີ, ຜະລິດຕະພັນ ແລະ ການບໍລິການ ເພື່ອປ້ອງກັນຄວາມປອດໄພໄຊເບີ.

ມາດຕາ 5 ຫຼັກການກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ

ວຽກງານຄວາມປອດໄພໄຊເບີ ໃຫ້ປະຕິບັດຕາມຫຼັກການ ດັ່ງນີ້:

1. ສອດຄ່ອງກັບ ແນວທາງ ນະໂຍບາຍ, ລັດຖະທຳມະນູນ, ກົດໝາຍ, ແຜນຍຸດທະສາດ ແລະ ແຜນພັດທະນາເສດຖະກິດ-ສັງຄົມແຫ່ງຊາດ;

2. ຮັບປະກັນ ຄວາມໝັ້ນຄົງຂອງຊາດ, ຄວາມສະຫງົບ ແລະ ຄວາມເປັນລະບຽບຮຽບຮ້ອຍຂອງສັງຄົມ;

3. ຮັບປະກັນຄວາມປອດໄພທາງດ້ານ ຂໍ້ມູນ ຂ່າວສານ ຂອງລັດ, ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ;

4. ຮັບປະກັນຄວາມສະເໝີພາບຕໍ່ໜ້າກົດໝາຍ, ປົກປ້ອງສິດ ແລະ ຜົນປະໂຫຍດຂອງຜູ້ຊົມໃຊ້;

5. ຮັບປະກັນການປະສານສົມທົບກັບ ກະຊວງ, ອົງການ, ອົງການປົກຄອງທ້ອງຖິ່ນ ແລະ ພາກສ່ວນອື່ນ ທີ່ກ່ຽວຂ້ອງ;

6. ສອດຄ່ອງກັບສົນທິສັນຍາ ທີ່ ສປປ ລາວ ເປັນພາຄີ ແລະ ສັນຍາສາກົນທີ່ກ່ຽວຂ້ອງ.

ມາດຕາ 6 ຂອບເຂດການນຳໃຊ້ກົດໝາຍ

ກົດໝາຍສະບັບນີ້ ນຳໃຊ້ສຳລັບ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທັງພາຍໃນ ແລະ ຕ່າງປະເທດ ທີ່ເຄື່ອນໄຫວ ແລະ ພົວພັນກັບວຽກງານຄວາມປອດໄພໄຊເບີ ຢູ່ ສປປ ລາວ.

ມາດຕາ 7 ການຮ່ວມມືສາກົນ

ລັດ ສົ່ງເສີມ ການພົວພັນ ແລະ ຮ່ວມມືກັບ ຕ່າງປະເທດ, ພາກພື້ນ ແລະ ສາກົນ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ ດ້ວຍການແລກປ່ຽນ ບົດຮຽນ, ປະສົບການ, ຂໍ້ມູນ ຂ່າວສານ, ເຕັກນິກ, ເຕັກໂນໂລຊີ, ນະວັດຕະກຳ, ຍົກລະດັບວິຊາສະເພາະ, ຄວາມຮູ້ ຄວາມສາມາດ ທາງດ້ານວິຊາການ ໃຫ້ບຸກຄະລາກອນ, ການພັດທະນາຊັບພະຍາກອນມະນຸດ, ປະຕິບັດສົນທິສັນຍາ ທີ່ ສປປ ລາວ ເປັນພາຄີ ແລະ ສັນຍາສາກົນທີ່ກ່ຽວຂ້ອງ.

ພາກທີ II
ອົງປະກອບທີ່ສຳຄັນຂອງຄວາມປອດໄພໄຊເບີ

ມາດຕາ 8 ອົງປະກອບທີ່ສຳຄັນຂອງຄວາມປອດໄພໄຊເບີ

ອົງປະກອບທີ່ສຳຄັນຂອງຄວາມປອດໄພໄຊເບີ ມີ ດັ່ງນີ້:

1. ການຮັກສາຄວາມລັບ;
2. ຄວາມຄົບຖ້ວນສົມບູນ;
3. ຄວາມພ້ອມໃຊ້ງານ;
4. ການພິສູດຕົວຕົນ ແລະ ການຄວບຄຸມການເຂົ້າເຖິງ;
5. ຫຼັກຖານດິຈິຕອນ ແລະ ຄວາມຮັບຜິດຊອບ.

ມາດຕາ 9 ການຮັກສາຄວາມລັບ

ການຮັກສາຄວາມລັບ ແມ່ນ ການປົກປ້ອງຂໍ້ມູນຈາກ ການເຂົ້າເຖິງ ຫຼື ການເປີດເຜີຍ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ຊຶ່ງການຮັກສາຄວາມລັບຂອງຂໍ້ມູນນັ້ນ ປະກອບດ້ວຍ ການເຂົ້າລະຫັດຂໍ້ມູນ, ການຄວບຄຸມການເຂົ້າເຖິງ, ການຈັດປະເພດຂໍ້ມູນ ແລະ ອື່ນໆ.

ມາດຕາ 10 ຄວາມຄົບຖ້ວນສົມບູນ

ຄວາມຄົບຖ້ວນສົມບູນ ແມ່ນ ຄວາມຖືກຕ້ອງ ແລະ ຄວາມສົມບູນດັ່ງເດີມຂອງຂໍ້ມູນ ທີ່ໄດ້ຮັບການຮັກສາໄວ້ຕະຫຼອດອາຍຸການນຳໃຊ້ຂໍ້ມູນ ດ້ວຍການນຳໃຊ້ເຕັກໂນໂລຊີ ເປັນຕົ້ນ ລາຍເຊັນເອເລັກໂຕຣນິກ, ການກວດສອບຄວາມຖືກຕ້ອງຂອງຂໍ້ມູນ, ການຄວບຄຸມການປ່ຽນແປງ, ການສຳຮອງຂໍ້ມູນ, ການກູ້ຄືນ.

ມາດຕາ 11 ຄວາມພ້ອມໃຊ້ງານ

ຄວາມພ້ອມໃຊ້ງານ ແມ່ນ ການຮັບປະກັນຄວາມພ້ອມໃນການສະໜອງ ຂໍ້ມູນ, ຊັບພະຍາກອນໃນລະບົບ ຊຶ່ງປະກອບດ້ວຍ ການວາງແຜນໃນການພັດທະນາຢ່າງຕໍ່ເນື່ອງ, ການສຳຮອງຂໍ້ມູນ, ການກູ້ຄືນຈາກໄພພິບັດ, ການບຳລຸງຮັກສາລະບົບ ແລະ ການຈັດການຄວາມສາມາດໃນການຮອງຮັບ ໃຫ້ແກ່ບຸກຄົນທີ່ຕ້ອງການ ຫຼື ລະບົບທີ່ໄດ້ຮັບອະນຸຍາດ.

ມາດຕາ 12 ການຜິສູດຕົວຕົນ ແລະ ການຄວບຄຸມການເຂົ້າເຖິງ

ການຜິສູດຕົວຕົນ ແມ່ນ ຂະບວນການກວດສອບຄວາມຖືກຕ້ອງຂອງສາຍ ກ່ຽວພັນລະຫວ່າງ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ກັບຂໍ້ມູນ ແລະ ຄຸນລັກສະນະ ທີ່ເອົາມາຈາກຖານຂໍ້ມູນຂອງການຈັດຕັ້ງທີ່ກ່ຽວຂ້ອງ ທີ່ນຳມາອ້າງອີງເປັນຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ນັ້ນ.

ການຄວບຄຸມການເຂົ້າເຖິງ ແມ່ນ ລະບົບທີ່ຮັບປະກັນວ່າມີພຽງແຕ່ ບຸກຄົນ ຫຼື ລະບົບທີ່ໄດ້ຮັບອະນຸຍາດ ເທົ່ານັ້ນ ຈຶ່ງສາມາດເຂົ້າເຖິງ ຂໍ້ມູນ ຫຼື ຊັບພະຍາກອນເຕັກໂນໂລຊີໄດ້ ໂດຍອີງຕາມສິດ ແລະ ຄວາມຈຳເປັນໃນ ການເຂົ້າເຖິງ ໂດຍມີການກວດສອບການເຂົ້າເຖິງຢ່າງເປັນລະບົບ.

ມາດຕາ 13 ຫຼັກຖານດິຈິຕອນ ແລະ ຄວາມຮັບຜິດຊອບ

ຫຼັກຖານດິຈິຕອນ ແມ່ນ ຂໍ້ມູນທີ່ບັນທຶກດ້ວຍເຄື່ອງມືເອເລັກໂຕຣນິກ ແລະ ເກັບຮັກສາໄວ້ຢູ່ໃນລະບົບ ຫຼື ຢູ່ລະຫວ່າງການສົ່ງ, ຮັບ ຊຶ່ງສາມາດພິສູດ ການກະທຳ ຫຼື ເຫດການໃດໜຶ່ງເກີດຂຶ້ນຈິງ.

ຄວາມຮັບຜິດຊອບ ແມ່ນ ພັນທະຂອງຜູ້ກໍ່ຄວາມເສຍຫາຍ ທີ່ຕ້ອງໄດ້ຮັບຜິດຊອບຕໍ່ການກະທຳຂອງຕົນ ເປັນຕົ້ນ ກອບກູ້ກຽດສັກສີ, ຂໍໂທດ, ສຶກສາອົບຮົມ, ກ່າວເຕືອນ, ລົງວິໄນ, ປັບໃໝ, ໃຊ້ແທນຄ່າເສຍຫາຍທາງແພ່ງ, ລົງໂທດທາງອາຍາ.

ພາກທີ III
ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ

ມາດຕາ 14 ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ

ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ແມ່ນ ລະບົບ, ຊັບສິນ, ສິ່ງອຳນວຍຄວາມສະດວກ ແລະ ເຄືອຂ່າຍ ທີ່ມີຄວາມສຳຄັນຫຼາຍຕໍ່ ຄວາມໝັ້ນຄົງ, ຄວາມສະຫງົບ, ຄວາມປອດໄພ, ເສດຖະກິດ-ສັງຄົມ, ວິທະຍາສາດ, ເຕັກໂນໂລຊີ ແລະ ການຕ່າງປະເທດ ຂອງ ສປປ ລາວ ຊຶ່ງການຢຸດສະງັກ ຫຼື ການທຳລາຍ ຂອງໂຄງ ລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ດັ່ງກ່າວ ສົ່ງຜົນກະທົບຮ້າຍແຮງໂດຍກົງຕໍ່ປະເທດຊາດ.

ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ໄດ້ກຳນົດເປັນແຕ່ລະຂະແໜງການ, ການປົກປ້ອງ ໜ່ວຍງານ ແລະ ລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ.

ໝວດທີ 1
ຂະແໜງການໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ

ມາດຕາ 15 ຂະແໜງການໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ

ຂະແໜງການໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ມີ ດັ່ງນີ້:

1. ປ້ອງກັນຊາດ-ປ້ອງກັນຄວາມສະຫງົບ;
2. ເຕັກໂນໂລຊີ ແລະ ການສື່ສານ;
3. ການເງິນ ແລະ ການທະນາຄານ;
4. ພະລັງງານ;
5. ການຄ້າ, ຄົມມະນາຄົມຂົນສົ່ງ ແລະ ໂລຊິດສະຕິກ;
6. ຂະແໜງການອື່ນ.

ມາດຕາ 16 ເງື່ອນໄຂການກຳນົດຂະແໜງການໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ

ຂະແໜງການໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ໄດ້ກຳນົດຕາມເງື່ອນໄຂ ດັ່ງນີ້:

1. ຄວາມສຳຄັນຕໍ່ການດຳລົງຊີວິດຂອງປະຊາຊົນ;
2. ການພັດທະນາປະເທດຊາດ;
3. ຄວາມສ່ຽງຕໍ່ການຖືກໂຈມຕີທາງໄຊເບີ ຫຼື ໄພພິບັດອື່ນ;
4. ຜົນກະທົບຈາກການຢຸດສະງັກ ຫຼື ການຖືກທຳລາຍການໃຫ້ບໍລິການ.

ໝວດທີ 2
ການປົກປ້ອງໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ

ມາດຕາ 17 ການກຳນົດໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ

ການກຳນົດໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ໃຫ້ປະຕິບັດ ດັ່ງນີ້:

1. ລະບຸ ແລະ ຈັດປະເພດໜ່ວຍງານ ທີ່ອາດຈະເປັນໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ;
2. ປະເມີນຄວາມສ່ຽງ ແລະ ຜົນກະທົບທີ່ອາດຈະເກີດຂຶ້ນ;
3. ຈັດລຳດັບຄວາມສຳຄັນຂອງໜ່ວຍງານ;
4. ກຳນົດ ແລະ ຮັບຮອງ ລາຍຊື່ໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ.

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນເຈົ້າການໃນການປະສານສົມທົບກັບ ກະຊວງ, ອົງການ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ທີ່ກ່ຽວຂ້ອງ ເພື່ອທົບທວນ ແລະ ປະເມີນໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ໜຶ່ງຄັ້ງ ຕໍ່ປີ ຫຼື ເມື່ອມີການປ່ຽນແປງທີ່ສຳຄັນຂອງເຕັກໂນໂລຊີ ຂໍ້ມູນ ຂ່າວສານ ແລ້ວສະເໜີລັດຖະບານ ພິຈາລະນາຮັບຮອງ.

ມາດຕາ 18 ການປົກປ້ອງທາງກາຍຍະພາບ ແລະ ການຄວບຄຸມການເຂົ້າເຖິງ

ໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ຕ້ອງມີການປົກປ້ອງທາງກາຍຍະພາບ ແລະ ການຄວບຄຸມການເຂົ້າເຖິງ ດັ່ງນີ້:

1. ລະບົບການຮັກສາຄວາມປອດໄພທາງກາຍຍະພາບທີ່ເຂັ້ມງວດ;
2. ການແຍກພື້ນທີ່ສຳຄັນອອກຈາກພື້ນທີ່ທົ່ວໄປ ແລະ ຈຳກັດການເຂົ້າເຖິງສະເພາະບຸກຄົນທີ່ໄດ້ຮັບອະນຸຍາດເທົ່ານັ້ນ;
3. ລະບົບການຜິສູດຕົວຕົນ ແລະ ການຄວບຄຸມການເຂົ້າເຖິງທີ່ເຂັ້ມງວດ;
4. ການບັນທຶກ ແລະ ຕິດຕາມການເຂົ້າ ອອກ ທຸກຄັ້ງ.

ມາດຕາ 19 ການຄວບຄຸມ ຜູ້ສະໜອງ ແລະ ຜູ້ໃຫ້ບໍລິການພາຍນອກ

ການຄວບຄຸມ ຜູ້ສະໜອງ ແລະ ຜູ້ໃຫ້ບໍລິການພາຍນອກ ໃຫ້ປະຕິບັດ ດັ່ງນີ້:

1. ຕ້ອງຜ່ານການກວດສອບພື້ນຖານ ແລະ ໄດ້ຮັບການຮັບຮອງ ຈາກຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ;
2. ຕ້ອງຄວບຄຸມການເຂົ້າເຖິງ ຂອງຜູ້ສະໜອງ ແລະ ຜູ້ໃຫ້ບໍລິການພາຍນອກ ຢ່າງເຂັ້ມງວດ;
3. ຕ້ອງຜ່ານການກວດສອບ ຕາມຂໍ້ກຳນົດດ້ານຄວາມປອດໄພໄຊເບີ ຢ່າງເຂັ້ມງວດ.

ມາດຕາ 20 ການລາຍງານ, ການແຈ້ງເຕືອນ ແລະ ການປະເມີນຜົນ

ໃນການລາຍງານ, ການແຈ້ງເຕືອນ ແລະ ການປະເມີນຜົນ ໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ໃຫ້ປະຕິບັດ ດັ່ງນີ້:

1. ສ້າງຕັ້ງລະບົບ ການລາຍງານ ແລະ ການແຈ້ງເຕືອນ ຄວາມປອດໄພໄຊເບີ;

2. ຕ້ອງລາຍງານເຫດການສຸກເສີນໂດຍທັນທີ ຕໍ່ໜ່ວຍງານຮັບຜິດຊອບວຽກງານຄວາມປອດໄພໄຊເບີ ໃນກໍລະນີເກີດມີໄພຄຸກຄາມທາງໄຊເບີ ຕໍ່ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ;

3. ຕ້ອງມີລະບົບແຈ້ງເຕືອນລ່ວງໜ້າ ສຳລັບໄພຄຸກຄາມທີ່ອາດຈະເກີດຂຶ້ນຕໍ່ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ;

4. ໃຫ້ໜ່ວຍງານຮັບຜິດຊອບວຽກງານຄວາມປອດໄພໄຊເບີ ດຳເນີນການກວດກາ ແລະ ປະເມີນຜົນ ຄວາມພ້ອມຂອງໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ຢ່າງເປັນປະຈຳ;

5. ຕ້ອງລາຍງານຜົນການກວດກາ ແລະ ການປະເມີນຜົນ ຕໍ່ລັດຖະບານ ໃນທັນທີ.

ມາດຕາ 21 ຄວາມຮັບຜິດຊອບຂອງໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ

ໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ຕ້ອງມີຄວາມຮັບຜິດຊອບ ດັ່ງນີ້:

1. ປະຕິບັດຕາມຂໍ້ກຳນົດທີ່ອອກໂດຍໜ່ວຍງານຮັບຜິດຊອບວຽກງານຄວາມປອດໄພໄຊເບີ;

2. ມີແຜນພັດທະນາ ແລະ ປັບປຸງ ທີ່ຮັບປະກັນການດຳເນີນງານໄດ້ຕໍ່ເນື່ອງ ພ້ອມທັງແກ້ໄຂໃນກໍລະນີເກີດໄພຄຸກຄາມທາງໄຊເບີ;

3. ມີລະບົບສຳຮອງທີ່ພ້ອມໃຊ້ງານ ໃນກໍລະນີລະບົບຫຼັກລົ້ມເຫຼວ;

4. ມີການປະເມີນຄວາມສ່ຽງ ແລະ ການກວດສອບຄວາມປອດໄພໄຊເບີ ຢ່າງເປັນປະຈຳ.

ໝວດທີ 3
ລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ

ມາດຕາ 22 ລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ

ລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ ແມ່ນ ສູນກາງການຕິດຕາມ, ວິເຄາະ ແລະ ຕອບໂຕ້ຕໍ່ໄພຄຸກຄາມທາງໄຊເບີຂອງປະເທດ. ລະບົບດັ່ງກ່າວຂຶ້ນກັບກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ, ມີພາລະບົດບາດຄຸ້ມຄອງໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ, ອິນເຕີເນັດ ໃນຂອບເຂດທົ່ວປະເທດ ເພື່ອຕິດຕາມ ແລະ ວິເຄາະໄພຄຸກຄາມທາງໄຊເບີຢ່າງຕໍ່ເນື່ອງ, ປະສານງານ ແລະ ຕອບໂຕ້ຕໍ່ເຫດການສຸກເສີນທາງໄຊເບີ, ແລກປ່ຽນ ຂໍ້ມູນ ແລະ ແຈ້ງເຕືອນກ່ຽວກັບໄພຄຸກຄາມ, ໃຫ້ຄຳແນະນຳ ແລະ ຊ່ວຍເຫຼືອທາງວິຊາການ, ຈັດຝຶກອົບຮົມ ແລະ ສ້າງຂີດຄວາມສາມາດໃຫ້ບຸກຄະລາກອນ.

ລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ ປະກອບດ້ວຍ ເຄື່ອງມືທັນສະໄໝ ແລະ ບຸກຄະລາກອນຊ່ຽວຊານ ຊຶ່ງດຳເນີນວຽກຕະຫຼອດ ຊາວສີ່ຊົ່ວໂມງ, ນຳໃຊ້ເຕັກໂນໂລຊີການວິເຄາະຂໍ້ມູນຂະໜາດໃຫຍ່ ແລະ ປັນຍາປະດິດ ເພື່ອກວດຈັບ ແລະ ຕອບໂຕ້ ຕໍ່ໄພຄຸກຄາມໄດ້ຢ່າງວ່ອງໄວ. ນອກຈາກນີ້, ລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ ຍັງປະສານງານກັບໜ່ວຍງານອື່ນ ທັງພາກລັດ ແລະ ເອກະຊົນ ເພື່ອຮັບປະກັນວຽກງານຄວາມປອດໄພໄຊເບີຂອງປະເທດ.

ມາດຕາ 23 ການເຊື່ອມຕໍ່ກັບລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ

ໃນການເຊື່ອມຕໍ່ກັບລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ ໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ໃຫ້ປະຕິບັດ ດັ່ງນີ້:

1. ຕ້ອງເຊື່ອມຕໍ່ກັບລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ;
2. ດຳເນີນຕາມຂັ້ນຕອນ ແລະ ມາດຕະຖານທາງເຕັກນິກໃນການເຊື່ອມຕໍ່ ທີ່ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ກຳນົດອອກ ແຕ່ລະໄລຍະ;
3. ຮັບປະກັນຄວາມປອດໄພ ແລະ ຄວາມໜ້າເຊື່ອຖືຂອງການເຊື່ອມຕໍ່;
4. ຮັກສາຄວາມລັບຂອງຂໍ້ມູນທີ່ແລກປ່ຽນຜ່ານລະບົບ;
5. ທົດສອບ ແລະ ບຳລຸງຮັກສາການເຊື່ອມຕໍ່.

ພາກທີ IV
ມາດຕະການຄວາມປອດໄພໄຊເບີ
ໝວດທີ 1
ມາດຕະການປ້ອງກັນ

ມາດຕາ 24 ມາດຕະການປ້ອງກັນ

ມາດຕະການປ້ອງກັນຄວາມປອດໄພໄຊເບີ ມີ ດັ່ງນີ້:

1. ການປະເມີນຄວາມສ່ຽງ;
2. ການຄວບຄຸມການເຂົ້າເຖິງ;
3. ການເຂົ້າລະຫັດຄວາມປອດໄພຂໍ້ມູນ;
4. ການຮັກສາຄວາມປອດໄພເຄືອຂ່າຍ;
5. ມາດຕະການປ້ອງກັນຄວາມປອດໄພໄຊເບີອື່ນ ທີ່ເຫັນວ່າມີຄວາມຈຳເປັນ.

ສຳລັບຂັ້ນຕອນ ແລະ ວິທີການ ກ່ຽວກັບມາດຕະການປ້ອງກັນຄວາມປອດໄພໄຊເບີ ໄດ້ກຳນົດໄວ້ໃນລະບຽບການຕ່າງຫາກ.

ມາດຕາ 25 ການປະເມີນຄວາມສ່ຽງ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງດຳເນີນມາດຕະການປະເມີນຄວາມສ່ຽງດ້ານຄວາມປອດໄພໄຊເບີທີ່ຄອບຄຸມ ລະບົບ, ຂໍ້ມູນ ແລະ ຊັບສິນດິຈິຕອນທີ່ສຳຄັນ ຊຶ່ງການປະເມີນດັ່ງກ່າວ ຕ້ອງດຳເນີນຢ່າງໜ້ອຍ ປີລະຄັ້ງ.

ຜົນການປະເມີນຄວາມສ່ຽງດ້ານຄວາມປອດໄພໄຊເບີ ຕ້ອງນຳໃຊ້ເຂົ້າໃນການປັບປຸງແຜນຄວາມປອດໄພ ແລະ ລາຍງານຕໍ່ຂັ້ນເທິງຖັດຕົນ.

ມາດຕາ 26 ການຄວບຄຸມການເຂົ້າເຖິງ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງດຳເນີນມາດຕະການຄວບຄຸມການເຂົ້າເຖິງລະບົບທີ່ມີປະສິດທິຜົນ ໂດຍໃຫ້ສິດໜ້ອຍສຸດ, ການແບ່ງແຍກໜ້າທີ່ ແລະ ການພິສູດຢືນຢັນຕົວຕົນຫຼາຍປັດໄຈ.

ມາດຕາ 27 ການເຂົ້າລະຫັດຄວາມປອດໄພຂໍ້ມູນ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງນຳໃຊ້ມາດຕະການ ການເຂົ້າລະຫັດຄວາມປອດໄພຂໍ້ມູນ ສຳລັບຂໍ້ມູນທີ່ສຳຄັນ ແລະ ອ່ອນໄຫວ ທີ່ເກັບຮັກສາໄວ້ ແລະ ກຳລັງສົ່ງຜ່ານເຄືອຂ່າຍ ຊຶ່ງການເຂົ້າລະຫັດຄວາມປອດໄພຂໍ້ມູນ ຕ້ອງນຳໃຊ້ວິທີການເຂົ້າລະຫັດທີ່ເຂັ້ມແຂງ.

ມາດຕາ 28 ການຮັກສາຄວາມປອດໄພເຄືອຂ່າຍ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງຈັດຕັ້ງປະຕິບັດ ມາດຕະການຮັກສາຄວາມປອດໄພເຄືອຂ່າຍ ດ້ວຍການຕິດຕັ້ງ ລະບົບໄຟວໍ ແລະ ລະບົບກວດຈັບປ້ອງກັນການບຸກລຸກ ພ້ອມທັງແບ່ງແຍກເຄືອຂ່າຍຢ່າງເໝາະສົມ ເພື່ອຮັບປະກັນຄວາມປອດໄພຂອງລະບົບເຄືອຂ່າຍ.

ໝວດທີ 2
ມາດຕະການຕອບໂຕ້ເຫດການສຸກເສີນ

ມາດຕາ 29 ມາດຕະການຕອບໂຕ້ເຫດການສຸກເສີນ

ມາດຕະການຕອບໂຕ້ເຫດການສຸກເສີນ ມີ ດັ່ງນີ້:

1. ລະບົບກວດຈັບ ແລະ ການວິເຄາະເຫດການສຸກເສີນທາງໄຊເບີ;
2. ການຈັດການ ແລະ ການຕອບໂຕ້ເຫດການສຸກເສີນທາງໄຊເບີ;
3. ມາດຕະການຕອບໂຕ້ອື່ນ ທີ່ເຫັນວ່າມີຄວາມຈຳເປັນ.

ມາດຕາ 30 ລະບົບກວດຈັບ ແລະ ການວິເຄາະເຫດການສຸກເສີນທາງໄຊເບີ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງນຳໃຊ້ລະບົບກວດຈັບ ແລະ ວິເຄາະເຫດການສຸກເສີນທາງໄຊເບີ ທີ່ມີປະສິດທິພາບ ທີ່ປະກອບດ້ວຍ ເຄື່ອງມືກວດຈັບ ແລະ ປ້ອງກັນການບຸກລຸກ, ເຕັກໂນໂລຊີ, ປັນຍາປະດິດສຳລັບການວິເຄາະຂໍ້ມູນ ແລະ ຈັດລຳດັບຄວາມສຳຄັນຂອງໄພຄຸກຄາມ ໂດຍມີຂັ້ນຕອນການລາຍງານ ແລະ ແຈ້ງເຕືອນທີ່ຊັດເຈນ ພ້ອມທັງຮັບປະກັນການເຮັດວຽກຕະຫຼອດ ຊາວສີ່ຊົ່ວໂມງ ໂດຍມີທີມງານຜູ້ຊ່ຽວຊານຕິດຕາມ ແລະ ມີແຜນສຳຮອງໃນກໍລະນີເກີດເຫດສຸກເສີນ.

ມາດຕາ 31 ການຈັດການ ແລະ ການຕອບໂຕ້ເຫດການສຸກເສີນທາງໄຊເບີ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງຈັດການ ແລະ ຕອບໂຕ້ເຫດການສຸກເສີນທາງໄຊເບີ ໂດຍມີການຜັກທະນາ ແລະ ຈັດຕັ້ງປະຕິບັດແຜນຕອບໂຕ້ເຫດການສຸກເສີນທາງໄຊເບີ ຊຶ່ງແຜນດັ່ງກ່າວຕ້ອງກຳນົດຂັ້ນຕອນລະອຽດ, ຊັດເຈນ ສຳລັບການຕອບໂຕ້, ບົດບາດຂອງໜ່ວຍງານຮັກສາຄວາມປອດໄພໄຊເບີ, ມາດຕະການຈຳກັດຄວາມເສຍຫາຍ ແລະ ຂັ້ນຕອນການລາຍງານ, ການປະສານສົມທົບກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ.

ສຳລັບຂັ້ນຕອນ ແລະ ວິທີການ ກ່ຽວກັບການຕອບໂຕ້ເຫດການສຸກເສີນທາງໄຊເບີ ໄດ້ກຳນົດໄວ້ໃນລະບຽບການຕ່າງຫາກ.

ໝວດທີ 3
ມາດຕະການໃນກໍລະນີເກີດເຫດສຸກເສີນ

ມາດຕາ 32 ມາດຕະການໃນກໍລະນີເກີດເຫດສຸກເສີນ

ມາດຕະການໃນກໍລະນີເກີດເຫດສຸກເສີນ ມີ ດັ່ງນີ້:

1. ການປະກາດພາວະສຸກເສີນ;
2. ການແຕ່ງຕັ້ງຄະນະສະເພາະກິດ;
3. ການຈຳກັດ ຫຼື ລະງັບການໃຫ້ການບໍລິການ;
4. ມາດຕະການອື່ນ ທີ່ເຫັນວ່າມີຄວາມຈຳເປັນ.

ມາດຕາ 33 ການປະກາດພາວະສຸກເສີນ

ລັດຖະບານ ເປັນຜູ້ປະກາດພາວະສຸກເສີນທາງໄຊເບີ ຕາມການສະເໜີຂອງກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເມື່ອເກີດເຫດການສຸກເສີນທາງໄຊເບີທີ່ຮ້າຍແຮງ ແລະ ສົ່ງຜົນກະທົບຢ່າງຫຼວງຫຼາຍຕໍ່ການພັດທະນາເສດຖະກິດ-ສັງຄົມຂອງຊາດ.

ມາດຕາ 34 ການແຕ່ງຕັ້ງຄະນະສະເພາະກິດ

ໃນກໍລະນີເກີດເຫດການສຸກເສີນທາງໄຊເບີທີ່ຮ້າຍແຮງ ແລະ ສົ່ງຜົນກະທົບຢ່າງຫຼວງຫຼາຍຕໍ່ການພັດທະນາເສດຖະກິດ-ສັງຄົມຂອງຊາດ ລັດຖະບານ ຕ້ອງແຕ່ງຕັ້ງຄະນະສະເພາະກິດ ຊຶ່ງປະກອບດ້ວຍ ຜູ້ຕາງໜ້າຈາກ ກະຊວງ, ອົງການ ແລະ ພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ເພື່ອດຳເນີນການຕອບໂຕ້ຕໍ່ເຫດການດັ່ງກ່າວ.

ມາດຕາ 35 ການຈຳກັດ ແລະ ລະງັບການໃຫ້ການບໍລິການ

ຄະນະສະເພາະກິດ ຕ້ອງນຳໃຊ້ມາດຕະການຈຳກັດ ຫຼື ລະງັບການໃຫ້ການບໍລິການ ເປັນຕົ້ນ ການໃຫ້ບໍລິການໂທລະຄົມມະນາຄົມ, ອິນເຕີເນັດ, ການສື່ສານ ທັງໝົດ ຫຼື ບາງສ່ວນ ເພື່ອປ້ອງກັນການແຜ່ລາມຂອງໄພຄຸກຄາມທີ່ເກີດຈາກເຫດການສຸກເສີນທາງໄຊເບີ.

ໃນການຄວບຄຸມ ແລະ ລະງັບການໃຫ້ການບໍລິການ ຄະນະສະເພາະກິດ ຕ້ອງປະສານສົມທົບກັບ ກະຊວງ, ອົງການ, ອົງການປົກຄອງທ້ອງຖິ່ນ ແລະ ພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ເພື່ອສະກັດກັ້ນບໍ່ໃຫ້ແຜ່ລາມ, ຫຼຸດຜ່ອນຜົນກະທົບ, ກູ້ຄືນລະບົບ ແລະ ນຳໃຊ້ມາດຕະການອື່ນ ທີ່ເຫັນວ່າມີຄວາມຈຳເປັນ.

ໝວດທີ 4
ມາດຕະການກູ້ຄືນລະບົບ

ມາດຕາ 36 ມາດຕະການກູ້ຄືນລະບົບ

ມາດຕະການກູ້ຄືນລະບົບ ມີ ດັ່ງນີ້:

1. ການຮັບມືເຫດການສຸກເສີນ;
2. ການສຳຮອງ ແລະ ການກູ້ຄືນລະບົບ;
3. ມາດຕະການອື່ນ ທີ່ເຫັນວ່າມີຄວາມຈຳເປັນ.

ມາດຕາ 37 ການຮັບມືເຫດການສຸກເສີນ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງກຳນົດ ຂັ້ນຕອນ ແລະ ວິທີການ ຮັບມືເຫດການສຸກເສີນ ເພື່ອປະເມີນ, ຄວບຄຸມ ແລະ ຈຳກັດ ໄພຄຸກຄາມທາງໄຊເບີ ຢ່າງທັນການ ແລ້ວລາຍງານຕໍ່ຄະນະສະເພາະກິດ ແລະ ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ.

ມາດຕາ 38 ການສຳຮອງ ແລະ ການກູ້ຄືນຂໍ້ມູນ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງສຳຮອງຂໍ້ມູນໄວ້ໃນລະບົບຄລາວ ແລະ/ຫຼື ຣາດແວ ລວມທັງສຳຮອງໄວ້ຫຼາຍບ່ອນ ເພື່ອໃຫ້ສາມາດກູ້ຄືນຂໍ້ມູນທີ່ໄດ້ສຳຮອງໄວ້ນັ້ນ ໃນກໍລະນີເກີດເຫດສຸກເສີນ.

ໝວດທີ 5
ການລາຍງານ ແລະ ການແລກປ່ຽນ ຂໍ້ມູນ

ມາດຕາ 39 ການລາຍງານຂໍ້ມູນ

ການລາຍງານຂໍ້ມູນ ມີ ດັ່ງນີ້:

1. ການລາຍງານເຫດການ;
2. ການແລກປ່ຽນຂໍ້ມູນ;
3. ການຮັກສາຄວາມລັບໃນການແລກປ່ຽນຂໍ້ມູນ;
4. ການຮ່ວມມືໃນການສຶບສວນ-ສອບສວນ;
5. ການລາຍງານປະຈຳປີ;
6. ການແລກປ່ຽນຂໍ້ມູນລະຫວ່າງປະເທດ;
7. ການລາຍງານຂໍ້ມູນອື່ນ ທີ່ເຫັນວ່າມີຄວາມຈຳເປັນ.

ມາດຕາ 40 ການລາຍງານເຫດການ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງລາຍງານເຫດການດ້ານຄວາມປອດໄພໄຊເບີ ທີ່ຈະສ້າງຄວາມເສຍຫາຍແກ່ຕົນ ແລະ/ຫຼື ແຜ່ລາມໄປຍັງພາກສ່ວນອື່ນ ຊຶ່ງຕ້ອງລາຍງານຕໍ່ໜ່ວຍງານຮັບຜິດຊອບຄວາມປອດໄພໄຊເບີທັນທີ ພາຍຫຼັງພົບເຫັນເຫດການດັ່ງກ່າວ ກໍຕ້ອງລາຍງານຂໍ້ມູນທີ່ຈຳເປັນ ເປັນຕົ້ນ ແຮນຊຳແວ, ມອນແວ, ການໂຈມຕີແບບດີດອດ ເພື່ອໃຫ້ສາມາດປະເມີນຜົນກະທົບ ແລະ ຕອບໂຕ້ ຢ່າງທັນການ.

ມາດຕາ 41 ການແລກປ່ຽນຂໍ້ມູນ

ໜ່ວຍງານຮັບຜິດຊອບຄວາມປອດໄພໄຊເບີ ຂອງຂະແໜງການໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ຕ້ອງແລກປ່ຽນຂໍ້ມູນກ່ຽວກັບໄພຄຸກຄາມທາງໄຊເບີ ແລະ ຊ່ອງໂຫວ່ດ້ານຄວາມປອດໄພ ກັບນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທີ່ກ່ຽວຂ້ອງ.

ໜ່ວຍງານຮັບຜິດຊອບຄວາມປອດໄພໄຊເບີຂອງ ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງປະສານສົມທົບ, ແລກປ່ຽນ ຂໍ້ມູນ ຂ່າວສານ ກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ກັບໜ່ວຍງານຮັກສາຄວາມປອດໄພໄຊເບີຂອງກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ.

ມາດຕາ 42 ການຮັກສາຄວາມລັບໃນການແລກປ່ຽນຂໍ້ມູນ

ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ ແລະ ໜ່ວຍງານຮັກສາຄວາມປອດໄພໄຊເບີຂອງກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຕ້ອງຮັບປະກັນວ່າຂໍ້ມູນທີ່ໄດ້ ລາຍງານເຫດການ ແລະ ແລກປ່ຽນ ຈະຖືກຮັກສາເປັນຄວາມລັບຕາມ ລະດັບຊັ້ນຄວາມລັບທີ່ໄດ້ກຳນົດໄວ້.

ມາດຕາ 43 ການຮ່ວມມືໃນການສືບສວນ-ສອບສວນ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງໃຫ້ການຮ່ວມມືກັບອົງການສືບສວນ-ສອບສວນທີ່ກ່ຽວຂ້ອງ ເປັນຕົ້ນ ການສະໜອງຂໍ້ມູນ, ຫຼັກຖານ, ການເຂົ້າເຖິງລະບົບທີ່ຈຳເປັນສຳລັບການສືບສວນ-ສອບສວນ ໃນກໍລະນີມີການ ລະເມີດຄວາມປອດໄພໄຊເບີ ທີ່ເປັນການກະທຳຜິດທາງອາຍາ.

ມາດຕາ 44 ການລາຍງານປະຈຳປີ

ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ຕ້ອງລາຍງານປະຈຳປີກ່ຽວກັບສະພາບການ ແລະ ການປະຕິບັດວຽກງານ ຄວາມປອດໄພໄຊເບີ ຕໍ່ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ພາຍໃນເດືອນມັງກອນ ຂອງທຸກປີ.

ການລາຍງານປະຈຳປີ ປະກອບດ້ວຍເນື້ອໃນ ດັ່ງນີ້:

1. ມາດຕະການຄວາມປອດໄພໄຊເບີທີ່ໄດ້ຈັດຕັ້ງປະຕິບັດ;
2. ເຫດການ ຫຼື ໄພຸກຄາມທາງໄຊເບີທີ່ເກີດຂຶ້ນ ແລະ ວິທີການແກ້ໄຂ;
3. ຄວາມຄືບໜ້າໃນການປະຕິບັດຕາມແຜນຄວາມປອດໄພໄຊເບີ;
4. ຊ່ອງໂຫວ່ຂອງລະບົບຄອມພິວເຕີ ທີ່ພົບເຫັນ ແລະ ວິທີການແກ້ໄຂ;
5. ການສ້າງຄວາມຮັບຮູ້ ແລະ ການຝຶກອົບຮົມ ດ້ານຄວາມປອດໄພໄຊເບີ;
6. ກຳນົດແຜນການສຳລັບປີຕໍ່ໄປ.

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຕ້ອງສັງລວມ, ວິເຄາະ ແລະ ລາຍງານຜົນ ຕໍ່ລັດຖະບານ ພາຍໃນ ເວລາ ສາມສິບວັນ.

ມາດຕາ 45 ການແລກປ່ຽນຂໍ້ມູນລະຫວ່າງປະເທດ

ການແລກປ່ຽນຂໍ້ມູນລະຫວ່າງປະເທດ ກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ມີ ດັ່ງນີ້:

1. ຂໍ້ມູນກ່ຽວກັບ ໄພຸກຄາມ ແລະ ຊ່ອງໂຫວ່ ຂອງລະບົບຄອມພິວເຕີ;
2. ເຕັກນິກການວິເຄາະ ແລະ ການຕອບໂຕ້ຕໍ່ໄພຸກຄາມທາງໄຊເບີ;
3. ບົດຮຽນ ແລະ ປະສົບການໃນການຈັດຕັ້ງປະຕິບັດວຽກງານຄວາມປອດໄພໄຊເບີ;
4. ຂໍ້ມູນອື່ນທີ່ເຫັນວ່າມີຄວາມຈຳເປັນ.

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນເຈົ້າການໃນການແລກປ່ຽນຂໍ້ມູນ ລະຫວ່າງປະເທດ ດ້ານຄວາມ ປອດໄພໄຊເບີ ໂດຍຮັບປະກັນຄວາມປອດໄພ, ການຮັກສາຄວາມລັບ ແລະ ສອດຄ່ອງກັບສົນທິສັນຍາ ທີ່ ສປປ ລາວ ເປັນພາຄີ ແລະ ສັນຍາສາກົນທີ່ກ່ຽວຂ້ອງ.

ໝວດທີ 6
ການສ້າງຄວາມຮັບຮູ້ ແລະ ການຝຶກອົບຮົມ

ມາດຕາ 46 ການສ້າງຄວາມຮັບຮູ້ ແລະ ການຝຶກອົບຮົມ

ການສ້າງຄວາມຮັບຮູ້ ແລະ ການຝຶກອົບຮົມ ມີ ດັ່ງນີ້:

1. ການສ້າງຄວາມຮັບຮູ້ດ້ານຄວາມປອດໄພໄຊເບີ;
2. ການຝຶກອົບຮົມດ້ານຄວາມປອດໄພໄຊເບີ.

ມາດຕາ 47 ການສ້າງຄວາມຮັບຮູ້ດ້ານຄວາມປອດໄພໄຊເບີ

ອີງການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ, ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ ແລະ ພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ຕ້ອງສ້າງຄວາມຮັບຮູ້ດ້ານຄວາມປອດໄພໄຊເບີ ເປັນຕົ້ນ ຄວາມຮັບຮູ້ກ່ຽວກັບໄພຄຸກຄາມທາງໄຊເບີ, ວິທີການປ້ອງກັນໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ຢ່າງເປັນປົກກະຕິ ແລະ ຕໍ່ເນື່ອງ ເພື່ອສ້າງວັດທະນະທຳດ້ານຄວາມປອດໄພໄຊເບີທີ່ເຂັ້ມແຂງໃຫ້ແກ່ ການຈັດຕັ້ງຂອງຕົນ ແລະ ສັງຄົມ.

ມາດຕາ 48 ການຝຶກອົບຮົມດ້ານຄວາມປອດໄພໄຊເບີ

ອີງການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ, ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ ແລະ ພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ຕ້ອງຈັດຝຶກອົບຮົມດ້ານຄວາມປອດໄພໄຊເບີ ດັ່ງນີ້:

1. ສ້າງຄວາມເຂົ້າໃຈພື້ນຖານກ່ຽວກັບຄວາມປອດໄພໄຊເບີ;
2. ພັດທະນາທັກສະໃນການລະບຸ ແລະ ຕອບໂຕ້ຕໍ່ໄພຄຸກຄາມທາງໄຊເບີ;
3. ຝຶກປະຕິບັດຕົວຈິງໃນການຮັບມືກັບເຫດການສຸກເສີນທາງໄຊເບີ;
4. ປັບປຸງຄວາມຮູ້ ແລະ ທັກສະໃຫ້ທັນກັບເຕັກໂນໂລຊີ ແລະ ໄພຄຸກຄາມທາງໄຊເບີ.

ການຝຶກອົບຮົມດ້ານຄວາມປອດໄພໄຊເບີ ຕ້ອງດຳເນີນການຢ່າງເປັນປົກກະຕິ ແລະ ຕໍ່ເນື່ອງ ໂດຍມີການປະເມີນຜົນ ແລະ ປັບປຸງຂຶ້ນຕອນ, ເຕັກນິກ ແລະ ວິທີການຝຶກອົບຮົມ ເພື່ອໃຫ້ການຝຶກອົບຮົມດ້ານຄວາມປອດໄພໄຊເບີ ມີປະສິດທິພາບ ແລະ ປະສິດທິຜົນ.

ພາກທີ V
ການດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ມາດຕາ 49 ປະເພດທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ປະເພດທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ມີ ດັ່ງນີ້:

1. ການໃຫ້ຄຳປຶກສາດ້ານຄວາມປອດໄພໄຊເບີ;
2. ການພັດທະນາ ແລະ ຕິດຕັ້ງລະບົບຄວາມປອດໄພ;
3. ການທົດສອບການເຈາະລະບົບ;
4. ການຕອບໂຕ້ຕໍ່ເຫດການ;
5. ການຝຶກອົບຮົມ;
6. ການກວດສອບມາດຕະຖານ;

7. ການບໍລິການເຝົ້າລະວັງ ແລະ ຕິດຕາມ;

8. ການກູ້ຄືນຂໍ້ມູນ ແລະ ລະບົບ;

9. ການບໍລິການຄລາວດ້ານຄວາມປອດໄພ;

10. ທຸລະກິດອື່ນ ທີ່ກ່ຽວຂ້ອງກັບຄວາມປອດໄພໄຊເບີ.

ສຳລັບທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີແຕ່ລະປະເພດ ໄດ້ກຳນົດໄວ້ໃນລະບຽບການຕ່າງຫາກ.

ມາດຕາ 50 ການຂໍອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ຜູ້ມີຈຸດປະສົງດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ຕ້ອງແຈ້ງຂຶ້ນທະບຽນວິສາຫະກິດ ນຳຂະແໜງການອຸດສາຫະກຳ ແລະ ການຄ້າ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍວ່າດ້ວຍວິສາຫະກິດ ພາຍຫຼັງໄດ້ຮັບໃບທະບຽນວິສາຫະກິດແລ້ວ ໃຫ້ຂໍອະນຸຍາດດຳເນີນທຸລະກິດນຳກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ.

ມາດຕາ 51 ເງື່ອນໄຂການຂໍອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ການຂໍອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ມີເງື່ອນໄຂ ດັ່ງນີ້:

1. ມີໃບທະບຽນວິສາຫະກິດ;

2. ມີສຳນັກງານຕັ້ງຢູ່ ສປປ ລາວ ຢ່າງຖາວອນ ແລະ ຖືກຕ້ອງຕາມກົດໝາຍ;

3. ມີຜູ້ບໍລິຫານ ທີ່ມີປະສົບການກ່ຽວກັບວຽກງານເຕັກໂນໂລຊີ ຂໍ້ມູນ ຂ່າວສານ ຢ່າງໜ້ອຍ ສອງປີ;

4. ມີບຸກຄະລາກອນວິຊາການທີ່ຈົບການສຶກສາ ລະດັບຊັ້ນສູງຂຶ້ນໄປ ທາງດ້ານເຕັກໂນໂລຊີ ຂໍ້ມູນ ຂ່າວສານ ຫຼື ສາຂາທີ່ກ່ຽວຂ້ອງ;

5. ມີຖານະການເງິນໝັ້ນຄົງ ໂດຍມີການຢັ້ງຢືນຈາກຂະແໜງການທີ່ກ່ຽວຂ້ອງ;

6. ບໍ່ເຄີຍຖືກສານຕັດສິນລົງໂທດຕັດອິດສະລະພາບ ຍ້ອນການກະທຳຜິດໂດຍເຈດຕະນາ;

7. ມີລະບົບເຕັກນິກ ທີ່ຮັບປະກັນໃຫ້ແກ່ການດຳເນີນກິດຈະການ;

8. ເງື່ອນໄຂອື່ນ ທີ່ເຫັນວ່າມີຄວາມຈຳເປັນ.

ມາດຕາ 52 ເອກະສານປະກອບການຂໍອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ເອກະສານປະກອບການຂໍອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ມີ ດັ່ງນີ້:

1. ຄຳຮ້ອງຕາມແບບຟອມ ທີ່ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ກຳນົດ;

2. ສຳເນົາໃບທະບຽນວິສາຫະກິດ;

3. ກົດລະບຽບພາຍໃນຂອງວິສາຫະກິດ;

4. ສັນຍາຮ່ວມທຸລະກິດ (ຖ້າມີ);

5. ຊີວະປະຫວັດຫຍໍ້ ຂອງຜູ້ສ້າງຕັ້ງ;

6. ໃບຢັ້ງຢືນຖານະການເງິນ;

7. ບົດວິພາກເສດຖະກິດ-ເຕັກນິກ ແລະ/ຫຼື ແຜນດຳເນີນທຸລະກິດ;

8. ເອກະສານອື່ນ ທີ່ຈຳເປັນ.

ມາດຕາ 53 ການພິຈາລະນາອອກໃບອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຕ້ອງພິຈາລະນາອອກໃບອະນຸຍາດດຳເນີນທຸລະກິດຄວາມປອດໄພໄຊເບີ ພາຍໃນເວລາ ສິບຫ້າວັນ ນັບແຕ່ວັນ ໄດ້ຮັບຄຳຮ້ອງ ແລະ ເອກະສານປະກອບ ຖືກຕ້ອງ, ຄົບຖ້ວນ ແລະ ມີການປະສານສົມທົບກັບຂະແໜງການອື່ນທີ່ກ່ຽວຂ້ອງ. ໃນກໍລະນີບໍ່ສາມາດອອກໃບອະນຸຍາດດຳເນີນທຸລະກິດຄວາມປອດໄພໄຊເບີໄດ້ ກໍຕ້ອງແຈ້ງເຫດຜົນເປັນລາຍລັກອັກສອນ ໃຫ້ຜູ້ຂໍອະນຸຍາດພາຍໃນກຳນົດເວລາດັ່ງກ່າວ.

ມາດຕາ 54 ໃບອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ໃບອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ມີອາຍຸການນຳໃຊ້ ໜຶ່ງປີ ແລະ ສາມາດຕໍ່ໄດ້. ໃບອະນຸຍາດດຳເນີນທຸລະກິດ ບໍ່ສາມາດ ມອບ, ໂອນ, ເຊົ່າ ຫຼື ໃຫ້ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງອື່ນນຳໃຊ້.

ການຂໍຕໍ່ອາຍຸໃບອະນຸຍາດ ໃຫ້ຍື່ນຄຳຮ້ອງຂໍ ຕໍ່ກະຊວງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຢ່າງໜ້ອຍ ສາມສິບວັນ ກ່ອນວັນໝົດອາຍຸ ແລະ ຕ້ອງປະກອບເອກະສານ ດັ່ງນີ້:

1. ຄຳຮ້ອງຂໍຕໍ່ອາຍຸໃບອະນຸຍາດ;
2. ສຳເນົາໃບອະນຸຍາດດຳເນີນທຸລະກິດ;
3. ສຳເນົາໃບຢັ້ງຢືນການມອບພັນທະອາກອນ, ຄ່າທຳນຽມ ແລະ ຄ່າບໍລິການ;
4. ບົດລາຍງານການດຳເນີນທຸລະກິດຜ່ານມາ.

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ພິຈາລະນາຕໍ່ອາຍຸໃບອະນຸຍາດ ພາຍໃນເວລາ ສິບວັນ ນັບແຕ່ວັນ ໄດ້ຮັບຄຳຮ້ອງ ແລະ ເອກະສານປະກອບ ຖືກຕ້ອງ ແລະ ຄົບຖ້ວນ ເປັນຕົ້ນໄປ.

ມາດຕາ 55 ສິດ ຂອງຜູ້ດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ຜູ້ດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ມີສິດ ດັ່ງນີ້:

1. ໃຫ້ບໍລິການກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ຕາມທີ່ໄດ້ຮັບອະນຸຍາດ;
2. ເກັບຮັກສາຂໍ້ມູນຂອງຜູ້ໃຊ້ບໍລິການຢ່າງປອດໄພ, ປິດລັບ ແລະ ນຳໃຊ້ສະເພາະ ກ່ຽວກັບການບໍລິການຄວາມປອດໄພໄຊເບີ, ຍົກເວັ້ນກົດໝາຍໄດ້ກຳນົດໄວ້ເປັນຢ່າງອື່ນ;
3. ຜະລິດ, ນຳເຂົ້າ, ສົ່ງອອກ, ຈຳໜ່າຍ ແລະ ຕິດຕັ້ງອຸປະກອນຄວາມປອດໄພໄຊເບີ ຕາມປະເພດທຸລະກິດທີ່ໄດ້ຮັບອະນຸຍາດ;
4. ນຳໃຊ້ສະຖານທີ່ ແລະ ສິ່ງອຳນວຍຄວາມສະດວກອື່ນ ໃນການດຳເນີນທຸລະກິດ ຕາມກົດໝາຍ;
5. ສະເໜີຂໍນຳໃຊ້ໂຄງລ່າງພື້ນຖານໂທລະຄົມມະນາຄົມ ຈາກຜູ້ໃຫ້ບໍລິການໂທລະຄົມມະນາຄົມ;
6. ໂຈະ ຫຼື ຍົກເລີກ ການໃຫ້ບໍລິການແກ່ຜູ້ໃຊ້ບໍລິການ ທີ່ບໍ່ຊຳລະຄ່າບໍລິການ ຫຼື ລະເມີດກົດໝາຍ;
7. ໄດ້ຮັບການປົກປ້ອງສິດ ແລະ ຜົນປະໂຫຍດອັນຊອບທຳ ຕາມກົດໝາຍ;
8. ສະເໜີມາດຕະການປ້ອງກັນ ແລະ ແກ້ໄຂໄພຄຸກຄາມທາງໄຊເບີ ຕໍ່ພາກສ່ວນທີ່ກ່ຽວຂ້ອງ;
9. ແລກປ່ຽນຂໍ້ມູນກ່ຽວກັບໄພຄຸກຄາມທາງໄຊເບີ ກັບຜູ້ໃຫ້ບໍລິການອື່ນ ແລະ ອົງການທີ່ກ່ຽວຂ້ອງ;
10. ສະເໜີຂໍການຢັ້ງຢືນມາດຕະຖານການບໍລິການ;
11. ສະເໜີ ໂຈະ ຫຼື ຖອນ ໃບອະນຸຍາດດຳເນີນທຸລະກິດຂອງຕົນ;
12. ນຳໃຊ້ສິດອື່ນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ.

ມາດຕາ 56 ພັນທະ ຂອງຜູ້ດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ຜູ້ດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ມີພັນທະ ດັ່ງນີ້:

1. ສ້າງແຜນການດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີຂອງຕົນ ໃຫ້ສອດຄ່ອງກັບແຜນຍຸດທະສາດການພັດທະນາຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ ແລະ ແຜນພັດທະນາເສດຖະກິດດິຈິຕອນແຫ່ງຊາດ;

2. ຖ່າຍທອດຄວາມຮູ້ທາງດ້ານເຕັກໂນໂລຊີ ທີ່ນຳໃຊ້ໃນການໃຫ້ບໍລິການ ໃຫ້ແກ່ພະນັກງານ-ລັດຖະກອນຂອງຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ແລະ ບຸກຄະລາກອນຂອງຕົນ;

3. ຮັບປະກັນລະບົບເຕັກນິກຂອງຕົນ ໃຫ້ສາມາດເຊື່ອມຕໍ່ກັບລະບົບເຕັກນິກ ຂອງຜູ້ໃຫ້ບໍລິການໂທລະຄົມມະນາຄົມອື່ນ;

4. ໃຫ້ບຸລິມະສິດ ໃນການສະໜອງການບໍລິການຄວາມປອດໄພໄຊເບີ ແກ່ອົງການຈັດຕັ້ງຂອງລັດ;

5. ມີແຜນກູ້ຄືນລະບົບຄວາມປອດໄພໄຊເບີ ໃນກໍລະນີເກີດໄພພິບັດ, ເຫດການສຸກເສີນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍສະບັບນີ້;

6. ໃຫ້ການຮ່ວມມືກັບໜ່ວຍງານປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ;

7. ຮັບ, ພິຈາລະນາ ແລະ ແກ້ໄຂ ຄຳສະເໜີຂອງຜູ້ໃຊ້ບໍລິການຄວາມປອດໄພໄຊເບີ;

8. ປະຕິບັດພັນທະ ພາສີ, ອາກອນ, ຄ່າທຳນຽມ ແລະ ຄ່າບໍລິການ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ ແລະ ລະບຽບການທີ່ກ່ຽວຂ້ອງ;

9. ສະໜອງການເຊື່ອມຕໍ່ເຂົ້າກັບລະບົບເຕັກນິກຄວາມປອດໄພໄຊເບີຂອງລັດ ຕາມຄວາມຕ້ອງການຂອງວຽກງານໃນແຕ່ລະໄລຍະ;

10. ສ້າງລະບົບເກັບກຳ ແລະ ປົກປ້ອງ ຂໍ້ມູນຂອງຜູ້ໃຊ້ບໍລິການບໍ່ໃຫ້ຮົ່ວໄຫຼ ຕາມການກຳນົດຂອງກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ;

11. ອຳນວຍຄວາມສະດວກ ແກ່ຜູ້ໃຫ້ບໍລິການອື່ນ ທີ່ກ່ຽວຂ້ອງກັບລະບົບຄວາມປອດໄພຂອງຕົນ;

12. ແກ້ໄຂຜົນກະທົບ ແລະ ທົດແທນຄວາມເສຍຫາຍ ທີ່ເກີດຈາກການໃຫ້ບໍລິການຂອງຕົນ;

13. ລາຍງານປະຈຳປີກ່ຽວກັບສະຖານະພາບຄວາມປອດໄພໄຊເບີ ຂອງຕົນຕໍ່ໜ່ວຍງານຮັບຜິດຊອບຄວາມປອດໄພໄຊເບີ;

14. ປະຕິບັດພັນທະອື່ນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ.

ມາດຕາ 57 ການໂຈະການດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ການດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ຈະຖືກໂຈະ ໃນກໍລະນີ ດັ່ງນີ້:

1. ສະເໜີໂຈະ ໂດຍຜູ້ດຳເນີນທຸລະກິດ ຫຼື ມີການສະເໜີ ຂອງການຈັດຕັ້ງທີ່ກ່ຽວຂ້ອງ;

2. ດຳເນີນທຸລະກິດບໍ່ຖືກຕ້ອງຕາມຈຸດປະສົງ ແລະ ເປົ້າໝາຍ ທີ່ໄດ້ຮັບອະນຸຍາດ;

3. ບໍ່ລາຍງານການລະເມີດຄວາມປອດໄພຕໍ່ອົງການທີ່ກ່ຽວຂ້ອງ;

4. ບໍ່ຊຳລະອາກອນ, ຄ່າທຳນຽມ ແລະ ຄ່າບໍລິການ ຕາມກົດໝາຍ ແລະ ລະບຽບການທີ່ກ່ຽວຂ້ອງ;

5. ກໍລະນີອື່ນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ.

ກ່ອນການໂຈະການດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຕ້ອງແຈ້ງເຕືອນຜູ້ດຳເນີນທຸລະກິດ ເພື່ອປັບປຸງ ແລະ ແກ້ໄຂ.

ໃນກໍລະນີ ມີໄພຄຸກຄາມທາງໄຊເບີທີ່ຮ້າຍແຮງ ຕໍ່ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ, ຄວາມສະຫງົບ ແລະ ຄວາມເປັນລະບຽບຮຽບຮ້ອຍຂອງສັງຄົມ ຕ້ອງໂຈະໃບອະນຸຍາດທັນທີ ໂດຍບໍ່ຕ້ອງມີການແຈ້ງເຕືອນລ່ວງໜ້າ.

ມາດຕາ 58 ການຖອນໃບອະນຸຍາດການດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ໃບອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ຈະຖືກຖອນໃນກໍລະນີ ດັ່ງນີ້:

1. ບໍ່ ປັບປຸງ, ແກ້ໄຂ ຕາມຄຳສັ່ງໂຈະ;
2. ມີການສະເໜີ ຂອງຜູ້ດຳເນີນທຸລະກິດ ຫຼື ການຈັດຕັ້ງທີ່ກ່ຽວຂ້ອງ;
3. ນຳເອົາໃບອະນຸຍາດໃຫ້ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງອື່ນ ນຳໃຊ້, ເຊົ່າ ຫຼື ໂອນ;
4. ລະເມີດກົດໝາຍ, ລະບຽບການຢ່າງຮ້າຍແຮງ, ສ້າງຜົນເສຍຫາຍຢ່າງຫຼວງຫຼາຍຕໍ່ ເສດຖະກິດ-ສັງຄົມ ຂອງຊາດ, ວຽກງານປ້ອງກັນຊາດ-ປ້ອງກັນຄວາມສະຫງົບ ແລະ ຜົນປະໂຫຍດອັນຊອບທຳຂອງຜົນລະເມືອງ.

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຕ້ອງແຈ້ງເປັນລາຍລັກອັກສອນ ກ່ຽວກັບການຖອນໃບອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ໃຫ້ກະຊວງອຸດສາຫະກຳ ແລະ ການຄ້າ ພາຍໃນເວລາ ຫ້າວັນລັດຖະການ ນັບແຕ່ວັນຖອນໃບອະນຸຍາດດຳເນີນທຸລະກິດ ພ້ອມທັງເປີດເຜີຍຕໍ່ສາທາລະນະຊົນ ໂດຍຜ່ານພາຫະນະສື່ມວນຊົນ.

ພາກທີ VI
ການຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເບີ

ມາດຕາ 59 ການຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເບີ

ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທີ່ໃຫ້ບໍລິການ, ແຈກຢາຍ, ສະໜອງ ແລະ ເຜີຍແຜ່ຂໍ້ມູນຜ່ານລະບົບອິນເຕີເນັດ ຢູ່ ສປປ ລາວ ຕ້ອງຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເບີ ນຳກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເພື່ອຮັບປະກັນຄວາມປອດໄພ ແລະ ຄວາມໂປ່ງໃສ ເປັນຕົ້ນ ການປ້ອງກັນລະບົບ ແລະ ຂໍ້ມູນທີ່ສຳຄັນ, ການປົກປ້ອງຂໍ້ມູນຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ, ສິ່ງເສີມການພັດທະນາລະບົບນິເວດດິຈິຕອນທີ່ປອດໄພ.

ຄ່າທຳນຽມ ແລະ ຄ່າບໍລິການ ຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເບີ ໃຫ້ປະຕິບັດຕາມລະບຽບການ ກ່ຽວກັບ ຄ່າທຳນຽມ ແລະ ຄ່າບໍລິການ ທີ່ປະກາດໃຊ້ໃນແຕ່ລະໄລຍະ.

ມາດຕາ 60 ເປົ້າໝາຍທີ່ຕ້ອງຂຶ້ນທະບຽນ

ເປົ້າໝາຍທີ່ຕ້ອງຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເບີ ມີ ດັ່ງນີ້:

1. ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທີ່ໃຫ້ບໍລິການ, ແຈກຢາຍ, ສະໜອງ ແລະ ເຜີຍແຜ່ຂໍ້ມູນຜ່ານລະບົບອິນເຕີເນັດ ໂດຍບໍ່ຫວັງຜົນກຳໄລ ເປັນຕົ້ນ ການໃຫ້ບໍລິການຖານຂໍ້ມູນ, ການໃຫ້ບໍລິການລະບົບຄວາມປອດໄພໄຊເບີ;
2. ການໃຫ້ບໍລິການກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ເປັນຕົ້ນ ການໃຫ້ບໍລິການຝາກເວັບໄຊ, ການໃຫ້ບໍລິການລະບົບຊຳລະເງິນແບບດິຈິຕອນ, ການໃຫ້ບໍລິການໂທລະຄົມມະນາຄົມ.

ມາດຕາ 61 ຂໍ້ມູນຂອງເປົ້າໝາຍທີ່ຕ້ອງຂຶ້ນທະບຽນ

ຂໍ້ມູນຂອງເປົ້າໝາຍທີ່ຕ້ອງຂຶ້ນທະບຽນ ມີ ດັ່ງນີ້:

1. ຊື່ ແລະ ທີ່ຢູ່ ຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ;
2. ຂໍ້ມູນຕິດຕໍ່ພົວພັນ ຂອງຜູ້ຮັບຜິດຊອບດ້ານຄວາມປອດໄພໄຊເບີ;
3. ຂໍ້ມູນກ່ຽວກັບການເກັບຮັກສາ ແລະ ປະມວນຜົນຂໍ້ມູນ;
4. ປະເພດການໃຫ້ບໍລິການ, ແຈກຢາຍ, ເຜີຍແຜ່ຂໍ້ມູນ;
5. ຂໍ້ມູນອື່ນ ທີ່ເຫັນວ່າມີຄວາມຈຳເປັນ.

ມາດຕາ 62 ການພິຈາລະນາຂຶ້ນທະບຽນ

ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທີ່ໃຫ້ບໍລິການ, ແຈກຢາຍ, ສະໜອງ ແລະ ເຜີຍແຜ່ຂໍ້ມູນຜ່ານລະບົບອິນເຕີເນັດ ຕ້ອງຍື່ນຄຳຮ້ອງຂໍຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເບີ ຕໍ່ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ.

ພາຍຫຼັງ ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ໄດ້ຮັບຄຳຮ້ອງຂໍຂຶ້ນທະບຽນ ແລະ ຂໍ້ມູນຂອງເປົ້າໝາຍທີ່ຕ້ອງຂຶ້ນທະບຽນແລ້ວ ຕ້ອງກວດກາຄວາມຖືກຕ້ອງຂອງຂໍ້ມູນດັ່ງກ່າວ ເພື່ອພິຈາລະນາອອກໃບຢັ້ງຢືນການຂຶ້ນທະບຽນ ພາຍໃນເວລາ ສາມສິບວັນ. ໃນກໍລະນີຂໍ້ມູນຫາກບໍ່ຄົບຖ້ວນ ຕ້ອງແຈ້ງໃຫ້ຜູ້ຮ້ອງຂໍຂຶ້ນທະບຽນ ສະໜອງຂໍ້ມູນເພີ່ມເຕີມ ພາຍໃນເວລາ ສິບຫ້າວັນ.

ໃນກໍລະນີມີການປ່ຽນແປງຂໍ້ມູນທີ່ໄດ້ຂຶ້ນທະບຽນແລ້ວ ໃຫ້ຜູ້ທີ່ໄດ້ຂຶ້ນທະບຽນນັ້ນແຈ້ງເປັນລາຍລັກອັກສອນກ່ຽວກັບການປ່ຽນແປງຂໍ້ມູນດັ່ງກ່າວ ຕໍ່ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ພາຍໃນເວລາ ສິບຫ້າວັນ ນັບແຕ່ວັນປ່ຽນແປງຂໍ້ມູນ ເປັນຕົ້ນໄປ.

ພາກທີ VII
ຂໍ້ຫ້າມ

ມາດຕາ 63 ຂໍ້ຫ້າມທົ່ວໄປ

ຫ້າມ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ມີພຶດຕິກຳ ດັ່ງນີ້:

1. ດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
2. ເຈາະ, ເຂົ້າເຖິງລະບົບ, ເຄືອຂ່າຍ, ໂປຣແກຣມ ແລະ ຂໍ້ມູນ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
3. ສ້າງ, ແຈກຢາຍ, ນຳໃຊ້ມອນແວ, ໄວຣັສ ຫຼື ໂປຣແກຣມ ທີ່ເປັນອັນຕະລາຍຕໍ່ລະບົບດີຈີຕອນ;
4. ດັກສະກັດ, ປອມແປງ, ບິດເບືອນ ຫຼື ທຳລາຍ ຂໍ້ມູນສ່ວນຕົວຂອງບຸກຄົນອື່ນ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
5. ຂັດຂວາງ ຫຼື ລົບກວນການປະຕິບັດງານ ຂອງລະບົບ ຫຼື ເຄືອຂ່າຍ;
6. ນຳເຂົ້າ, ສົ່ງອອກ, ນຳໃຊ້ ອຸປະກອນ ຫຼື ເຕັກໂນໂລຊີ ດ້ານຄວາມປອດໄພໄຊເບີ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
7. ຊື້ ຂາຍ ຫຼື ແລກປ່ຽນຂໍ້ມູນສ່ວນຕົວຂອງບຸກຄົນອື່ນ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
8. ປະຕິເສດ ຫຼື ຫຼີກລ່ຽງການໃຫ້ຄວາມຮ່ວມມື ກັບອົງການທີ່ກ່ຽວຂ້ອງຂອງລັດ ໃນການສືບສວນ-ສອບສວນ ເຫດການໄພຄຸກຄາມຄວາມປອດໄພໄຊເບີ;
9. ມີພຶດຕິກຳອື່ນ ທີ່ເປັນການລະເມີດກົດໝາຍ.

ມາດຕາ 64 ຂໍ້ຫ້າມສຳລັບຜູ້ດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

ຫ້າມ ຜູ້ດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ມີພຶດຕິກຳ ດັ່ງນີ້:

1. ດຳເນີນທຸລະກິດບໍ່ຖືກຕ້ອງຕາມຈຸດປະສົງທີ່ໄດ້ຮັບອະນຸຍາດ;
2. ເປີດເຜີຍ, ນຳໃຊ້ ຂໍ້ມູນ ຂອງຜູ້ໃຊ້ບໍລິການ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
3. ເມີນເສີຍຕໍ່ການປະຕິບັດຕາມມາດຕະຖານຄວາມປອດໄພໄຊເບີ;
4. ປິດບັງ ຫຼື ເມີນເສີຍ ການລາຍງານການລະເມີດຄວາມປອດໄພໄຊເບີ ຕໍ່ອົງການທີ່ກ່ຽວຂ້ອງຂອງລັດ;
5. ປະຕິເສດການໃຫ້ບໍລິການ ໂດຍບໍ່ມີເຫດຜົນທີ່ໜັກແໜ້ນ ຫຼື ເລືອກປະຕິບັດຕໍ່ຜູ້ໃຊ້ບໍລິການ;
6. ສະໜອງ ຫຼື ລາຍງານ ຂໍ້ມູນກ່ຽວກັບຄວາມປອດໄພໄຊເບີ ໂດຍບໍ່ຖືກຕ້ອງ ຫຼື ບໍ່ຄົບຖ້ວນ ຕໍ່ອົງການທີ່ກ່ຽວຂ້ອງຂອງລັດ;
7. ມີພຶດຕິກຳອື່ນ ທີ່ເປັນການລະເມີດກົດໝາຍ.

ມາດຕາ 65 ຂໍ້ຫ້າມສຳລັບຜູ້ໃຊ້ບໍລິການ

ຫ້າມ ຜູ້ໃຊ້ບໍລິການຄວາມປອດໄພໄຊເບີ ມີພຶດຕິກຳ ດັ່ງນີ້:

1. ນຳໃຊ້ການບໍລິການຄວາມປອດໄພໄຊເບີ ໃນທາງທີ່ບໍ່ຖືກຕ້ອງຕາມກົດໝາຍ;
2. ບໍ່ປະຕິບັດຕາມເງື່ອນໄຂຂອງການນຳໃຊ້ ຕາມສັນຍາບໍລິການ;
3. ບໍ່ປະຕິບັດຕາມຄຳແນະນຳດ້ານຄວາມປອດໄພໄຊເບີ ຂອງຜູ້ດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ;
4. ເປີດເຜີຍຂໍ້ມູນກ່ຽວກັບຊ່ອງໂຫວ່ຂອງລະບົບຄອມພິວເຕີ ຂອງຜູ້ດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ;
5. ມີພຶດຕິກຳອື່ນ ທີ່ເປັນການລະເມີດກົດໝາຍ.

ມາດຕາ 66 ຂໍ້ຫ້າມສຳລັບພະນັກງານ-ລັດຖະກອນ ແລະ ເຈົ້າໜ້າທີ່ ທີ່ກ່ຽວຂ້ອງ

ຫ້າມ ພະນັກງານ-ລັດຖະກອນ ແລະ ເຈົ້າໜ້າທີ່ ທີ່ກ່ຽວຂ້ອງ ມີພຶດຕິກຳ ດັ່ງນີ້:

1. ສວຍໃຊ້ສິດ, ໜ້າທີ່, ຕຳແໜ່ງ, ເພື່ອຜົນປະໂຫຍດຂອງຕົນ, ຄອບຄົວ, ຍາດພີ່ນ້ອງ ແລະ ພັກພວກຂອງຕົນ ຊຶ່ງກໍ່ຄວາມເສຍຫາຍໃຫ້ແກ່ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ສັງຄົມ ແລະ ການຈັດຕັ້ງ;
2. ເປີດເຜີຍຂໍ້ມູນລັບທາງລັດຖະການ ຫຼື ຂໍ້ມູນຂອງຜູ້ດຳເນີນທຸລະກິດ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;
3. ກົດໜ່ວງ ຖ່ວງດຶງ, ປອມແປງເອກະສານ ກ່ຽວກັບຄວາມປອດໄພໄຊເບີ;
4. ເມີນເສີຍ ຕໍ່ການປະຕິບັດຕາມຂັ້ນຕອນ ແລະ ມາດຕະຖານຄວາມປອດໄພໄຊເບີ;
5. ເຂົ້າເຖິງຂໍ້ມູນ ຫຼື ລະບົບ ທີ່ຢູ່ໃນຄວາມຮັບຜິດຊອບ ບໍ່ຖືກຕ້ອງຕາມສິດ ແລະ ໜ້າທີ່ຂອງຕົນ;
6. ໃຊ້ອຸປະກອນ ຫຼື ຊອບແວ ທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດໃນການປະຕິບັດໜ້າທີ່;
7. ມີພຶດຕິກຳອື່ນ ທີ່ເປັນການລະເມີດກົດໝາຍ.

ພາກທີ VIII

ການຄຸ້ມຄອງ ແລະ ການກວດກາ ວຽກງານຄວາມປອດໄພໄຊເບີ

ໝວດທີ 1

ການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ

ມາດຕາ 67 ອົງການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ

ລັດຖະບານ ຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ ຢ່າງລວມສູນ ແລະ ເປັນເອກະພາບໃນຂອບເຂດທົ່ວປະເທດ ໂດຍມອບໃຫ້ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເປັນຜູ້ຮັບຜິດຊອບໂດຍກົງ ແລະ ເປັນເຈົ້າການປະສານສົມທົບກັບ ກະຊວງ, ອົງການ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ທີ່ກ່ຽວຂ້ອງ.

ອົງການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ ປະກອບດ້ວຍ:

1. ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ;
2. ພະແນກເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ນະຄອນຫຼວງ, ແຂວງ;
3. ຫ້ອງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເມືອງ, ນະຄອນ.

ເພື່ອຮັບປະກັນໃຫ້ວຽກງານຄວາມປອດໄພໄຊເບີ ໄດ້ດຳເນີນໄປຢ່າງມີປະສິດທິພາບ ແລະ ປະສິດທິຜົນນັ້ນ ອົງການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ ອາດມອບໃຫ້ຄະນະກຳມະການປົກຄອງຕາແສງ ຊ່ວຍໃນການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ ຕາມລະບຽບການໃນແຕ່ລະໄລຍະ.

ມາດຕາ 68 ສິດ ແລະ ໜ້າທີ່ ຂອງກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ

ໃນການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ມີ ສິດ ແລະ ໜ້າທີ່ ດັ່ງນີ້:

1. ຄົ້ນຄວ້າ ສ້າງ ແລະ ປັບປຸງ ນະໂຍບາຍ, ກົດໝາຍ, ແຜນຍຸດທະສາດ ແລະ ລະບຽບການ ກ່ຽວກັບ ວຽກງານຄວາມປອດໄພໄຊເບີ ເພື່ອສະເໜີລັດຖະບານ ພິຈາລະນາ;
2. ຜັນຂະຫຍາຍ ນະໂຍບາຍ, ກົດໝາຍ, ແຜນຍຸດທະສາດ ແລະ ລະບຽບການ ກ່ຽວກັບວຽກງານ ຄວາມປອດໄພໄຊເບີ ເປັນແຜນການ, ແຜນງານ, ໂຄງການ ແລະ ຈັດຕັ້ງປະຕິບັດ;
3. ໂຄສະນາ ເຜີຍແຜ່ ນະໂຍບາຍ, ກົດໝາຍ, ແຜນຍຸດທະສາດ ແລະ ລະບຽບການ ກ່ຽວກັບວຽກງານ ຄວາມປອດໄພໄຊເບີ;
4. ອອກ ຂໍ້ຕົກລົງ, ຄຳສັ່ງ, ຄຳແນະນຳ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;
5. ສ້າງ ແລະ ພັດທະນາ ມາດຕະຖານດ້ານຄວາມປອດໄພໄຊເບີ;
6. ຄຸ້ມຄອງ, ຕິດຕາມ ແລະ ກວດກາ ການຈັດຕັ້ງປະຕິບັດວຽກງານຄວາມປອດໄພໄຊເບີ ພ້ອມທັງແກ້ໄຂບັນຫາທີ່ເກີດຂຶ້ນ ໃນຂອບເຂດທົ່ວປະເທດ;
7. ສ້າງ ແລະ ຄຸ້ມຄອງ ລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ ໃຫ້ມີຄວາມພ້ອມດ້ານບຸກຄະລາກອນຊ່ຽວຊານ ແລະ ອຸປະກອນທີ່ທັນສະໄໝ;
8. ສະເໜີລັດຖະບານ ປະກາດພາວະສຸກເສີນທາງໄຊເບີ;
9. ຄົ້ນຄວ້າ ແລະ ພິຈາລະນາ ການຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເບີ;
10. ອອກ, ໂຈະ ຫຼື ຖອນໃບອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ;

11. ຄົ້ນຄວ້າ ການກຳນົດ, ປະເມີນ ຫຼື ທົບທວນ ໜ່ວຍງານໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສຳຄັນຂອງຊາດ ເພື່ອສະເໜີລັດຖະບານ ພິຈາລະນາ ໃນແຕ່ລະໄລຍະ;

12. ສ້າງ, ບຳລຸງ, ຍົກລະດັບ ແລະ ພັດທະນາ ບຸກຄະລາກອນ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

13. ຄົ້ນຄວ້າ, ພັດທະນາ ແລະ ນຳໃຊ້ເຕັກໂນໂລຊີດ້ານຄວາມປອດໄພໄຊເບີ;

14. ສ້າງຈິດສຳນຶກ ແລະ ຄວາມຮັບຮູ້ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ ໃຫ້ແກ່ສັງຄົມ;

15. ຮັບ, ພິຈາລະນາ ແລະ ແກ້ໄຂຄຳສະເໜີ ຂອງບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ກ່ຽວກັບວຽກ ງານຄວາມປອດໄພໄຊເບີ;

16. ປະສານສົມທົບກັບ ກະຊວງ, ອົງການ, ອົງການປົກຄອງທ້ອງຖິ່ນ ແລະ ພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

17. ພົວພັນ ແລະ ຮ່ວມມືກັບຕ່າງປະເທດ, ພາກພື້ນ ແລະ ສາກົນ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

18. ສະຫຼຸບ ແລະ ລາຍງານ ການເຄື່ອນໄຫວວຽກງານຄວາມປອດໄພໄຊເບີ ຕໍ່ລັດຖະບານ ຢ່າງເປັນ ປົກກະຕິ;

19. ນຳໃຊ້ສິດ ແລະ ປະຕິບັດໜ້າທີ່ອື່ນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ.

ມາດຕາ 69 ສິດ ແລະ ໜ້າທີ່ ຂອງພະແນກເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ນະຄອນຫຼວງ, ແຂວງ

ໃນການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ ພະແນກເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ນະຄອນຫຼວງ, ແຂວງ ມີ ສິດ ແລະ ໜ້າທີ່ ຕາມຂອບເຂດຄວາມຮັບຜິດຊອບຂອງຕົນ ດັ່ງນີ້:

1. ຈັດຕັ້ງປະຕິບັດ ນະໂຍບາຍ, ກົດໝາຍ, ແຜນຍຸດທະສາດ ແລະ ລະບຽບການ ກ່ຽວກັບວຽກງານຄວາມ ປອດໄພໄຊເບີ;

2. ໂຄສະນາ ເຜີຍແຜ່ ນະໂຍບາຍ, ກົດໝາຍ, ແຜນຍຸດທະສາດ ແລະ ລະບຽບການ ກ່ຽວກັບວຽກງານ ຄວາມປອດໄພໄຊເບີ;

3. ສ້າງແຜນການ ແລະ ໂຄງການລະອຽດ ເພື່ອຈັດຕັ້ງປະຕິບັດວຽກງານຄວາມປອດໄພໄຊເບີ;

4. ຄຸ້ມຄອງ, ຕິດຕາມ ແລະ ກວດກາ ການຈັດຕັ້ງປະຕິບັດວຽກງານຄວາມປອດໄພໄຊເບີ ພ້ອມທັງແກ້ ໄຂບັນຫາທີ່ເກີດຂຶ້ນ;

5. ປະສານສົມທົບກັບ ພະແນກ, ຫ້ອງການ ແລະ ພາກສ່ວນທີ່ກ່ຽວຂ້ອງກັບວຽກງານຄວາມປອດໄພ ໄຊເບີ;

6. ສົ່ງເສີມ ແລະ ສະໜັບສະໜູນ ການພັດທະນາບຸກຄະລາກອນ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

7. ສະເໜີບຳລຸງ, ຍົກລະດັບ ແລະ ພັດທະນາ ບຸກຄະລາກອນ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

8. ຮັບ ແລະ ຄົ້ນຄວ້າ ຄຳຮ້ອງຂໍ ຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເບີ ແລະ ໃບອະນຸຍາດດຳເນີນທຸລະກິດ ກ່ຽວກັບຄວາມປອດໄພໄຊເບີ;

9. ສະເໜີ ການຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເບີ;

10. ສະເໜີ ອອກ, ໂຈະ ຫຼື ຖອນໃບອະນຸຍາດດຳເນີນທຸລະກິດກ່ຽວກັບຄວາມປອດໄພໄຊເບີ;

11. ເກັບກຳ ແລະ ລາຍງານຂໍ້ມູນກ່ຽວກັບສະພາບການຄວາມປອດໄພໄຊເບີ;

12. ປະສານງານກັບໜ່ວຍງານຕອບໂຕ້ເຫດສຸກເສີນທາງຄອມພິວເຕີ ໃນກໍລະນີເກີດເຫດການສຸກເສີນ ທາງໄຊເບີ;

13. ໃຫ້ຄຳປຶກສາ ແລະ ຊ່ວຍເຫຼືອທາງດ້ານວິຊາການ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

14. ສ້າງຈິດສຳນຶກ ແລະ ຄວາມຮັບຮູ້ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ ໃຫ້ແກ່ສັງຄົມ;

15. ຮັບ, ພິຈາລະນາ ແລະ ແກ້ໄຂຄຳສະເໜີ ຂອງບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

16. ຕິດຕາມ ແລະ ປະເມີນຜົນການຈັດຕັ້ງປະຕິບັດໂຄງການຄວາມປອດໄພໄຊເບີ;

17. ພົວພັນ ແລະ ຮ່ວມມື ກັບຕ່າງປະເທດ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ ຕາມການມອບໝາຍ;

18. ສະຫຼຸບ ແລະ ລາຍງານ ການເຄື່ອນໄຫວ ວຽກງານຄວາມປອດໄພໄຊເບີ ຕໍ່ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ແລະ ຄະນະກຳມະການປົກຄອງ ນະຄອນຫຼວງ, ແຂວງ ຢ່າງເປັນປົກກະຕິ;

19. ນຳໃຊ້ສິດ ແລະ ປະຕິບັດໜ້າທີ່ອື່ນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ.

ມາດຕາ 70 ສິດ ແລະ ໜ້າທີ່ ຂອງຫ້ອງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເມືອງ, ນະຄອນ

ໃນການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ ຫ້ອງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ເມືອງ, ນະຄອນ ມີ ສິດ ແລະ ໜ້າທີ່ ຕາມຂອບເຂດຄວາມຮັບຜິດຊອບຂອງຕົນ ດັ່ງນີ້:

1. ຈັດຕັ້ງປະຕິບັດ ນະໂຍບາຍ, ກົດໝາຍ, ແຜນຍຸດທະສາດ ແລະ ລະບຽບການ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

2. ເຜີຍແຜ່ ນະໂຍບາຍ, ກົດໝາຍ, ແຜນຍຸດທະສາດ ແລະ ລະບຽບການ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

3. ສ້າງຈິດສຳນຶກ ແລະ ຄວາມຮັບຮູ້ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ ໃຫ້ແກ່ສັງຄົມ;

4. ຕິດຕາມ, ກວດກາ ແລະ ລາຍງານກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

5. ໃຫ້ຄຳແນະນຳກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

6. ເກັບກຳ ແລະ ສະໜອງຂໍ້ມູນ ຂອງຜູ້ໃຫ້ບໍລິການ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

7. ສະເໜີແຜນສ້າງ, ຍົກລະດັບ, ພັດທະນາບຸກຄະລາກອນ ໃນວຽກງານຄວາມປອດໄພໄຊເບີ;

8. ຮັບ, ພິຈາລະນາ ແລະ ແກ້ໄຂຄຳສະເໜີ ຂອງບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

9. ປະສານສົມທົບກັບຂະແໜງການ, ຫ້ອງການ ແລະ ພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

10. ສະຫຼຸບ ແລະ ລາຍງານ ການເຄື່ອນໄຫວວຽກງານຄວາມປອດໄພໄຊເບີ ຕໍ່ພະແນກເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ນະຄອນຫຼວງ, ແຂວງ ແລະ ຄະນະກຳມະການປົກຄອງ ເມືອງ, ນະຄອນ ຢ່າງເປັນປົກກະຕິ;

11. ນຳໃຊ້ສິດ ແລະ ປະຕິບັດໜ້າທີ່ອື່ນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນກົດໝາຍ.

ມາດຕາ 71 ສິດ ແລະ ໜ້າທີ່ ຂອງກະຊວງ, ອົງການ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ທີ່ກ່ຽວຂ້ອງ

ກະຊວງ, ອົງການ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ທີ່ກ່ຽວຂ້ອງ ມີ ສິດ ແລະ ໜ້າທີ່ ໃນການ ຄຸ້ມຄອງ, ຕິດຕາມ, ຮ່ວມມື ແລະ ປະສານສົມທົບກັບ ຂະແໜງການເຕັກໂນໂລຊີ ແລະ ການສື່ສານ, ຂະແໜງການປ້ອງກັນຊາດ-ປ້ອງກັນຄວາມສະຫງົບ ຂັ້ນຂອງຕົນ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ ຕາມພາລະບົດບາດ ແລະ ຂອບເຂດຄວາມຮັບຜິດຊອບຂອງຕົນ.

ໝວດທີ 2
ການກວດກາວຽກງານຄວາມປອດໄພໄຊເບີ

ມາດຕາ 72 ອົງການກວດກາວຽກງານຄວາມປອດໄພໄຊເບີ

ອົງການກວດກາວຽກງານຄວາມປອດໄພໄຊເບີ ປະກອບດ້ວຍ:

1. ອົງການກວດກາພາຍໃນ ຊຶ່ງແມ່ນ ອົງການດຽວກັນກັບອົງການຄຸ້ມຄອງວຽກງານຄວາມປອດໄພໄຊເບີ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນມາດຕາ 67 ຂອງກົດໝາຍສະບັບນີ້;

2. ອົງການກວດກາພາຍນອກ ຊຶ່ງແມ່ນ ສະພາແຫ່ງຊາດ, ສະພາປະຊາຊົນຂັ້ນແຂວງ, ອົງການກວດກາລັດແຕ່ລະຂັ້ນ, ອົງການກວດສອບແຫ່ງລັດ, ແນວລາວສ້າງຊາດ, ສະຫະພັນນັກຮົບເກົ່າລາວ, ອົງການຈັດຕັ້ງມະຫາຊົນ ແລະ ສື່ມວນຊົນ.

ມາດຕາ 73 ເນື້ອໃນການກວດກາ

ການກວດກາວຽກງານຄວາມປອດໄພໄຊເບີ ມີເນື້ອໃນ ດັ່ງນີ້:

1. ການຈັດຕັ້ງປະຕິບັດ ນະໂຍບາຍ, ກົດໝາຍ, ແຜນຍຸດທະສາດ ແລະ ລະບຽບການ ກ່ຽວກັບວຽກງານຄວາມປອດໄພໄຊເບີ;

2. ການໃຫ້ບໍລິການ ວຽກງານຄວາມປອດໄພໄຊເບີ;

3. ການນຳໃຊ້ສິດ ແລະ ປະຕິບັດໜ້າທີ່ ຂອງພະນັກງານ-ລັດຖະກອນ ແລະ ເຈົ້າໜ້າທີ່ ທີ່ກ່ຽວຂ້ອງ;

4. ເນື້ອໃນອື່ນ ທີ່ເຫັນວ່າມີຄວາມສຳຄັນ ແລະ ຈຳເປັນ.

ມາດຕາ 74 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 IX
ນະໂຍບາຍຕໍ່ຜູ້ມີຜົນງານ ແລະ ມາດຕະການຕໍ່ຜູ້ລະເມີດ

ມາດຕາ 75 ນະໂຍບາຍຕໍ່ຜູ້ມີຜົນງານ

ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ທີ່ມີຜົນງານດີເດັ່ນໃນການຈັດຕັ້ງປະຕິບັດກົດໝາຍສະບັບນີ້ ຈະໄດ້ຮັບການຍ້ອງຍໍ ຫຼື ນະໂຍບາຍອື່ນ ຕາມລະບຽບການ.

ມາດຕາ 76 ມາດຕະການຕໍ່ຜູ້ລະເມີດ

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

ພາກທີ X

ບົດບັນຍັດສຸດທ້າຍ

ມາດຕາ 77 ງົບປະມານ

ງົບປະມານ ນຳໃຊ້ເຂົ້າໃນວຽກງານຄວາມປອດໄພໄຊເບີ ແມ່ນ ງົບປະມານຂອງລັດ, ກອງທຶນພັດທະນາ ໂທລະຄົມມະນາຄົມ ແລະ ການຫັນເປັນດິຈິຕອນ, ການຊ່ວຍເຫຼືອ ແລະ ການປະກອບສ່ວນຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທັງພາຍໃນ ແລະ ຕ່າງປະເທດ ແລະ ລາຍຮັບອື່ນ ທີ່ຖືກຕ້ອງຕາມກົດໝາຍ.

ມາດຕາ 78 ການຈັດຕັ້ງປະຕິບັດ

ລັດຖະບານ ແຫ່ງ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ ເປັນຜູ້ຈັດຕັ້ງປະຕິບັດກົດໝາຍສະບັບນີ້.

ມາດຕາ 79 ຜົນສັກສິດ

ກົດໝາຍສະບັບນີ້ ມີຜົນສັກສິດ ນັບແຕ່ວັນທີ 1 ກັນຍາ 2025 ພາຍຫຼັງປະທານປະເທດ ແຫ່ງ ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ ອອກລັດຖະດຳລັດປະກາດໃຊ້ ແລະ ໄດ້ລົງຈົດໝາຍເຫດທາງ ລັດຖະການ ເປັນຕົ້ນໄປ.

ປະທານສະພາແຫ່ງຊາດ

ປອ ໄຊສົມພອນ ພົມວິຫານ