



ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ
ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ

ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ

ເລກທີ 2126 /ປທສ
ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ 08 ສິງຫາ 2018

ຄໍາແນະນໍາ

ການຈັດຕັ້ງປະຕິບັດ ກົດໝາຍວ່າດ້ວຍ ການປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ

- ອີງຕາມ ກົດໝາຍວ່າດ້ວຍ ການປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ, ສະບັບເລກທີ 25/ສພຊ, ລົງວັນທີ 12 ພຶດສະພາ 2017.
- ອີງຕາມ ດໍາລັດຂອງນາຍົກລັດຖະມົນຕີ ສະບັບເລກທີ 22/ນຍ, ລົງວັນທີ 16 ມັງກອນ 2017 ວ່າດ້ວຍ ການຈັດຕັ້ງ ແລະ ເຄື່ອນໄຫວ ຂອງ ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ.

ລັດຖະມົນຕີ ອອກຄໍາແນະນໍາ:

I. ຈຸດປະສົງ

ຄໍາແນະນໍາສະບັບນີ້ ຜັນຂະຫຍາຍ ແລະ ແນະນໍາການຈັດຕັ້ງປະຕິບັດ ເນື້ອໃນບາງຂໍ້ໃນບາງມາດຕາຂອງກົດໝາຍວ່າດ້ວຍ ການປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ, ສະບັບເລກທີ 25/ສພຊ, ລົງວັນທີ 12 ພຶດສະພາ 2017 ເພື່ອເຮັດໃຫ້ເນື້ອໃນຂອງກົດໝາຍດັ່ງກ່າວ ມີຄວາມລະອຽດ ແລະ ຈະແຈ້ງຂຶ້ນຕື່ມ ໂດຍການອະທິບາຍເພີ່ມຕື່ມບັນດາເນື້ອໃນທີ່ມີລັກສະນະເຕັກນິກວິຊາການ ພ້ອມທັງຍົກຕົວຢ່າງປະກອບໃຫ້ເຂົ້າໃຈໄດ້ງ່າຍໃນການນໍາໃຊ້ ແນໃສ່ເຮັດໃຫ້ການຈັດ ຕັ້ງປະຕິບັດກົດໝາຍໃຫ້ຖືກຕ້ອງ, ມີປະສິດທິພາບ, ປະສິດທິຜົນ ແລະ ມີຄວາມເປັນເອກະພາບໃນຂອບເຂດທົ່ວປະເທດ.

II. ອະທິບາຍເພີ່ມຕື່ມເນື້ອໃນຄໍາສັບບາງມາດຕາ

1. ມາດຕາ 8 ຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນຂໍ້ຄວາມທີ່ເປັນຕົວເລກ, ຕົວອັກສອນ, ຮູບພາບເໜັງຕີງ, ຮູບພາບບໍ່ເໜັງຕີງ, ສຽງ, ວິດີໂອ ແລະ ອື່ນໆ ທີ່ເກັບຮັກສາໄວ້ໃນຮູບແບບເອເລັກໂຕຣນິກ ປະກອບມີຂໍ້ມູນຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ, ຄວາມລັບ, ຄວາມໝັ້ນຄົງ, ຂໍ້ມູນທີ່ເປັນລິຂະສິດ ແລະ ຂໍ້ມູນອື່ນໆ. ຂໍ້ມູນດັ່ງກ່າວນີ້ ມີທັງຂໍ້ມູນທີ່ສາມາດເປີດເຜີຍໄດ້ ເອີ້ນວ່າ ຂໍ້ມູນທົ່ວໄປ ແລະ ຂໍ້ມູນທີ່ບໍ່ສາມາດເປີດເຜີຍໄດ້ ເອີ້ນວ່າ ຂໍ້ມູນສະເພາະ.

ດັ່ງນັ້ນ, ໃນກົດໝາຍວ່າດ້ວຍ ການປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ ຈຶ່ງໄດ້ຕົກລົງເຫັນດີເປັນເອກະພາບກັບທຸກຂະແໜງການ ໃຫ້ປະກອບມີ ສອງ ປະເພດ ຄື: ຂໍ້ມູນທົ່ວໄປ ແລະ ຂໍ້ມູນສະເພາະ.

2. ມາດຕາ 9 ຂໍ້ມູນທົ່ວໄປ ແມ່ນ ຂໍ້ມູນຂອງບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ທີ່ສາມາດເຂົ້າເຖິງ, ນໍາໃຊ້ ແລະ ເປີດເຜີຍໄດ້ ແຕ່ຕ້ອງບອກແຫຼ່ງຂໍ້ມູນທີ່ໄດ້ມາໃຫ້ຖືກຕ້ອງ. ✓

ຕົວຢ່າງ: ຂໍ້ມູນຂອງບຸກຄົນ ເຊັ່ນ: ຊື່, ຕໍາແໜ່ງ, ທີ່ຢູ່, ໝາຍເລກໂທລະສັບ, ທີ່ຢູ່ທາງຈົດໝາຍເອເລັກໂຕຣນິກ, ຂໍ້ມູນຂອງການຈັດຕັ້ງ, ຂໍ້ມູນສະຖິຕິທົ່ວໄປ, ບົດຄວາມເຜີຍແຜ່ທາງດ້ານວິຊາການ ແລະ ອື່ນໆ.

3. ມາດຕາ 10 ຂໍ້ມູນສະເພາະ ແມ່ນ ຂໍ້ມູນທີ່ບໍ່ອະນຸຍາດໃຫ້ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ເຂົ້າເຖິງ, ນຳໃຊ້ ຫຼື ເປີດເຜີຍຖ້າຫາກບໍ່ໄດ້ຮັບອະນຸຍາດຈາກເຈົ້າຂອງຂໍ້ມູນ ຫຼື ການຈັດຕັ້ງທີ່ກ່ຽວຂ້ອງ.

ຕົວຢ່າງ: ຂໍ້ມູນຂອງລູກຄ້າ, ຂໍ້ມູນທາງການເງິນ, ຊີວະປະຫວັດສ່ວນຕົວ, ປະຫວັດການປົ່ນປົວສຸຂະພາບ, ເຊື້ອຊາດ, ສາສະໜາ, ແຜນໂຄງການ, ແຜນງົບປະມານ, ຄວາມລັບທາງລັດຖະການ ແລະ ອື່ນໆ.

4. ມາດຕາ 11 ວຽກງານປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການນຳໃຊ້ວິທີການ ແລະ ມາດຕະການ ເພື່ອປ້ອງກັນຂໍ້ມູນທີ່ຄຸ້ມຄອງ ແລະ ເກັບຮັກສາໄວ້ໃນຮູບແບບເອເລັກໂຕຣນິກ ບໍ່ໃຫ້ມີການເຂົ້າເຖິງ, ນຳໃຊ້, ເປີດເຜີຍ, ດັດແປງ, ສິ່ງ, ໂອນ ຫຼື ທຳລາຍ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.

5. ມາດຕາ 12 ການເກັບກຳຂໍ້ມູນ ແມ່ນ ການລວບລວມຂໍ້ມູນໄວ້ໃນຄັງຂໍ້ມູນ ຫຼື ຖານຂໍ້ມູນ ເພື່ອສະດວກໃນການເຂົ້າເຖິງ, ກວດກາ ແລະ ນຳໃຊ້ ໃຫ້ມີຄວາມປອດໄພ ບົນພື້ນຖານການເຫັນດີເປັນເອກະພາບ ລະຫວ່າງ ຜູ້ຄຸ້ມຄອງຂໍ້ມູນ ແລະ ເຈົ້າຂອງຂໍ້ມູນ ຊຶ່ງຕ່າງຝ່າຍຕ່າງໄດ້ຮັບຜົນປະໂຫຍດ.

ຕົວຢ່າງ: ທະນາຄານໃດໜຶ່ງ ຕ້ອງການເກັບກຳຂໍ້ມູນບັນຊີທຸລະກຳທາງການເງິນຂອງ ທ້າວ ກໍ ທະນາຄານດັ່ງກ່າວ ຕ້ອງແຈ້ງໃຫ້ ທ້າວ ກໍ ຮັບຊາບກ່ຽວກັບ ຈຸດປະສົງ, ລາຍລະອຽດຂໍ້ມູນທີ່ຕ້ອງການເກັບກຳ ເປັນຕົ້ນ ຊື່ ແລະ ນາມສະກຸນ, ວັນເດືອນປີເກີດ, ເພດ, ທີ່ຢູ່ອາໄສ, ອາຊີບ, ໝາຍເລກໂທລະສັບ ແລະ ເງື່ອນໄຂການຮັບຝາກຂອງທະນາຄານວາງອອກ.

6. ມາດຕາ 13 ການກວດກາຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການກວດກາລາຍລະອຽດຕ່າງໆຂອງຂໍ້ມູນ ເພື່ອຮັບປະກັນວ່າຂໍ້ມູນດັ່ງກ່າວຖືກຕ້ອງ, ໜ້າເຊື່ອຖື, ບໍ່ຂັດກັບກົດໝາຍ ແລະ ລະບຽບການ ພ້ອມທັງຮັບປະກັນໃຫ້ສາມາດນຳໃຊ້ທັນກັບສະພາບການ ເຊັ່ນ: ຂໍ້ມູນທີ່ໄດ້ມາຕ້ອງຖືກຕ້ອງ, ຄົບຖ້ວນ, ສົມບູນ, ບໍ່ມີການດັດແກ້, ປ່ຽນແປງ, ປອມແປງ, ສູນເສຍ, ເສຍຫາຍບາງສ່ວນ ຫຼື ທັງໝົດ ແລະ ຖືກສ້າງຂຶ້ນໃໝ່.

ຕົວຢ່າງ: ທ້າວ ກໍ ຕ້ອງການຝາກຂໍ້ມູນໄວ້ໃນສູນໃຫ້ບໍລິການຮັບຝາກຂໍ້ມູນໃດໜຶ່ງ ຈະຕ້ອງລະບຸ ແລະ ກວດກາຂໍ້ມູນຂອງຕົນໃຫ້ລະອຽດ ກ່ອນຈະມອບໃຫ້ຜູ້ຄຸ້ມຄອງຂໍ້ມູນກວດສອບວ່າ ຖືກຕ້ອງຕາມລະບຽບ ແລະ ເງື່ອນໄຂຂອງຂັ້ນຕອນການຮັບຝາກ.

7. ມາດຕາ 14 ການຝາກຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການນຳເອົາຂໍ້ມູນໃນຮູບແບບເອເລັກໂຕຣນິກທີ່ເປັນຕົວເລກ, ຕົວອັກສອນ, ຮູບພາບເໜັງຕີງ, ຮູບພາບບໍ່ເໜັງຕີງ, ສຽງ, ວິດີໂອ ແລະ ອື່ນໆ ໄປຝາກໄວ້ນຳຜູ້ຄຸ້ມຄອງຂໍ້ມູນ ໂດຍການປະຕິບັດຕາມສັນຍາຂອງສອງຝ່າຍ ເພື່ອຮັບປະກັນໃຫ້ຂໍ້ມູນດັ່ງກ່າວມີຄວາມປອດໄພ, ຖືກຕ້ອງ ແລະ ສອດຄ່ອງກັບກົດໝາຍວ່າດ້ວຍ ການປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ.

8. ມາດຕາ 15 ການເກັບຮັກສາຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການຄຸ້ມຄອງ ແລະ ຮັກສາຂໍ້ມູນ ເພື່ອຮັບປະກັນໃຫ້ຂໍ້ມູນມີຄວາມປອດໄພ, ບໍ່ໃຫ້ສູນເສຍ, ເສຍຫາຍພ້ອມທັງເຮັດໃຫ້ມີຄວາມສະດວກວ່າໄວໃນການເຂົ້າເຖິງ ແລະ ໃຊ້ງານ.

ຜູ້ຄຸ້ມຄອງຂໍ້ມູນ ຕ້ອງມີການກຳນົດມາດຕະການ ແລະ ວິທີການເກັບຮັກສາທີ່ປອດໄພ ເຊັ່ນ: ສ້າງລາຍການເກັບຮັກສາຂໍ້ມູນເອເລັກໂຕຣນິກທີ່ສາມາດກວດເບິ່ງໄດ້ງ່າຍ, ການຈັດລະດັບຄວາມປອດໄພຂອງຂໍ້ມູນ, ການກຳນົດສິດການເຂົ້າເຖິງຂໍ້ມູນ, ກຳນົດໄລຍະເວລາໃນການເກັບຮັກສາຂໍ້ມູນ, ການສຳຮອງຂໍ້ມູນ ແລະ ອື່ນໆ. ✓

ຕົວຢ່າງ: ສູນໃຫ້ບໍລິການຮັບຝາກຂໍ້ມູນໃດໜຶ່ງ ຕ້ອງເກັບຮັກສາຂໍ້ມູນ ຂອງ ທ້າວ ກໍ ເຊັ່ນ: ປະຫວັດການ ໂທລະສັບ ຫຼື ການສົ່ງຂໍ້ມູນຜ່ານຈົດໝາຍເອເລັກໂຕຣນິກ ຢ່າງໜ້ອຍ 90 ວັນ, ຫຼັງຈາກໝົດກຳນົດເວລາຂໍ້ມູນຂອງ ທ້າວ ກໍ ອາດຈະຖືກລຶບຖິ້ມ, ປົດກັ້ນການເຂົ້າເຖິງ ຫຼື ປະຕິບັດຕາມສັນຍາຂອງທັງສອງຝ່າຍ.

9. ມາດຕາ 16 ການນຳໃຊ້ ຫຼື ເປີດເຜີຍຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການນຳເອົາຂໍ້ມູນອອກມານຳໃຊ້ ຫຼື ເປີດເຜີຍໃຫ້ແກ່ບຸກຄົນທີສາມ ເພື່ອຕອບສະໜອງຕາມຄວາມຮຽກຮ້ອງຕ້ອງການຂອງວຽກງານ ຊຶ່ງຕ້ອງໄດ້ຮັບການ ເຫັນດີຈາກເຈົ້າຂອງຂໍ້ມູນ ເວັ້ນເສຍແຕ່ມີການສະເໜີຈາກອົງການຈັດຕັ້ງລັດທີ່ມີສິດອຳນາດກ່ຽວຂ້ອງ.

ຕົວຢ່າງ: ທ້າວ ກໍ ໄດ້ກະທຳຜິດຖານສໍ້ໂກງຊັບພິນລະເມືອງ ໂດຍການໂທລະສັບຕົວະຍິວະຫຼອກລວງໃຫ້ບຸກຄົນອື່ນ ຈ່າຍເງິນໃຫ້ຕົນ ຊຶ່ງເຮັດໃຫ້ບຸກຄົນອື່ນໄດ້ຮັບຄວາມເສຍຫາຍ. ໃນກໍລະນີດັ່ງກ່າວ ຫາກມີການສະເໜີຂໍ້ມູນການໂທ ລະສັບຈາກອົງການຈັດຕັ້ງລັດທີ່ມີສິດອຳນາດກ່ຽວຂ້ອງ ເພື່ອຂໍຂໍ້ມູນຂອງ ທ້າວ ກໍ, ຜູ້ຄຸ້ມຄອງຂໍ້ມູນ ຕ້ອງສະໜອງຂໍ້ມູນ ຕາມທີ່ໄດ້ສະເໜີມາ ໂດຍບໍ່ຈຳເປັນຕ້ອງແຈ້ງໃຫ້ ທ້າວ ກໍ ຮັບຊາບ.

10. ມາດຕາ 17 ການສົ່ງ ຫຼື ໂອນຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການສົ່ງຂໍ້ມູນຈາກຕົ້ນທາງໄປຫາປາຍທາງທີ່ໄດ້ ກຳນົດໄວ້ ໂດຍຜ່ານອຸປະກອນເອເລັກໂຕຣນິກ ຫຼື ເຄື່ອງຄອມພິວເຕີ ໃນການຖ່າຍໂອນ ເຊັ່ນ: ການສົ່ງຂໍ້ມູນຜ່ານ ທາງເຄືອຂ່າຍອິນເຕີເນັດ, ອຸປະກອນບັນທຶກຂໍ້ມູນ ແລະ ອື່ນໆ ໂດຍປະຕິບັດຕາມເງື່ອນໄຂທີ່ໄດ້ຕົກລົງກັນ ລະຫວ່າງ ຜູ້ຮັບ ແລະ ຜູ້ສົ່ງ ເພື່ອຮັບປະກັນໃຫ້ຂໍ້ມູນມີຄວາມປອດໄພ, ຖືກຕ້ອງ ແລະ ບໍ່ຂັດກັບກົດໝາຍ.

ຕົວຢ່າງ 1: ສູນໃຫ້ບໍລິການຮັບຝາກຂໍ້ມູນໃດໜຶ່ງ ຕ້ອງການໂອນຂໍ້ມູນຂອງ ທ້າວ ກໍ ໄປໃຫ້ ທ້າວ ຂໍ ສູນໃຫ້ບໍ ລິການຮັບຝາກຂໍ້ມູນດັ່ງກ່າວ ຕ້ອງໄດ້ຮັບອະນຸຍາດຈາກ ທ້າວ ກໍ ເສຍກ່ອນ ຈຶ່ງສາມາດສົ່ງ ຫຼື ໂອນ ຂໍ້ມູນດັ່ງກ່າວໄດ້.

ຕົວຢ່າງ 2: ທ້າວ ກໍ ຕ້ອງການສົ່ງຂໍ້ມູນທີ່ສຳຄັນ ເປັນຕົ້ນ ຂໍ້ມູນທຸລະກຳທາງການເງິນ, ການທະນາຄານ, ການ ລົງທຶນ ແລະ ການບັນຊີ ຜ່ານທາງຈົດໝາຍເອເລັກໂຕຣນິກ (ອີເມວ) ໄປຫາ ທ້າວ ຂໍ ເພື່ອຮັບປະກັນໃຫ້ຂໍ້ມູນມີຄວາມ ປອດໄພ, ຖືກຕ້ອງ ແລະ ຄົບຖ້ວນ ທ້າວ ກໍ ຕ້ອງເຂົ້າລະຫັດຄວາມປອດໄພຂໍ້ມູນກ່ອນຈະສົ່ງໄປຫາ ທ້າວ ຂໍ.

11. ມາດຕາ 18 ການເຂົ້າເຖິງຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການເຂົ້າເຖິງ ຂໍ້ມູນທົ່ວໄປ ຫຼື ຂໍ້ມູນສະເພາະ ເພື່ອນຳ ໃຊ້ ແລະ ເປີດເຜີຍ ຕາມຄວາມຮຽກຮ້ອງຕ້ອງການຂອງວຽກງານ.

ໃນກໍລະນີ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ມີຈຸດປະສົງຢາກເຂົ້າເຖິງຂໍ້ມູນສະເພາະ ຕ້ອງສະເໜີຕໍ່ຜູ້ຄຸ້ມຄອງຂໍ ມູນທີ່ກ່ຽວຂ້ອງ ຄົ້ນຄວ້າ, ຜິຈາລະນາ ຕາມກົດໝາຍ ແລະ ລະບຽບການ.

12. ມາດຕາ 19 ການປັບປຸງ ຫຼື ແກ້ໄຂຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການດັດແກ້ ຫຼື ປ່ຽນແປງ ຈາກຂໍ້ມູນເດີມ ເພື່ອເຮັດໃຫ້ຂໍ້ມູນໄດ້ຮັບການປັບປຸງໃຫ້ຖືກຕ້ອງ ແລະ ສອດຄ່ອງ ຕາມການສະເໜີຂອງເຈົ້າຂອງຂໍ້ມູນ.

ຕົວຢ່າງ: ທ້າວ ກໍ ຕ້ອງການປັບປຸງ ຫຼື ແກ້ໄຂ ຂໍ້ມູນຂອງຕົນ ເຊັ່ນ: ທີ່ຢູ່, ໝາຍເລກໂທລະສັບ, ຂະໜາດຂອງຂໍ້ມູນ ແລະ ອື່ນໆ. ທ້າວ ກໍ ຕ້ອງໄດ້ສະເໜີຫາ ຜູ້ຄຸ້ມຄອງຂໍ້ມູນ ຜິຈາລະນາແກ້ໄຂ ຫຼື ສະໜອງວິທີການໃຫ້ແກ້ ທ້າວ ກໍ ເພື່ອ ໃຫ້ສາມາດປັບປຸງ ແລະ ແກ້ໄຂຂໍ້ມູນດ້ວຍຕົນເອງ.

13. ມາດຕາ 20 ການລຶບຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການທຳລາຍຂໍ້ມູນ ອອກຈາກອຸປະກອນເອເລັກໂຕຣນິກ ຫຼື ລະບົບຖານຂໍ້ມູນ.

ຕົວຢ່າງ: ທ້າວ ກໍ ຕ້ອງການລຶບຂໍ້ມູນທີ່ບໍ່ຕ້ອງການນຳໃຊ້ ທ້າວ ກໍ ຕ້ອງສະເໜີໃຫ້ຜູ້ຄຸ້ມຄອງຂໍ້ມູນ ລຶບ ຫຼື ທຳ ລາຍຂໍ້ມູນຂອງຕົນ ອອກຈາກລະບົບຖານຂໍ້ມູນ.

ໃນກໍລະນີ ທີ່ຂໍ້ມູນ ໝົດອາຍຸການເກັບກຳ, ເກັບຮັກສາ ແລະ ສົ່ນສຸດການນຳໃຊ້ ຜູ້ຄຸ້ມຄອງຂໍ້ມູນ ມີສິດລຶບ ຫຼື ທຳ ລາຍ ຂໍ້ມູນອອກຈາກລະບົບຖານຂໍ້ມູນ ແຕ່ຕ້ອງແຈ້ງໃຫ້ເຈົ້າຂອງຂໍ້ມູນຮັບຊາບ. ✓

ໃນກໍລະນີ ທີ່ຂໍ້ມູນຂອງ ທ້າວ ກໍ ຫາກກະທົບເຖິງຄວາມໝັ້ນຄົງຂອງຊາດ, ຄວາມສະຫງົບ, ຄວາມເປັນລະ

ບຽບຮຽບຮ້ອຍຂອງສັງຄົມ, ວັດທະນະທຳ ແລະ ຮີດຄອງປະເພນີອັນດີງາມຂອງຊາດ ຫຼື ຂໍ້ມູນທີ່ໃສ່ຮ້າຍປ້າຍສີຜູ້ອື່ນ ຜູ້ຖືກຄອງຂໍ້ມູນ ຕ້ອງລຶບ ຫຼື ທຳລາຍ ຂໍ້ມູນຕາມການສະເໜີຂອງເຈົ້າໜ້າທີ່ ຫຼື ບຸກຄົນ ທີ່ກ່ຽວຂ້ອງ.

14. ມາດຕາ 21 ມາດຕະການປ້ອງກັນຂໍ້ມູນເອເລັກໂຕຣນິກ ແມ່ນ ການກຳນົດວິທີການ, ຂໍ້ກຳນົດ ແລະ ລະບຽບການສະເພາະໃນການປ້ອງກັນຂໍ້ມູນເອເລັກໂຕຣນິກ ເພື່ອຮັບປະກັນຄວາມປອດໄພຂໍ້ມູນ ເຊັ່ນ: ການຈັດ ລະດັບຄວາມປອດໄພຂໍ້ມູນທາງລັດຖະການ, ການເກັບຮັກສາ, ການເຂົ້າເຖິງ, ການເຂົ້າລະຫັດຄວາມປອດໄພ ແລະ ການຕອບໂຕ້ການບຸກລຸກຂໍ້ມູນ.

15. ມາດຕາ 22 ການຈັດລະດັບຄວາມປອດໄພຂໍ້ມູນທາງລັດຖະການ ແມ່ນ ການກຳນົດລະດັບຄວາມສຳຄັນ ຂອງຂໍ້ມູນ ເພື່ອໃຫ້ສາມາດຈຳແນກ ແລະ ຈັດການກັບຂໍ້ມູນທີ່ຖືກທຳລາຍ ຫຼື ຖືກເປີດເຜີຍ ໃຫ້ທັນກັບສະພາບການ. ການຈັດລະດັບຄວາມປອດໄພຂໍ້ມູນທາງລັດຖະການ ມີ ດັ່ງນີ້:

15.1 ລະດັບ ໜຶ່ງ ເມື່ອຂໍ້ມູນຖືກທຳລາຍ ຫຼື ຖືກເປີດເຜີຍ ເຮັດໃຫ້ສິດ ແລະ ຜົນປະໂຫຍດຂອງລັດ, ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ຖືກເສຍຫາຍ ເປັນຕົ້ນ ຂໍ້ມູນຂອງລູກຄ້າ, ຂໍ້ມູນທາງການເງິນ, ຊີວະປະຫວັດສ່ວນຕົວ, ປະຫວັດການປົນປົວສຸຂະພາບ, ການເຄື່ອນໄຫວໃນຂະບວນການຕ່າງໆ ແລະ ອື່ນໆ;

15.2 ລະດັບ ສອງ ເມື່ອຂໍ້ມູນຖືກທຳລາຍ ຫຼື ຖືກເປີດເຜີຍ ເຮັດໃຫ້ສິດ ແລະ ຜົນປະໂຫຍດຂອງລັດ, ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ຖືກເສຍຫາຍຢ່າງຮ້າຍແຮງ ຫຼື ສ້າງຜົນກະທົບໃຫ້ແກ່ຜົນປະໂຫຍດສ່ວນລວມ ເປັນຕົ້ນ ເຊື້ອຊາດ, ສາສະໜາ, ຂໍ້ມູນຊັບສິນທາງປັນຍາ, ຂໍ້ມູນການວິໄຈທາງການແພດ, ງານວິໄຈດ້ານວິທະຍາສາດ, ການປະ ມຸນໂຄງການຕ່າງໆ, ຂໍ້ມູນການດຳເນີນໂຄງການ, ງົບປະມານໂຄງການ, ການກວດສອບໂຄງການ ແລະ ອື່ນໆ;

16. ມາດຕາ 24 ຄວາມປອດໄພໃນການເຂົ້າເຖິງຂໍ້ມູນ ແມ່ນ ການປະຕິບັດຕາມ ມາດຕະການ, ລະບຽບການ ຫຼື ນະໂຍບາຍ ໃນການເຂົ້າເຖິງຂໍ້ມູນໃຫ້ມີຄວາມປອດໄພ ເຊັ່ນ: ການກຳນົດ ສິດ, ຂັ້ນຕອນ, ວິທີການເຂົ້າເຖິງ ແລະ ບັນ ທຶກປະຫວັດການ ເຂົ້າ-ອອກ ລະບົບຢ່າງລະອຽດ.

ໃນກໍລະນີ ຂໍ້ມູນມີການປ່ຽນແປງ, ແກ້ໄຂ, ສຸນເສຍ ຫຼື ເສຍຫາຍ ຕ້ອງສາມາດກວດສອບຄືນຝາຍຫຼັງໄດ້ຢ່າງ ວ່ອງໄວ ແລະ ທັນກັບສະພາບການ. ນອກຈາກນີ້, ເຈົ້າຂອງຂໍ້ມູນ ຕ້ອງຮັບປະກັນບໍ່ໃຫ້ລະຫັດຜ່ານຂອງຕົນຮົ່ວໄຫຼ ເພື່ອ ບໍ່ໃຫ້ຜູ້ອື່ນນຳໄປໃຊ້.

17. ມາດຕາ 25 ການເຂົ້າລະຫັດຄວາມປອດໄພ ແມ່ນ ການຮັກສາຄວາມລັບຂອງຂໍ້ມູນ ໂດຍການໃສ່ລະຫັດຂໍ້ ມູນ ເພື່ອປ້ອງກັນບໍ່ໃຫ້ຂໍ້ມູນຖືກ ເຂົ້າເຖິງ, ອ່ານ, ທຳລາຍ, ນຳໃຊ້, ເປີດເຜີຍ, ສົ່ງ, ໂອນ, ປັບປຸງ, ລຶບ, ປ່ຽນແປງ ແລະ ກະທຳອື່ນໆ ທີ່ກໍ່ໃຫ້ເກີດຄວາມເສຍຫາຍ.

ຕົວຢ່າງ: ຜູ້ຖືກຄອງຂໍ້ມູນ ຕ້ອງນຳໃຊ້ໃບຮັບຮອງເອເລັກໂຕຣນິກ (Certificate Authority) ໃສ່ລະບົບໃຫ້ ບໍລິການຂໍ້ມູນຂ່າວສານ, ການເຂົ້າລະຫັດໃນຮູບແບບ PGP (Pretty Good Privacy) ເພື່ອສົ່ງ ຫຼື ໂອນ ຂໍ້ມູນ ເອເລັກໂຕຣນິກທີ່ສຳຄັນ ຝ່ານທາງຈິດໝາຍເອເລັກໂຕຣນິກ (ອີເມວ), ການເຂົ້າລະຫັດຝາຍຂໍ້ມູນເອເລັກໂຕຣນິກ ໃນຮູບແບບປົກກະຕິ ແລະ ຮູບແບບອື່ນ ໃຫ້ຖືກຕ້ອງຕາມມາດຕະຖານດ້ານຄວາມປອດໄພ.

ສຳລັບ ການເຂົ້າລະຫັດຄວາມປອດໄພຂໍ້ມູນ ລາຍລະອຽດໄດ້ລະບຸໄວ້ໃນ ຄຳແນະນຳກ່ຽວກັບ ການຮັກສາ ຄວາມປອດໄພທາງລະບົບຄອມພິວເຕີ. ✓

18. ມາດຕາ 26 ການຕອບໂຕ້ການບຸກລຸກຂໍ້ມູນ ແມ່ນ ການກວດສອບ ແລະ ລວບລວມຂໍ້ມູນ, ຫຼືກຖານກ່ຽວກັບການບຸກລຸກ ພ້ອມທັງປະສານງານກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ເພື່ອລະງັບ ແລະ ແກ້ໄຂເຫດການໃຫ້ທັນການ.

ໃນກໍລະນີ ໄດ້ຮັບແຈ້ງເຫດຈາກບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ຜູ້ຄຸ້ມຄອງຂໍ້ມູນ ຕ້ອງຮີບຮ້ອນກວດສອບ, ວິເຄາະ, ຈັດການ, ແກ້ໄຂ, ແຈ້ງເຕືອນ ແລະ ກຳນົດແນວທາງການປ້ອງກັນຕ່າງໆ ເພື່ອບໍ່ໃຫ້ເກີດການບຸກລຸກຂໍ້ມູນອີກ. ຜູ້ຄຸ້ມຄອງຂໍ້ມູນ ຕ້ອງແຈ້ງເຫດສຸກເສີນຫາ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີຂອງ ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ເພື່ອເກັບກຳຂໍ້ມູນ, ປະສານງານ ແລະ ດຳເນີນການແກ້ໄຂໃຫ້ທັນການ.

19. ມາດຕາ 31 ຂໍ້ຫ້າມທົ່ວໄປ ແມ່ນ ການກຳນົດລະບຽບການ ເພື່ອຫ້າມ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ມີພິດຕິກຳທີ່ເປັນການລະເມີດກົດໝາຍ ແລະ ລະບຽບການ, ຂໍ້ຫ້າມທົ່ວໄປ ມີ ດັ່ງນີ້:

19.1 ສິ່ງຂໍ້ມູນເອເລັກໂຕຣນິກທີ່ບໍ່ມີແຫຼ່ງທີ່ມາ, ໂປຣແກຣມອັນຕະລາຍ, ໄວຣັດ ຊຶ່ງໝາຍເຖິງການສົ່ງຂໍ້ມູນເອເລັກໂຕຣນິກ ທີ່ບໍ່ລະບຸຂໍ້ມູນຂອງ ຜູ້ສົ່ງ, ເນື້ອໃນ ຫຼື ຂໍ້ມູນອ້າງອີງທີ່ບໍ່ໜ້າເຊື່ອຖື ລວມທັງລິ້ງເວັບໄຊທີ່ຄັດຕິດມາ ທີ່ເປັນການຫຼອກລວງເອົາຂໍ້ມູນສ່ວນຕົວ, ໂປຣແກຣມອັນຕະລາຍ ຫຼື ການແຜ່ກະຈາຍໄວຣັດ ແລະ ອື່ນໆ ຊຶ່ງອາດຈະສົ່ງຜົນກະທົບແກ່ລະບົບຄອມພິວເຕີ;

19.2 ສ້າງຂໍ້ມູນເອເລັກໂຕຣນິກປອມ ຫຼື ຂໍ້ມູນທີ່ເປັນອັນຕະລາຍ ແລະ ສ້າງຄວາມເສຍຫາຍໃຫ້ຜູ້ອື່ນ ຊຶ່ງໝາຍເຖິງການສ້າງຂໍ້ມູນຂຶ້ນມາໃໝ່ ທີ່ບໍ່ເປັນຄວາມຈິງ ຫຼື ບິດເບືອນໄປຈາກຂໍ້ມູນເດີມ ໂດຍວິທີການໃຊ້ ໂປຣແກຣມຄອມພິວເຕີ ຫຼື ສະມາດໂຟນ ເປັນຕົ້ນ Photoshop, Illustator, ໂປຣແກຣມ Photo Editor, video editor ຕ່າງໆ ເພື່ອຕັດຕໍ່ ຮູບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອ ຫຼື ການໂຄສະນາຊວນເຊື່ອ. ການໃສ່ໄວຣັດໃນຂໍ້ມູນເອເລັກໂຕຣນິກ ເປັນຕົ້ນ ຝ່າຍເອກະສານ (Word, Excel, PDF ແລະ ອື່ນໆ) ໄປສ້າງຄວາມເສຍໃຫ້ຜູ້ອື່ນ;

19.3 ສວຍໃຊ້ຊ່ອງວ່າງ ຫຼື ຈຸດອ່ອນຂອງລະບົບຂໍ້ມູນ ເພື່ອ ເຂົ້າເຖິງ, ເກັບກຳ, ນຳໃຊ້ ແລະ ເປີດເຜີຍ ຂໍ້ມູນເອເລັກໂຕຣນິກ ເຊັ່ນ: ການສວຍໃຊ້ໂອກາດທາງດ້ານເຕັກນິກ ແລະ ນິຕິກຳ ເປັນຕົ້ນ ການເຫັນຊ່ອງໂຫວ່ຂອງລະບົບ ກຳຄື ໂປຣແກຣມມີຂໍ້ບົກຜ່ອງ, ຊອບແວທີ່ບໍ່ສົມບູນ ຫຼື ບໍ່ໄດ້ຮັບການປັບປຸງ, ການຕັ້ງຄ່າຂອງລະບົບຜິດພາດ ບໍ່ຖືກຕ້ອງຕາມມາດຕະຖານທີ່ກຳນົດໄວ້, ມາດຕະການການເຂົ້າເຖິງບໍ່ຮັດກຸມ ແລະ ອື່ນໆ;

20. ມາດຕາ 32 ຂໍ້ຫ້າມສຳລັບເຈົ້າຂອງຂໍ້ມູນ ແມ່ນ ການກຳນົດລະບຽບການ ເພື່ອຫ້າມເຈົ້າຂອງຂໍ້ມູນ ມີພິດຕິກຳທີ່ເປັນການລະເມີດກົດໝາຍ ແລະ ລະບຽບການ, ຂໍ້ຫ້າມສຳລັບເຈົ້າຂອງຂໍ້ມູນ ມີ ດັ່ງນີ້:

20.1 ບຸກລຸກ ຫຼື ກະທຳສິ່ງໃດໜຶ່ງ ເຮັດໃຫ້ການປະຕິບັດງານຂອງລະບົບຄວາມປອດໄພຂໍ້ມູນ ບໍ່ສາມາດເຮັດວຽກໄດ້ ເປັນຕົ້ນ ການຮ່ວມມືກັບພາກສ່ວນອື່ນ ເພື່ອໂຈມຕີລະບົບຄອມພິວເຕີ ໃນສູນໃຫ້ບໍລິການຮັບຝາກຂໍ້ມູນດ້ວຍວິທີການທາງດ້ານເຕັກນິກ ເຊັ່ນ: DDoS attack, ການກະຈາຍເມົາແວໃນລະບົບຄອມພິວເຕີ ແລະ ອື່ນໆ;

21. ມາດຕາ 54 ມາດຕະການທາງອາຍາ ແມ່ນ ບຸກຄົນ ທີ່ລະເມີດກົດໝາຍວ່າດ້ວຍ ການປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ ຊຶ່ງເປັນການກະທຳຜິດທາງອາຍາ ຈະຖືກລົງໂທດ ຕາມກົດໝາຍອາຍາ, ກົດໝາຍວ່າດ້ວຍ ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ຊຶ່ງລະບຸໄວ້ໃນ ມາດຕາ 62 ຫຼື ກົດໝາຍອື່ນໆກ່ຽວຂ້ອງ ແລ້ວແຕ່ລະກໍລະນີເບົາ ຫຼື ໜັກ. ✓

III. ການຈັດຕັ້ງປະຕິບັດ

ມອບໃຫ້ ສຸນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ ປະສານສົມທົບກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ຈັດຕັ້ງໂຄສະນາ, ເຜີຍແຜ່, ແນະນຳ ແລະ ປະຕິບັດຄຳແນະນຳສະບັບນີ້ໃຫ້ໄດ້ຮັບຜົນດີ.

ບັນດາກະຊວງ, ອົງການທຽບເທົ່າກະຊວງ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ, ບຸກຄົນ, ນິຕິບຸກຄົນ ພາຍໃນ ສປປ ລາວ ຈົ່ງຮັບຮູ້ ແລະ ນຳໄປຈັດຕັ້ງປະຕິບັດໃຫ້ຖືກຕ້ອງ.

IV. ຜົນສັກສິດ

ຄຳແນະນຳສະບັບນີ້ ມີຜົນສັກສິດແຕ່ວັນລົງລາຍເຊັນ ແລະ ພາຍຫຼັງທີ່ໄດ້ລົງໃນຈົດໝາຍເຫດທາງລັດຖະການ ສືບທຳວັນ. ✓

ລັດຖະມົນຕີ



ປອ. ທັນສະໄໝ ກິມມະສິດ