ສຳລັບ ວິສາຫະກິດຂະໜາດນ້ອຍຫາກາງ ແລະ ຜູ້ດຳເນີນທຸລະກິດຂະໜາດນ້ອຍ

ປະເມີນຄວາມປອດໄພຂໍ້ມູນຂ່າວສານ ຂອງບໍລິສັດດ້ວຍຕົນເອງ ພາຍໃນ 5 ນາທີ

ທ່ານຮູ້ບໍ່? ແນວໂນ້ມຄວາມປອດໄພຂໍ້ມູນຂ່າວສານ

ການປ່ຽນແປງຂອງໄພຄຸກຄາມ ແລະ ຮູບແບບການໂຈມຕີ

- ແຣນຊຳແວ (ມັນແວຮຽກຄ່າໄຖ່)
- ການເຈາະລະຫັດຜ່ານ
- ການໂຈມຕີອີເມວທີ່ເປັນເປົ້າໝາຍ

ການປ່ຽນແປງຂອງສະພາບແວດລ້ອມໄອຊີທີ

- ຄລາວ (ລະບົບຝາກຂໍ້ມູນອອນລາຍ)
- ແທັບເລັດ
- ສະມາດໂຟນ

ນຳໃຊ້ **“ໃບປະເມີນຄວາມປອດໄພຂໍ້ມູນຂ່າວສານ ຂອງບໍລິສັດດ້ວຍຕົນເອງ ພາຍໃນ 5 ນາທີ”**
ເພື່ອກວດກາເບິ່ງສະພາບຄວາມປອດໄພຂອງບໍລິສັດ
ກ່ອນທີ່ຈະສູນເສຍຂໍ້ມູນໄປ!

ASEAN · JAPAN
Cybersecurity Cooperation

ປະເມີນຕົນເອງ

1 ກະລຸນາອ່ານຂໍ້ມູນຕໍ່ໄປນີ້ ກ່ອນເຮັດການປະເມີນ

ວິທີການນຳໃຊ້

ພວກເຮົາໄດ້ແນໃສ່ 25 ມາດຕະການດ້ານຄວາມປອດໄພຂອງຂໍ້ມູນຂ່າວສານທີ່ມີປະສິດທິພາບ ແລະ ນຳໃຊ້ງົບປະມານເລັກນ້ອຍໃນການຈັດຕັ້ງປະຕິບັດສຳລັບອົງກອນ.
ກະລຸນາກວດເບິ່ງສະຖານະພາບຂອງລາຍການເຫຼົ່ານີ້ ແລະ ຈັດຕັ້ງປະຕິບັດບັນດາມາດຕະການຕ່າງໆທີ່ຍັງບໍ່ໄດ້ດຳເນີນການ ໃນຂະນະທີ່ອ້າງອີງເຖິງການອະທິບາຍໃນໃບແຜ່ນພັບນີ້.

ວິທີການອ່ານຄຳອະທິບາຍ

ກະລຸນາ ຕັດສິນໃຈ ໂດຍບໍ່ຈຳເປັນອີງໃສ່ຕົວຢ່າງຂອງຄຳອະທິບາຍ ເຊັ່ນ:
ຄຳຖາມທີ 16 ກ່ຽວກັບ “ມາດຕະການປ້ອງກັນການລັກຂະໂມຍ” ຄຳຖາມມີຢູ່ວ່າ ຖ້າອົງກອນຂອງທ່ານໃຊ້ແລັບທັອບ ທ່ານໄດ້ດຳເນີນການຕາມຂັ້ນຕອນເພື່ອປ້ອງກັນການລັກຂະໂມຍ ໂດຍການນຳເອົາແລັບທັອບໄວ້ໃນລິ້ນຊັກຕູ້ ຫຼື ບໍ່.
ຄຳຖາມຍັງຖາມອີກວ່າ ຫາກອົງກອນຂອງທ່ານບໍ່ມີແລັບທັອບ ທ່ານໄດ້ດຳເນີນຕາມຂັ້ນຕອນເພື່ອປ້ອງກັນການລັກຂະໂມຍ ໂດຍການບໍ່ວາງອຸປະກອນເສີມ ເຊັ່ນ USB ຫຼື ອຸປະກອນບັນທຶກຂໍ້ມູນພາຍນອກ (External Hard Drive) ໄວ້ເທິງໜ້າໂຕະ ຫຼື ບໍ່. ຖ້າຫາກ ທ່ານບໍ່ເຂົ້າໃຈຈຸດປະສົງຂອງຄຳຖາມ ຫຼື ເຫັນວ່າເຂົ້າໃຈຍາກ ໃຫ້ອີງໃສ່ແຜ່ນພັບດັ່ງກ່າວ.

ຈຸດປະສົງ ແລະ ຜົນປະໂຫຍດທີ່ຈະໄດ້ຮັບ

- ໃບປະເມີນຜົນນີ້ ຈະເຮັດໃຫ້ທ່ານເຂົ້າໃຈບັນຫາຕ່າງໆທີ່ອາດຈະມີຢູ່.
- ເມື່ອເຂົ້າໃຈເຖິງບັນຫາ, ທ່ານສາມາດຊອກຫາວິທີການແກ້ໄຂໃນຂັ້ນຕອນຕໍ່ໄປໄດ້.

ຖ້າຫາກ ບໍລິສັດຂອງທ່ານ ບໍ່ໄດ້ນຳໃຊ້ລາຍການໃດໜຶ່ງ

ບາງລາຍການລຸ່ມນີ້ ອາດຈະບໍ່ສາມາດນຳໃຊ້ກັບບໍລິສັດຂອງທ່ານ ຂຶ້ນກັບປະເພດທຸລະກິດ. ໃນກໍລະນີນັ້ນ, ໃຫ້ໝາຍວົງມົນ “ໄດ້ຈັດຕັ້ງປະຕິບັດແລ້ວ”

- No.4 ເຄືອຂ່າຍໄດ້ເຊື່ອມຕໍ່ເຂົ້າກັບເຄື່ອງສຳເນົາເອກະສານ ແລະ ອຸປະກອນບັນທຶກຂໍ້ມູນ (Hard Drive).
- No.5 ການບໍລິການເວັບໄຊ.
- No.9 ເຄືອຂ່າຍແບບໄຮ້ສາຍ.
- No.23 ການບໍລິການຄລາວ (Cloud Services)

ຖ້າຫາກທ່ານຄິດວ່າ, “ພວກເຮົາບໍ່ມີ ‘ຂໍ້ມູນທີ່ເປັນຄວາມລັບ’, ລາຍການຕ່າງໆລຸ່ມນີ້ ແມ່ນສິ່ງທີ່ເປັນຄວາມລັບ!

- ທີ່ຢູ່ຂອງພະນັກງານ ແລະ ໃບຈ່າຍເງິນເດືອນ
- ຂໍ້ມູນກ່ຽວກັບການເຮັດທຸລະກຳ ແລະ ການຊຳລະເງິນ ສຳລັບແຕ່ລະຄູ່ຮ່ວມທຸລະກິດ
- ຂໍ້ມູນການບັນຊີຂອງອົງກອນທ່ານ
- ລາຍຊື່ຂໍ້ມູນຕິດຕໍ່ຂອງຄູ່ຮ່ວມທຸລະກິດ ແລະ ລູກຄ້າ
- ຂໍ້ມູນການພັດທະນາ ເຊັ່ນ ຮູບແຕ້ມອອກແບບສຳລັບຜະລິດຕະພັນໃໝ່
- ຂໍ້ມູນອື່ນໆຈາກຄູ່ຮ່ວມທຸລະກິດທີ່ຕ້ອງໄດ້ຈັດການຢ່າງລະມັດລະວັງ

ມີຂໍ້ມູນທີ່ຕ້ອງໄດ້ຄຸ້ມຄອງຈັດການ ທີ່ເປັນຄວາມລັບໃນກຸ່ມຂໍ້ມູນພື້ນຖານຂອງອົງກອນ. ທ່ານຕ້ອງໄດ້ຢືນຢັນ ແລະ ຈັດປະເພດຂໍ້ມູນທີ່ມີຢູ່ໃນບໍລິສັດຂອງທ່ານທີ່ເປັນຄວາມລັບ. ການຈັດປະເພດຂໍ້ມູນແມ່ນຂັ້ນຕອນທຳອິດຂອງການຮັກສາຄວາມປອດໄພຂອງຂໍ້ມູນ.

2 ກະລຸນາຕອບ 25 ຄຳຖາມ ໃນໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ

ຖ້າຫາກ ທ່ານໄດ້ 100 ຄະແນນເຕັມ	ມາດຕະການຄວາມປອດໄພຂັ້ນພື້ນຖານຂອງທ່ານ ແມ່ນສົມບູນແບບແລ້ວ. ໃຫ້ສືບຕໍ່ວາງມາດຕະການຂອງທ່ານ ໃນລະດັບຕໍ່ໄປ.
ຖ້າຫາກ ທ່ານໄດ້ 70-99 ຄະແນນ	ຂ້ອນຂ້າງສົມບູນແບບ ແຕ່ອາດຈະມີບາງສ່ວນຂອງມາດຕະການທີ່ຍັງບໍ່ຄົບຖ້ວນ.
ຖ້າຫາກ ທ່ານໄດ້ 50-69 ຄະແນນ	ມີບາງສ່ວນທີ່ພົ້ນເດັ່ນ ແຕ່ອາດຈະຍັງບໍ່ມີມາດຕະການພຽງພໍ.
ຖ້າຫາກ ທ່ານໄດ້ 49 ຄະແນນ	ເປັນເລື່ອງປົກກະຕິ ທີ່ຈະມີເຫດການ ເຊັ່ນ ການຮົ່ວໄຫຼຂອງຂໍ້ມູນເກີດຂຶ້ນ.

ບັນດາມາດຕະການທີ່ໄດ້ອະທິບາຍໄວ້ ໃນໃບປະເມີນຂອງບໍລິສັດດ້ວຍຕົນເອງ ແມ່ນລະບຸໄວ້ດັ່ງຕໍ່ໄປນີ້:

■ ຜູ້ບໍລິຫານ (ຜູ້ຕາງໜ້າ) ສາມາດສັ່ງການໂດຍກົງ ແລະ ຢືນຢັນວ່າ ບັນດາມາດຕະການທາງດ້ານນະໂຍບາຍ ແມ່ນຖືກຈັດຕັ້ງປະຕິບັດແລ້ວ.
■ ພະນັກງານທຸກຄົນຮູ້ຈັກເຊິ່ງກັນ ແລະ ກັນ.
■ ບໍລິສັດ ບໍ່ໄດ້ເປັນເຈົ້າຂອງເຊີເວີ ຫຼື ອຸປະກອນເຄືອຂ່າຍທີ່ຕ້ອງການການຕັ້ງຄ່າທີ່ມີຄວາມສັບຊ້ອນໃນບໍລິສັດ.
- ເວັບໄຊຂອງບໍລິສັດ ບໍ່ໄດ້ໃຊ້ເຊີເວີ ທີ່ເຊື່ອມຕໍ່ເຂົ້າກັບອິນເຕີເນັດໂດຍກົງ ເຊັ່ນ ການນຳໃຊ້ບໍລິການຄລາວ (Cloud Services).
- ບໍ່ມີ ແອັບພິເຄຊັ່ນ ຊ໋ອບແວ ທີ່ພັດທະນາໂດຍບໍລິສັດ ແລະ ນຳໃຊ້ ສະເພາະແອັບພິເຄຊັ່ນ ຊ໋ອບແວ ທີ່ມີຂາຍທົ່ວໄປເທົ່ານັ້ນ.
- ຄອມພິວເຕີສ່ວນບຸກຄົນ ໄດ້ຮັບອະນຸຍາດໃຫ້ນຳໃຊ້ໄດ້ສະເພາະເມື່ອມີການນຳໃຊ້ ມາດຕະການດຽວກັນສຳລັບຄອມພິວເຕີທີ່ເປັນຂອງບໍລິສັດ.

ປະເມີນຕົນເອງ

ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ ພາຍໃນ 5 ນາທີ

ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ ເພື່ອລະບຸບັນດາມາດຕະການຮັກສາຄວາມປອດໄພຂອງຂໍ້ມູນຂ່າວສານທີ່ທ່ານຄວນໃຫ້ຄວາມສຳຄັນໃນຖານະເປັນອົງກອນ.

- ກະລຸນາອ່ານ 1 ໃນໜ້າກ່ອນໜ້ານີ້ ກ່ອນເຮັດການປະເມີນນີ້.
- ອ່ານລາຍການຕ່າງໆໃນການປະເມີນຜົນລຸ່ມນີ້ ແລະ ໝາຍວົງມົນໃນຖັນທີ່ເໝາະສົມ.
- ໃບປະເມີນນີ້ ຕ້ອງໄດ້ຕື່ມຂໍ້ມູນໃສ່ ໂດຍຜູ້ບໍລິຫານລະດັບສູງ ຫຼື ຜູ້ຈັດການ.
- ກະລຸນາຕອບວ່າ ລາຍການທີ່ລະບຸດ້ວຍ ຖືກຈັດຕັ້ງປະຕິບັດ ໂດຍພະນັກງານທຸກຄົນ ຫຼື ບໍ່. ຖ້າຫາກວ່າ ລາຍການໃດໜຶ່ງຖືກຈັດຕັ້ງປະຕິບັດ ສະເພາະແຕ່ພະນັກງານບາງຄົນເທົ່ານັ້ນ, ໃຫ້ເລືອກ “ໄດ້ຈັດຕັ້ງປະຕິບັດບາງສ່ວນ.” ກະລຸນາຕອບວ່າ ລາຍການທີ່ລະບຸດ້ວຍ ຖືກຈັດຕັ້ງປະຕິບັດໂດຍບໍລິສັດຂອງທ່ານ.
- ເພີ່ມຄະແນນຂອງທ່ານໃນດ້ານລຸ່ມຂອງໜ້າເຈ້ຍ ແລະ ສືບຕໍ່ອ່ານ 2 ໃນໜ້າກ່ອນນີ້.

ອົງກອນ: _____

ຜູ້ຕອບ: _____

ວັນທີ: _____

ລາຍການການປະເມີນຜົນ	ລຳດັບ	ຄຳອະທິບາຍ	ຄຳຕອບ: ໄດ້ຈັດຕັ້ງປະຕິບັດ	ໄດ້ຈັດຕັ້ງປະຕິບັດບາງສ່ວນ	ບໍ່ໄດ້ຈັດຕັ້ງປະຕິບັດ	ບໍ່ຮູ້
ພາກທີ 1 ມາດຕະການພື້ນຖານ	1	ທ່ານໄດ້ປ້ອງກັນລະບົບປະຕິບັດການ ແລະ ຊ່ອມແວ ດ້ວຍການອັບເດດ ວິນໂດ ເປັນປະຈຳ (Windows Update)*1 ຫຼື ນຳໃຊ້ມາດຕະການອື່ນໆ ບໍ?	4	2	0	0
	2	ທ່ານໄດ້ຈັດຕັ້ງປະຕິບັດມາດຕະການ ເພື່ອປ້ອງກັນຄອມພິວເຕີສ່ວນຕົວ (PC) ຂອງທ່ານ ຈາກໄວຣັດ ເຊັ່ນ ການຕິດຕັ້ງຊ່ອມແວປ້ອງກັນໄວຣັດ ແລະ ອັບເດດ ໄຟລ໌ທີ່ໃຊ້ກວດສອບໄວຣັດ (Virus Definiton File)?*2	4	2	0	0
	3	ທ່ານໄດ້ຕັ້ງລະຫັດຜ່ານທີ່ຍາກຕໍ່ການຄາດເດົາ ແລະ ບໍ່ໃຊ້ລະຫັດຜ່ານ ເຊັ່ນ ຊື່, ໝາຍເລກໂທລະສັບ ຫຼື ວັນເດືອນປີເກີດຂອງທ່ານ ແລະ ທ່ານບໍ່ໄດ້ນຳໃຊ້ລະຫັດຜ່ານດຽວໃນຫຼາຍໆເວັບໄຊທີ່ໃຫ້ບໍລິການບໍ?	4	2	0	0
	4	ທ່ານໄດ້ຈຳກັດການເຂົ້າເຖິງຂໍ້ມູນຂ່າວສານທີ່ສຳຄັນຢ່າງເໝາະສົມ ເຊັ່ນ ການຈຳກັດການແບ່ງປັນເຄືອຂ່າຍທີ່ໄດ້ເຊື່ອມຕໍ່ກັບເຄື່ອງສຳເນົາເອກະສານ ຫຼື ອຸປະກອນຈັດເກັບຂໍ້ມູນ (Hard drive) ສະເພາະແຕ່ກັບຜູ້ທີ່ທ່ານຕ້ອງການໃຫ້ເຂົ້າເຖິງເທົ່ານັ້ນ ບໍ?	4	2	0	0
	5	ທ່ານມີລະບົບໄວ້ ເພື່ອລະບຸໄພຄຸກຄາມ ຫຼື ວິທີການໂຈມຕີແບບໃໝ່ ແລະ ໄດ້ແບ່ງປັນຢູ່ພາຍໃນ ໂດຍການກວດກາ ແລະ ແບ່ງປັນການແຈ້ງເຕືອນດ້ານຄວາມປອດໄພຈາກຜູ້ຜະລິດສິນຄ້າ ຫຼື ເວັບໄຊທີ່ໃຫ້ບໍລິການ*3 ທີ່ທ່ານນຳໃຊ້ ບໍ?	4	2	0	0
ພາກທີ 2 ມາດຕະການ ສຳລັບພະນັກງານ	6	ທ່ານມີສະຕິລະມັດລະວັງຕໍ່ກັບອີເມວຫຼອກລວງ (Phishing Email) ແລະ ພະຍາຍາມບໍ່ເປີດເອກະສານຄັດຕິດໃນອີເມວທີ່ໜ້າສົງໄສ ຫຼື ກົດລິ້ງໃນຂໍ້ຄວາມຂອງອີເມວ ບໍ?	4	2	0	0
	7	ທ່ານມີລະບົບໄວ້ ເພື່ອກວດກາ ແລະ ປ້ອງກັນ ການສົ່ງອີເມວແບບຜິດພາດ ເຊັ່ນ ການກວດສອບທີ່ຢູ່ອີເມວ ກ່ອນທີ່ຈະສົ່ງ ບໍ?	4	2	0	0
	8	ທ່ານປ້ອງກັນຂໍ້ມູນທີ່ສຳຄັນ ໂດຍການໃສ່ລະຫັດໃຫ້ກັບເອກະສານຄັດຕິດ ຫຼື ມາດຕະການທີ່ຄ້າຍຄືກັນອື່ນໆ ກ່ອນການສົ່ງອອກ ໂດຍນຳໃຊ້ອີເມວ ບໍ?	4	2	0	0
	9	ທ່ານໄດ້ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອຄວາມປອດໄພຂອງລະບົບ ເຄືອຂ່າຍແບບໄຮ້ສາຍ ເຊັ່ນ ການເຂົ້າລະຫັດທີ່ສັບຊ້ອນສະເໝີ ເມື່ອນຳໃຊ້ລະບົບນີ້ ບໍ?	4	2	0	0
	10	ທ່ານໄດ້ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອຄວບຄຸມການນຳໃຊ້ອິນເຕີເນັດ ເຊັ່ນ ການຕັ້ງກົດລະບຽບກ່ຽວກັບການເຂົ້າຢ້ຽມຊົມເວັບໄຊ ແລະ ການໂພສລົງໃນສື່ສັງຄົມອອນລາຍ ຈາກຄອມພິວເຕີຂອງຫ້ອງການ ບໍ?	4	2	0	0
	11	ທ່ານໄດ້ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອສຳຮອງຂໍ້ມູນຢ່າງສະໝ່ຳສະເໝີ, ເພື່ອປ້ອງກັນ ຂໍ້ມູນທີ່ສຳຄັນຈາກການສູນຫາຍ ທີ່ເກີດຈາກຄວາມຜິດປົກກະຕິ ຫຼື ການປະຕິບັດງານຜິດພາດ ບໍ?	4	2	0	0
	12	ທ່ານໄດ້ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອປ້ອງກັນ ການສູນເສຍ ຫຼື ການຮົ່ວໄຫຼຂອງຂໍ້ມູນທີ່ສຳຄັນ ເຊັ່ນ ການເກັບຮັກສາຂໍ້ມູນທີ່ສຳຄັນໃນຕູ້ທີ່ມີກະແຈລັອກໄວ້ ແທນທີ່ຈະປະໄວ້ເທິງໜ້າໂຕະ ບໍ?	4	2	0	0
	13	ເມື່ອນຳເອົາຂໍ້ມູນທີ່ສຳຄັນອອກຈາກຫ້ອງການ, ທ່ານໄດ້ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ປ້ອງກັນການລັກຂະໂມຍ ຫຼື ສູນຫາຍ ເຊັ່ນ ປ້ອງກັນຂໍ້ມູນດ້ວຍການໃສ່ລະຫັດຜ່ານ ຫຼື ເຂົ້າລະຫັດຂໍ້ມູນໄວ້ ແລະ ຮັກສາໄວ້ກັບຕົວທ່ານຕະຫຼອດເວລາ ບໍ?	4	2	0	0
	14	ທ່ານໄດ້ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອຮັບປະກັນວ່າບຸກຄົນອື່ນໆ ບໍ່ໄດ້ໃຊ້ຄອມພິວເຕີຂອງທ່ານ ເຊັ່ນ ຕັ້ງຄ່າລັອກໜ້າຈໍຄອມພິວເຕີ ເມື່ອທ່ານອອກຈາກໂຕະເຮັດວຽກບໍ?	4	2	0	0
	15	ທ່ານພະຍາຍາມປ້ອງກັນ ບຸກຄົນທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດເຂົ້າມາໃນຫ້ອງການ ໂດຍການເຂົ້າຫາຄົນແປກໜ້າ ເມື່ອທ່ານສັງເກດເຫັນບາງຄົນທີ່ບໍ່ຄຸ້ນເຄີຍໃນຫ້ອງການ ຫຼື ໂດຍການດຳເນີນຕາມມາດຕະການອື່ນໆບໍ?	4	2	0	0
	16	ທ່ານໄດ້ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອປ້ອງກັນການລັກຂະໂມຍ ເມື່ອອອກຈາກຫ້ອງການແຕ່ລະມື້ ເຊັ່ນ ການລັອກແລັບທັອບ ແລະ ອຸປະກອນຕ່າງໆໃນລິ້ນຊັກຕູ້ ແທນທີ່ຈະປະໄວ້ເທິງໜ້າໂຕະ ບໍ?	4	2	0	0
	17	ກະແຈທີ່ໃຊ້ໄຂເຂົ້າຫ້ອງການຖືກຄຸ້ມຄອງຈັດການຢ່າງເໝາະສົມ ບໍ ເຊັ່ນ ບຸກຄົນສຸດທ້າຍທີ່ອອກຈາກຫ້ອງການໃນແຕ່ລະມື້ ໄດ້ໃສ່ກະແຈຫ້ອງການ ແລະ ມີການບັນທຶກໄວ້ (ຊື່, ວັນທີ ແລະ ເວລາ)?	4	2	0	0
	18	ເມື່ອມີການກຳຈັດຂໍ້ມູນທີ່ສຳຄັນ, ທ່ານໄດ້ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອເຮັດໃຫ້ຂໍ້ມູນທີ່ສຳຄັນນັ້ນບໍ່ສາມາດອ່ານໄດ້ ເຊັ່ນ ການໃຊ້ເຄື່ອງຈັກທຳລາຍເອກະສານ ຫຼື ໃຊ້ເຄື່ອງມືການລຶບຂໍ້ມູນ ບໍ?	4	2	0	0
ພາກທີ 3 ມາດຕະການສຳລັບອົງກອນ	19	ທ່ານມີການກຳນົດຄວາມປະພຶດຂອງພະນັກງານ ເພື່ອຮັກສາຄວາມລັບໄວ້ ເຊັ່ນ ການແຈ້ງພະນັກງານ ເມື່ອພວກເຂົາໄດ້ຮັບການຈ້າງງານແລ້ວວ່າ ພວກເຂົາມີພັນທະໃນການຮັກສາຄວາມລັບໄວ້ ແລະ ມີຂໍ້ບັນຍັດກ່ຽວກັບການລົງໂທດ ບໍ?	4	2	0	0
	20	ທ່ານໄດ້ມີການຝຶກອົບຮົມເພື່ອໃຫ້ພະນັກງານຮັບຮູ້ເຖິງຄວາມສຳຄັນຂອງການຄຸ້ມຄອງຈັດການຂໍ້ມູນ ເຊັ່ນ ການອະທິບາຍເຖິງຄວາມສຳຄັນຂອງຂໍ້ມູນ ຢ່າງສະໝ່ຳສະເໝີ?	4	2	0	0
	21	ທ່ານໄດ້ຊີ້ແຈງວ່າ ພະນັກງານ ອາດຈະຕ້ອງໄດ້ນຳໃຊ້ອຸປະກອນສ່ວນຕົວໃນການເຮັດວຽກ ເຊັ່ນ ການສ້າງນະໂຍບາຍກ່ຽວກັບການນຳໃຊ້ຄອມພິວເຕີສ່ວນບຸກຄົນ ແລະ ສະມາດໂຟນທັງພາຍໃນ ແລະ ພາຍນອກບໍລິສັດ ຫຼື ບໍ່?	4	2	0	0
	22	ທ່ານໄດ້ຮຽກຮ້ອງໃຫ້ຄູ່ຮ່ວມທຸລະກິດ ຮັກສາຂໍ້ມູນທີ່ເປັນຄວາມລັບ ເຊັ່ນ ລວມທັງ ຂໍ້ມູນຄວາມລັບ (ພັນທະເພື່ອຮັກສາຄວາມລັບ) ໃນສັນຍາບໍ?	4	2	0	0
	23	ທ່ານຢືນຢັນຄວາມປອດໄພຂອງການບໍລິການ ແລະ ຄວາມໜ້າເຊື່ອຖືໄດ້ ໂດຍການກວດກາ ເງື່ອນໄຂຂອງການນຳໃຊ້ ແລະ ມາດຕະການຄວາມປອດໄພກ່ອນການເລືອກການບໍລິການຈາກພາຍນອກ ເຊັ່ນ ການບໍລິການ ຄລາວ ບໍ?	4	2	0	0
	24	ໄດ້ມີການກະກຽມໃນກໍລະນີເກີດເຫດການກ່ຽວກັບຄວາມປອດໄພຂອງຂໍ້ມູນ ເຊັ່ນ ການສ້າງຂັ້ນຕອນການແກ້ໄຂສຳລັບການຮົ່ວໄຫຼ, ການສູນຫາຍ ຫຼື ການລັກຂະໂມຍຂໍ້ມູນທີ່ເປັນຄວາມລັບ ບໍ?	4	2	0	0
	25	ທ່ານກຳນົດເນື້ອໃນຂອງມາດຕະການຄວາມປອດໄພຂອງຂໍ້ມູນ ເຊັ່ນ ສ້າງມາດຕະການຄວາມປອດໄພຂອງຂໍ້ມູນ (ດັ່ງ ລາຍການທີ 1 ຫາ 24 ຂ້າງເທິງ) ຄືກັບເປັນນະໂຍບາຍຂອງບໍລິສັດ ບໍ?	4	2	0	0

*1 ໂປຣແກຣມ ທີ່ສະໜອງໃຫ້ໂດຍບໍລິສັດ Microsoft ທີ່ມີການແກ້ໄຂຂໍ້ບົກຜ່ອງໃນ ວິນໂດ PCs

*2 ໄຟລ໌ຖານຂໍ້ມູນ ຊຶ່ງເອີ້ນວ່າ “ໄຟລ໌ຮູບແບບ” ສຳລັບການກວດຈັບໄວຣັດຄອມພິວເຕີ.

*3 ຊື່ທົ່ວໄປຂອງການບໍລິການຖືກນຳໃຊ້ຜ່ານອິນເຕີເນັດ ເຊັ່ນ ການທະນາຄານຜ່ານອິນເຕີເນັດ, ສື່ສັງຄົມອອນລາຍ, ເວັບເມວ, ແລະ ປະຕິທິນ.

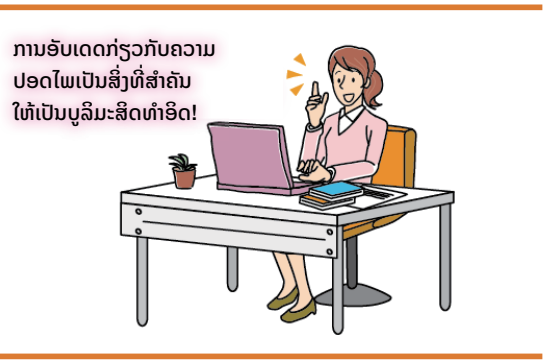
★ ມາດຕະການໃນໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ ທີ່ໄດ້ອະທິບາຍໄວ້ນັ້ນ ບໍ່ໄດ້ຮັບປະກັນວ່າຈະສາມາດປ້ອງກັນໄດ້ຢ່າງຄົບຖ້ວນ.

ກ ຄະແນນທີ່ໄດ້ ຈັດຕັ້ງປະຕິບັດທັງໝົດ	ຂ ຄະແນນທີ່ໄດ້ ຈັດຕັ້ງປະຕິບັດບາງສ່ວນ	ຄະແນນ ກ+ຂ
ຄະແນນ	ຄະແນນ	ຄະແນນ

ຄຳອະທິບາຍ

ພາກທີ 1 ມາດຕະການພື້ນຖານ

ລາຍການ No.1 ຫາ No.5 ແມ່ນມາດຕະການທີ່ຕ້ອງໄດ້ດຳເນີນການ ໂດຍບໍ່ກ່ຽວກັບຂະໜາດ ແລະ ຮູບແບບຂອງບໍລິສັດ ຊຶ່ງເປັນສິ່ງສຳຄັນຫຼາຍທີ່ຈະຕ້ອງມີການສືບຕໍ່ກວດສອບຄືນມາດຕະການເຫຼົ່ານີ້ ແລະ ບໍ່ແມ່ນຈະເຮັດພຽງແຕ່ຄັ້ງດຽວເທົ່ານັ້ນ. ມັນຈຳເປັນໃນການຈັດຕັ້ງປະຕິບັດມາດຕະການເຫຼົ່ານັ້ນ ຄືກັບ ເປັນກົດລະບຽບຂອງບໍລິສັດ ເພື່ອເຮັດໃຫ້ ພະນັກງານທຸກຄົນສາມາດປະຕິບັດຕາມໄດ້.



No. 1 ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 1 ມາດຕະການກ່ຽວກັບຊ່ອງໂຫວ່

ການອັບເດດລະບົບປະຕິການ (OS) ແລະ ຊໍ່ອບແວ ເປັນປະຈຳ

ການລະເລີຍຕໍ່ບັນຫາຄວາມປອດໄພຂອງລະບົບປະຕິບັດການ ແລະ ຊໍ່ອບແວ ເຮັດໃຫ້ ອຸປະກອນຂອງທ່ານມີຄວາມສ່ຽງທີ່ຈະຕິດໄວຣັດທີ່ເປັນອັນຕະລາຍໄດ້. ໃຫ້ແນ່ໃຈວ່າ ໄດ້ອັບເດດແພັດແກ້ໄຂ (Patches) ລະບົບປະຕິບັດການ ແລະ ຊໍ່ອບແວຂອງທ່ານ ຫຼື ນຳໃຊ້ເວີຊັ່ນຫຼ້າສຸດ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ນຳໃຊ້ການອັບເດດວິນໂດ (Windows OS) ຫຼື ການນຳໃຊ້ ເວີຊັ່ນຫຼ້າສຸດຂອງ Adobe Flash Player, Adobe Reader, Java runtime environment ແລະ ຊໍ່ອບແວອື່ນໆ.

No. 2 ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 2 ມາດຕະການປ້ອງກັນໄວຣັດ

ຕິດຕັ້ງຊໍ່ອບແວປ້ອງກັນໄວຣັດ ແລະ ນຳໃຊ້ຢ່າງຖືກຕ້ອງເໝາະສົມ.

ມີຈຳນວນໄວຣັດເພີ່ມຂຶ້ນ ທີ່ລັກຂະໂມຍເອົາຊື່ບັນຊີ ແລະ ລະຫັດຜ່ານ, ການຄວບຄຸມຄອມພິວເຕີຈາກໄລຍະໄກ ແລະ ເຂົ້າລະຫັດໄຟລ໌ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ. ຕ້ອງ ຮັບປະກັນວ່າໄດ້ຕິດຕັ້ງຊໍ່ອບແວປ້ອງກັນໄວຣັດ ແລະ ໃຫ້ແນ່ໃຈວ່າ ໄຟລ໌ທີ່ໃຊ້ກວດສອບໄວຣັດ (ໄຟລ໌ຮູບແບບ) ມີການອັບເດດເປັນປະຈຳ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ຕັ້ງຄ່າອຸປະກອນຂອງທ່ານເພື່ອອັບເດດ ໄຟລ໌ກ່ຽວກັບໄວຣັດແບບອັດຕະໂນມັດ ແລະ ພິຈາລະນາການຕິດຕັ້ງຊໍ່ອບແວຮັກ ສາຄວາມປອດໄພໄວ້ນຳກັນ.

No. 3 ໃບປະເມີນຜົນບໍລິສັດດ້ວຍຕົນເອງ No. 3 ການຄຸ້ມຄອງຈັດການລະຫັດຜ່ານ

ການນຳໃຊ້ລະຫັດຜ່ານທີ່ປອດໄພ

ຈຳນວນຄວາມເສຍຫາຍເພີ່ມຂຶ້ນຈາກການເຂົ້າເຖິງລະບົບທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດ ເນື່ອງຈາກ ການຄາດເດົາລະຫັດຜ່ານ ແລະ ການນຳໃຊ້ຊື່ບັນຊີທີ່ເປັນອັນຕະລາຍ ແລະ ລະຫັດຜ່ານທີ່ ຮົ່ວໄຫຼຈາກເວັບໄຊທ໌ທີ່ໃຫ້ບໍລິການ. ຄວນຈະເຮັດໃຫ້ລະຫັດຜ່ານຂອງທ່ານຍາກຕໍ່ການຄາດເດົາ ໂດຍປະກອບດ້ວຍລະຫັດທີ່ຍາວ, ສະຫຼັບສັບຊ້ອນ ແລະ ບໍ່ໃຊ້ຊ້ຳຄືນ.

*ລະຫັດຜ່ານທີ່ງ່າຍ: ລະຫັດຜ່ານທີ່ງ່າຍໃນການຄາດເດົາຈາກບຸກຄົນທີສາມ ເຊັ່ນ ຊື່ຂອງທ່ານ, ຊື່ບໍລິສັດ ຫຼື ຄຳສັບພາສາອັງກິດງ່າຍໆໃນວັດຈະນານຸກົມ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ສ້າງລະຫັດຜ່ານທີ່ມີການປະສົມປະສານກັນ ຄວາມຍາວຢ່າງຕ່ຳ 10 ຕົວ ທີ່ມີທັງຕົວເລກ, ຕົວອັກສອນ ແລະ ສັນຍາລັກຕ່າງໆ. ບໍ່ຄວນໃຊ້ຊື່, ໝາຍເລກໂທລະສັບ, ວັນເດືອນປີເກີດ ແລະ ອື່ນໆ, ບໍ່ຄວນໃຊ້ລະ ຫັດຜ່ານຄືກັນສຳລັບການບໍລິການຫຼາຍເວັບໄຊ ແລະ ເວັບໄຊອື່ນໆ.

No. 4 ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 4 ການຕັ້ງຄ່າອຸປະກອນ

ທົບທວນຄືນການຕັ້ງຄ່າການແບ່ງປັນ (Sharing)

ມີຄວາມກັງວົນເພີ່ມຂຶ້ນກ່ຽວກັບບຸກຄົນທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດໃນການເຂົ້າເບິ່ງຂໍ້ມູນ ເນື່ອງຈາກ ຂໍ້ມູນທີ່ເກັບຮັກສາໄວ້ໃນເຊີເວີໄຟລ໌ຂໍ້ມູນ ຫຼື ບ່ອນຈັດເກັບອອນລາຍ ຫຼື ການຕັ້ງຄ່າລະບົບ ເຄືອຂ່າຍເຄື່ອງສຳເນົາເອກະສານທີ່ບໍ່ຖືກຕ້ອງ. ໃຫ້ແນ່ໃຈວ່າ ເຊີເວີ ແລະ ອຸປະກອນເຄືອຂ່າຍ ຖືກແບ່ງປັນກັບບຸກຄົນທີ່ທ່ານອະນຸຍາດເພື່ອເຂົ້າເຖິງຂໍ້ມູນເທົ່ານັ້ນ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ຈຳກັດຂອບເຂດໃນການແບ່ງປັນບໍລິການຄລາວ, ຈຳກັດຂອບເຂດຂອງການແບ່ງປັນເຄືອຂ່າຍທີ່ເຊື່ອມຕໍ່ກັບອຸປະກອນຕ່າງໆ ແລະ ປ່ຽນແປງການຕັ້ງຄ່າ ເມື່ອພະນັກງານຍ້າຍໄປພະແນກອື່ນ ຫຼື ອອກຈາກວຽກ.

No. 5 ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 5 ການສັງລວມຂໍ້ມູນ

ຮຽນຮູ້ກ່ຽວກັບໄພຄຸກຄາມ, ການໂຈມຕີ ແລະ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອຕອບໂຕ້ສິ່ງເຫຼົ່ານັ້ນ.

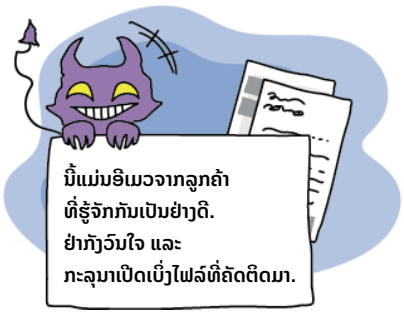
ມີການໂຈມຕີ ເພີ່ມຂຶ້ນເປັນຈຳນວນຫຼວງຫຼາຍ (Phishing) ເພື່ອລັກຂະໂມຍເອົາຂໍ້ມູນຊື່ບັນຊີ ແລະ ລະຫັດຜ່ານ ໂດຍຜ່ານທາງອີເມວ ດ້ວຍໄວຣັດທີ່ປອມຕົວເປັນຄູ່ຮ່ວມທຸລະ ກິດ, ຜູ້ຮ່ວມຮຸ້ນອື່ນໆ ຫຼື ນຳບຸກຄົນໄປສູ່ເວັບໄຊຫຼອກລວງທີ່ຄືກັບເວັບໄຊຕົວຈິງ. ດຳເນີນຕາມຂັ້ນຕ່າງໆ ເພື່ອຕອບໂຕ້ໄພຄຸກຄາມ ແລະ ວິທີການໂຈມຕີດ້ວຍການຮຽນຮູ້ກ່ຽວ ກັບສິ່ງເຫຼົ່ານັ້ນ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ການກວດກາເວັບໄຊ IPA ແລະ ການສະໝັກສະມາຊິກວາລະສານທາງອີເມວ ເພື່ອຮຽນຮູ້ກ່ຽວກັບໄພຄຸກຄາມ ແລະ ວິທີການໂຈມຕີຫຼ້າສຸດ ແລະ ການຢືນຢັນການແຈ້ງເຕືອນທີ່ສະໜອງໃຫ້ໂດຍທຸລະກຳ ທະນາຄານຜ່ານອິນເຕີເນັດ ແລະ ການບໍລິການອື່ນໆທີ່ນຳໃຊ້.

ຄຳອະທິບາຍ

ພາກທີ 2 ມາດຕະການ ສຳລັບພະນັກງານ

ລາຍການ No. 6 ຫາ No. 18 ແມ່ນລາຍການທີ່ພະນັກງານຄວນຈະຕ້ອງຮັບຮູ້. ຄວາມຜິດພາດຂອງຄົນສາມາດເກີດຂຶ້ນໄດ້ໂດຍງ່າຍ ເນື່ອງຈາກວ່າ ຄວາມລິ້ງເຄີຍ ແລະ ບໍ່ໃສ່ໃຈໃນການຈັດການກັບຂໍ້ມູນສຳຄັນ ໃນແຕ່ລະວັນ. ພ້ອມນັ້ນ, ທຳມະຊາດຂອງໄພຄຸກຄາມມີການປ່ຽນແປງໃນແຕ່ລະວັນ, ທ່ານຕ້ອງມີສະຕິຕື່ນຕົວຕະຫຼອດເວລາ.



No. 6 ใบประเมินบริษัทด้วยตัวเอง No. 6 ກົດລະບຽບການນຳໃຊ້ອີເມວ

ให้มีสะติละมัดละวังก่ยวกับอีเมวใดหนึ่งที่ได้รับจากบางคนที่ท่านบ่รู้จัก.

ສິ່ງນີ້ອາດເຮັດໃຫ້ຕິດໄວຣັດ ໂດຍການເປີດເບິ່ງເອກະສານຄັດຕິດໃນອີເມວ ຫຼື ໂດຍການກົດລິ້ງ URL ໃນອີເມວ. ໃຫ້ມີສະຕິລະມັດລະວັງກ່ຽວກັບໄຟລ໌ຄັດຕິດມານຳ ແລະ ການກົດລິ້ງ URL ຈາກຜູ້ສົ່ງທີ່ທ່ານບໍ່ຮູ້ຈັກ.

การจัดตั้งปะติบัด ดำเนินตามขั้นตอนต่างๆ เช่น บ่เปิดไฟล์ที่ถัดติดมา หื ก็ด ลิ้ง URL ในอีเมวที่พ้าส่งไส และ ลายงานอีเมวที่พ้าส่งไสนั้นให้กับพะแมกถวามปอดไพ เพื่อแบ่งปันข้อมูมก่ยวกับอีเมวที่พ้าส่งไสนั้นพายในบริษัด.

No. 7 ใบประเมินบริษัทด้วยตัวเอง No. 7 ກົດລະບຽບການນຳໃຊ້ອີເມວ

ป้องกันการส่งอีเมวไปหาผู้รับที่ผิดคน

จะเกิดเหตุการข้อมูลข่าวสารรั่วไหลไปหาคนอื่น โดยการส่งอีเมว หื แฟ้กหาผู้รับผิดคน. ให้แน่ใจว่า มีการกวดกาย่างละมัดละวังว่า ท่านส่งอีเมว หื แฟ้กหาใผ. พ้อมนั้น, การรั่วไหลของข้อมูลข่าวสารอาดเกิดขึ้นได้ ในเวลาที่ท่านให้ที่ย่อีเมวบ่ถืกต้องกับบางคน. เมื่อท่านส่งอีเมวหนึ่งหาหลายคนให้รับปะกัน ถวามถืกต้องของที่ย่อีเมวของบันดาผู้รับนั้น.

การจัดตั้งปะติบัด ดำเนินตามขั้นตอนต่างๆ เช่น กวดกาคืนอีกเที่ยวหนึ่งก่ยวกับที่ย่อีเมว ก่อนจะส่งอีเมว หื แฟ้ก และ เลือกแยกที่ย่อีเมวต่างหาก ละหว่างผู้ที่จะส่งหา (To), ผู้ที่จะส่งสำเม็าให้ (CC) และ ผู้ที่จะส่งสำเม็าให้แบบบ่ให้ผู้อื่นร้นำ (BCC)

No. 8 ใบประเมินบริษัทด้วยตัวเอง No. 8 ກົດລະບຽບການນຳໃຊ້ອີເມວ

ปิกป้องข้อมูลข่าวสารที่สำคัน เมื่อส่งทางอีเมว

เมื่อส่งข้อมูลที่สำคันทางอีเมว, บ่ให้ถรุนเนื้อในใส่ในอีเมว ให้ถรุนเนื้อในใส่ในไฟล์, ป้องกันโดยการใส่ละหัดผ่าน ແລະ ให้ถัดติดเอกะสารไฟล์นั้นกับอีเมวแทน. แจ้งผู้รับอีเมวก่ยวกับละหัดผ่าน โดยการโทละสับบอก หื ผ่านสื่ทางอื่นๆ, แทนที่จะถรุนใส่ในอีเมว.

การจัดตั้งปะติบัด ดำเนินตามขั้นตอนต่างๆ เช่น ถรุนข้อมูลที่สำคันในไฟล์ ແລະ ป้องกันโดยการใส่ละหัดผ่าน. แจ้งบอกผู้รับอีเมวทางโทละสับ หื ผ่านทางสื่ทางอื่นๆ.

No. 9 ใบประเมินบริษัทด้วยตัวเอง No. 9 ກົດລະບຽບການນຳໃຊ້ລະບົບ ເຄືອຂ່າຍ ແບບໄຮ້ສາຍ

ป้องกันการลักขะโมยข้อมูล ແລະ การนำใช้ละบบ เถือข่าย แบบไร้สายที่บ่ได้รับอะนุยาด

ละบบ เถือข่าย แบบไร้สาย ที่บ่มีการตั้งถ่าถวามปอดไพดีพรุงพ้, ข้อมูลของพวกเขาอาดจะถืกอ่าน หื นำใช้ในการกะทำผิดทางอายา โดยการเชื่อมต่อกับละบบแบบบ่ถืกต้องตามก็ดพาย. ให้รับปะกันในการติดตั้งถวามปอดไพของละบบ เถือข่าย แบบไร้สาย เพื่อป้องกัน การดักฟัง ແລະ การนำใช้ที่บ่ได้รับอะนุยาด.

การจัดตั้งปะติบัด ดำเนินตามขั้นตอนต่างๆ เช่น การนำใช้การตั้งถ่าเข้าละหัด (ตัวย่าง: WPA2-PSK) ແລະ นำใช้ละหัดผ่านที่ยาว ແລະ ยากที่จะถาดเด็าได้.

No. 10 ใบประเมินบริษัทด้วยตัวเอง No. 10 ກົດລະບຽບການນຳໃຊ້ອິນເຕີເນັດ

ป้องกันบันหาเมื่อนำใช้อินเตเน็ด

การเข้าเบิ่งเวับไซที่มีไวรัด หื เวับไซที่มีบันหาด้านถวามปอดไพ สามาดเรัดให้อุปะกอนของท่านติดไวรัดได้. พ้อมนั้น, บันดาบริษัด อาดจะเกิดถวามเสยหายอันเนื่องจากการถรุนยอกหื้มที่เอาล้งในสื่สังค์มออนลาย, กะดานข้อถาม หื การเอาข้อมูมที่เป็นถวามลับล้งโดยบ่ตั้งใจ. เป็นสิ่งจำเป็นที่จะต้องได้ป้องกันถวามเสยหายที่อาดจะเกิดขึ้นนั้น โดยการวางละบบ ແລະ ก็ดละบรบที่จำกัดการนำใช้อินเตเน็ดในเวลาเรัดวรก.

การจัดตั้งปะติบัด ดำเนินตามขั้นตอนต่างๆ เช่น การส้างก็ดละบรบการเข้าเพื่อนำใช้อินเตเน็ด, สื่สังค์มออนลายต่างๆ ແລະ ใช้ตัวกั้นตองเวับไซ เพื่อจำกัดการนำใช้อินเตเน็ดย่างเป็นละบบ.

No. 11 ใบประเมินบริษัทด้วยตัวเอง No. 11 ກົດລະບຽບການສຳຮອງຂໍ້ມູນ

ส่งเสิมให้มีการสำรองข้อมูนย่างเป้นปิกกะติ

ข้อมูนที่บันทึกไว้ในถอมพิวเตเส่วนบุกคน (PC) หื เซิเว้ สามาดสูนหายได้ เนื่องจากการเรัดวรกผิดปิกกะติ, การปะติบัดงานที่ผิดพาด, หื ติดไวรัด. การสำรองข้อมูน เพื่อกะกรุมไว้สำลับสะถานะการที่อาดเกิดขึ้นได้โดยบ่ถาดถิด.

การจัดตั้งปะติบัด ดำเนินตามขั้นตอนต่างๆ เช่น ดำเนินการสำรองข้อมูนสำถัมไว้เป้นปิกกะติ ແລະ เกับรักสาข้อมูนสำรองไว้ในบ่อนอื่นแยกกันต่างหาก.

ຄໍາອະທິບາຍ

No. 12	ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 12 ກົດລະບຽບການເກັບຮັກສາຂໍ້ມູນ

ຂໍ້ມູນ/ເອກະສານສໍາຄັນ ຕ້ອງຈັດການເກັບມ້ຽນຢ່າງຖືກຕ້ອງເໝາະສົມ.

ການປະຂໍ້ມູນ/ເອກະສານໄວ້ໂດຍບໍ່ຕັ້ງໃຈເທິງໜ້າໂຕະຈະເຮັດໃຫ້ມີຄວາມສ່ຽງ ເພາະວ່າ ບາງຄົນອາດຈະອ່ານ ຫຼື ເອົາເອກະສານນັ້ນໄປ. ຂໍ້ມູນ/ເອກະສານສໍາຄັນ ຕ້ອງໄດ້ຈັດການເກັບມ້ຽນຢ່າງຖືກຕ້ອງເໝາະສົມ ເພື່ອປ້ອງກັນບຸກຄົນອື່ນເຫັນ ຫຼື ເອົາໄປ ແລະ ຮັບປະກັນວ່າ ຂໍ້ມູນ/ເອກະສານນັ້ນ ຈະບໍ່ຖືກປະປ່ອຍໄວ້ໂດຍບໍ່ຕັ້ງໃຈ. ກໍານົດບ່ອນເກັບມ້ຽນສໍາລັບຂໍ້ມູນ/ເອກະສານ, ເອົາເອກະສານອອກມາສະເພາະແຕ່ເວລາທີ່ຈໍາເປັນເພື່ອໃຊ້ເຮັດວຽກ ແລະ ຮັບປະກັນວ່າ ໃຫ້ເກັບມ້ຽນຄືນເມື່ອເຮັດວຽກແລ້ວ.

ການຈັດຕັ້ງປະຕິບັດ	ດໍາເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ເຮັດໃຫ້ໂຕະເຮັດວຽກສະອາດ, ເປັນລະບຽບຮຽບຮ້ອຍ ແລະ ເກັບມ້ຽນຂໍ້ມູນ/ເອກະສານສໍາຄັນໃນຕູ້ເກັບເອກະສານທີ່ມີກະແຈລັອກໄວ້.

No. 13	ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 13 ກົດລະບຽບການສົ່ງຂໍ້ມູນ

ສົ່ງຂໍ້ມູນສໍາຄັນໃນລັກສະນະທີ່ປອດໄພ

ເມື່ອນໍາເອົາຂໍ້ມູນສໍາຄັນອອກໄປນອກບໍລິສັດ, ມັນອາດຈະຖືກລັກຂະໂມຍ ຫຼື ສູນຫາຍໂດຍບໍ່ຄາດຄິດ. ດໍາເນີນຂັ້ນຕອນຕ່າງໆລ່ວງໜ້າ ເມື່ອນໍາໃຊ້ຄອມພິວເຕີແລັບທັອບ ຫຼື ສະມາດໂຟນ ເຊັ່ນ ການຕັ້ງຄ່າລະຫັດຜ່ານ ຫຼື ໃສ່ລະຫັດໃນໄຟລຂໍ້ມູນ ເພື່ອບໍ່ໃຫ້ຂໍ້ມູນເປີດເບິ່ງໄດ້ງ່າຍໃນກໍລະນີທີ່ຖືກລັກຂະໂມຍ ຫຼື ສູນຫາຍ.

ການຈັດຕັ້ງປະຕິບັດ	ດໍາເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ການສົ່ງຂໍ້ມູນສໍາຄັນ ຕ້ອງໄດ້ຮັບການອະນຸຍາດກ່ອນທຸກຄັ້ງ, ຮັກສາຂໍ້ມູນໃຫ້ປອດໄພດ້ວຍການໃສ່ລະຫັດຜ່ານໃນຄອມພິວເຕີແລັບທັອບ, ສະມາດໂຟນ, ຢູເອສບີ (USBs) ແລະ ບໍ່ໃຫ້ປະຖິ້ມໃສ່ເຄື່ອງ ຫຼື ກະເປົາໄວ້ຊະຊາຍ.

No. 14	ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 14 ການຄຸ້ມຄອງຈັດການຄວາມປອດໄພໃນຫ້ອງການ

ບໍ່ໃຫ້ບຸກຄົນໃດໜຶ່ງນໍາໃຊ້ອຸປະກອນໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.

ໃນເວລາເຮັດວຽກບໍ່ຄວນປະຄອມພິວເຕີໄວ້ຊະຊາຍ, ບຸກຄົນໃດໜຶ່ງສາມາດເຂົ້າໃຊ້ງານຄອມພິວເຕີນັ້ນໄດ້ໂດຍບໍ່ໃສ່ລະຫັດຜ່ານ, ສາມາດນໍາໃຊ້ໄປໃນທາງທີ່ບໍ່ເໝາະສົມ. ດໍາເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອປ້ອງກັນຄອມພິວເຕີສ່ວນບຸກຄົນຈາກການນໍາໃຊ້ທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດ.

ການຈັດຕັ້ງປະຕິບັດ	ດໍາເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ລັອກໜ້າຈໍຄອມພິວເຕີສ່ວນບຸກຄົນ (PC) ເມື່ອທ່ານບໍ່ຢູ່ໂຕະເຮັດວຽກ, ປິດຄອມພິວເຕີສ່ວນບຸກຄົນ (PC) ທຸກຄັ້ງເມື່ອອອກຈາກຫ້ອງການແຕ່ລະມື້ ເພື່ອປ້ອງກັນບໍ່ໃຫ້ບຸກຄົນອື່ນນໍາໃຊ້ຄອມພິວເຕີຂອງທ່ານ.

No. 15	ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 15 ການຄຸ້ມຄອງຈັດການຄວາມປອດໄພໃນຫ້ອງການ

ເຂົ້າຫາຄົນທີ່ທ່ານບໍ່ຮູ້ຈັກ

ຂໍ້ມູນຈະເປັນອັນຕະລາຍຈາກການຖືກລັກຂະໂມຍ ຖ້າຫາກທ່ານບໍ່ຈໍາກັດການເຂົ້າເຖິງຂອງບຸກຄົນທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດເຂົ້າມາໃນຫ້ອງການ. ໃຫ້ຮັບປະກັນວ່າ ບຸກຄົນທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດບໍ່ສາມາດເຂົ້າມາໃນສະຖານທີ່ເກັບມ້ຽນຂໍ້ມູນ/ເອກະສານສໍາຄັນ ເຊັ່ນ ຫ້ອງເຊີເວີ, ບ່ອນເກັບມ້ຽນເອກະສານ ແລະ ຕູ້ນິລະໄພ.

ການຈັດຕັ້ງປະຕິບັດ	ດໍາເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ການເຂົ້າເຖິງບຸກຄົນທີ່ທ່ານບໍ່ຮູ້ຈັກໃນຫ້ອງການ ຫຼື ຈັດໂຕະຕ້ອນຮັບ.

No. 16	ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 16 ການຄຸ້ມຄອງຈັດການຄວາມປອດໄພໃນຫ້ອງການ

ດໍາເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອປ້ອງກັນການລັກຂະໂມຍອຸປະກອນ ແລະ ອຸປະກອນເສີມຕ່າງໆ

ໃນຂະນະທີ່ອຸປະກອນຕ່າງໆ ເຊັ່ນ ຄອມພິວເຕີແລັບທັອບ, ແທັບເລັດ ແລະ ຢູເອສບີ (USBs) ແມ່ນສະດວກ ແລະ ຖືໄປໄດ້, ສິ່ງນີ້ ຍັງເຮັດໃຫ້ເກີດຄວາມສ່ຽງສູງໃນການຖືກລັກຂະໂມຍ. ເມື່ອອຸປະກອນເຫຼົ່ານີ້ ບໍ່ໄດ້ຖືກນໍາໃຊ້, ໃຫ້ດໍາເນີນຂັ້ນຕອນຕ່າງໆ ເພື່ອເກັບມ້ຽນພວກມັນໄວ້ໃນບ່ອນທີ່ປອດໄພ ເຊັ່ນ ໃນຕູ້ລີ້ນຊັກທີ່ມີກະແຈໃສ່ລັອກໄດ້.

ການຈັດຕັ້ງປະຕິບັດ	ດໍາເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ການໃສ່ກະແຈລັອກ ຄອມພິວເຕີແລັບທັອບ, ແທັບເລັດ ແລະ ອຸປະກອນເສີມຕ່າງໆ (ຊີດີ, ຢູເອສບີ (USBs), ອຸປະກອນບັນທຶກຂໍ້ມູນພາຍນອກ (Hard drive) ແລະ ອື່ນໆ) ໄວ້ໃນລີ້ນຊັກຕູ້ເມື່ອອອກຈາກຫ້ອງການແຕ່ລະມື້

No. 17	ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 17 ການຄຸ້ມຄອງຈັດການຄວາມປອດໄພໃນຫ້ອງການ

ຕ້ອງມີສະຕິຕື່ນຕົວໃນການລັອກປະຕູຫ້ອງການ

ບັນທຶກເວລາຄົນສຸດທ້າຍທີ່ອອກຈາກຫ້ອງການ ຈະຊ່ວຍໃນການເຕືອນສະຕິຕໍ່ຄວາມຮັບຜິດຊອບຂອງບຸກຄົນສຸດທ້າຍ ໃຫ້ໃສ່ກະແຈລັອກປະຕູຫ້ອງການ ເພື່ອໃຊ້ໃນການຄຸ້ມຄອງກະແຈ ແລະ ບັນທຶກຕ່າງໆ.

ການຈັດຕັ້ງປະຕິບັດ	ດໍາເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ການຄຸ້ມຄອງກະແຈ ແລະ ບັນທຶກການລັອກປະຕູຂອງຄົນສຸດທ້າຍທີ່ຢູ່ຫ້ອງການ (ວັນທີ, ເວລາ ແລະ ຊື່)

No. 18	ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 18 ການກໍາຈັດຂໍ້ມູນທີ່ປອດໄພ

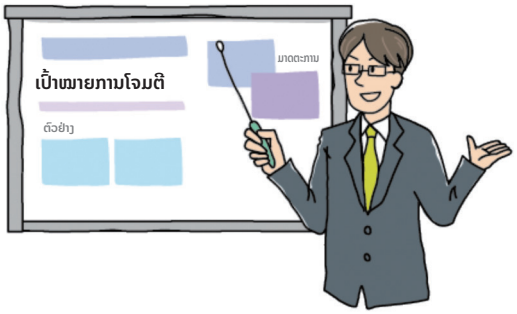
ການລຶບຂໍ້ມູນສໍາຄັນ ເພື່ອບໍ່ໃຫ້ສາມາດກູ້ຄືນມາໄດ້

ການກໍາຈັດເອກະສານຕ່າງໆທີ່ມີຂໍ້ມູນສໍາຄັນແບບງ່າຍດາຍໃສ່ຖົງຂີ້ເຫຍື້ອ ສາມາດເຮັດໃຫ້ເກີດການຮົ່ວໄຫຼຂອງຂໍ້ມູນຢ່າງຫຼວງຫຼາຍ ເນື່ອງຈາກວ່າ ບຸກຄົນອື່ນຈະສາມາດອ່ານເອກະສານໄດ້. ພ້ອມນັ້ນ, ຂໍ້ມູນທີ່ຮັກສາໄວ້ໃນອຸປະກອນເອເລັກໂຕຣນິກ ແລະ ສື່ເອເລັກໂຕຣນິກ ສາມາດກູ້ຄືນມາໄດ້ ເຖິງແມ່ນວ່າ ໄຟລ໌ນັ້ນຈະຖືກລຶບຖິ້ມກໍຕາມ. ເມື່ອກໍາຈັດຂໍ້ມູນສໍາຄັນ, ໃຫ້ກໍາຈັດສິ່ງບັນຈຸຂໍ້ມູນນັ້ນຢ່າງເໝາະສົມ ເຊັ່ນ ການໃຊ້ເຄື່ອງຈັກທໍາລາຍເອກະສານ ຫຼື ຊອບແວລຶບຂໍ້ມູນ.

ການຈັດຕັ້ງປະຕິບັດ	ດໍາເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເພື່ອກໍາຈັດຂໍ້ມູນ ເຊັ່ນ ການນໍາໃຊ້ ຊອບແວລຶບຂໍ້ມູນ, ການທໍາລາຍຂໍ້ມູນທາງກາຍະພາບ ຫຼື ຮ້ອງຂໍໃຫ້ຊ່ຽວຊານລຶບຂໍ້ມູນໃຫ້.

ພາກທີ 3 ມາດຕະການສຳລັບອົງກອນ

ລາຍການ No. 19 ຫາ No. 25 ແມ່ນມາດຕະການທີ່ຈະດຳເນີນການ ພາຍຫຼັງການສ້າງນະໂຍບາຍສຳລັບອົງກອນ. ເພີ່ມລະດັບຄວາມຮັບຮູ້ຄວາມສາມາດຂອງພະນັກງານ ໂດຍການສ້າງກົດລະບຽບຢ່າງຊັດເຈນຂອງບໍລິສັດ ແລະ ເຜີຍແຜ່ພາຍໃນ.



No. 19 ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 19 ແຈ້ງໃຫ້ພະນັກງານຕ້ອງມີຄວາມຮັບຜິດຊອບໃນການເກັບຮັກສາຄວາມລັບຂອງບໍລິສັດ

ໃຫ້ພະນັກງານທຳຄວາມເຂົ້າໃຈກ່ຽວກັບຄວາມຮັບຜິດຊອບຂອງພວກເຂົາ ໃນການເກັບຮັກສາຄວາມລັບຂອງບໍລິສັດ

ເຖິງແມ່ນວ່າ ກົດລະບຽບຂອງບໍລິສັດນັ້ນໄດ້ກຳນົດໄວ້ແລ້ວວ່າ ໃຫ້ພະນັກງານເກັບຮັກສາຄວາມລັບໃນວຽກຂອງຕົນເອງ. ເຖິງຢ່າງໃດກໍຕາມ, ມັນກໍ່ເປັນການດີທີ່ຕ້ອງແຈ້ງໃຫ້ພະນັກງານເຂົ້າໃຈຢ່າງຊັດເຈນ ແລະ ປະຕິບັດຕາມກົດລະບຽບ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ແຈ້ງໃຫ້ພະນັກງານຮູ້ກ່ຽວກັບຄວາມຮັບຜິດຊອບໃນການເກັບຮັກສາຄວາມລັບຂອງບໍລິສັດ ເມື່ອເຂົ້າມາເປັນພະນັກງານ.

No. 20 ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No. 20 ການຝຶກອົບຮົມພະນັກງານ

ຈັດການຝຶກອົບຮົມພະນັກງານຢ່າງເປັນປົກກະຕິ

ພະນັກງານທີ່ຮັບຜິດຊອບກ່ຽວກັບຂໍ້ມູນຂ່າວສານໃນແຕ່ລະມື້ ຕາມໜ້າທີ່ຮັບຜິດຊອບຂອງພວກເຂົາ ແລະ ຄວາມເຄີຍຊິນນີ້ ໝາຍເຖິງ ຈະມີການຄຸ້ມຄອງແບ໋ງແຍງ ແລະ ພວກເຂົາຈະລືມກ່ຽວກັບການຈັດການຂໍ້ມູນຂ່າວສານໃຫ້ປອດໄພ. ມີການຝຶກອົບຮົມໃຫ້ພະນັກງານຢ່າງເປັນປະຈຳ ແມ່ນຈະເພີ່ມຄວາມຮັບຮູ້ແລະເຂົ້າໃຈຂອງພະນັກງານ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ອະທິບາຍກ່ຽວກັບຄວາມສຳຄັນຂອງຂໍ້ມູນຂ່າວສານເປັນປະຈຳ ແລະ ດຳເນີນການຝຶກອົບຮົມພາຍໃນບໍລິສັດ.

No. 21 ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No.21 ການນຳໃຊ້ອຸປະກອນສ່ວນບຸກຄົນ

ການຕັດສິນໃຈ ໃນການອະນຸຍາດໃຫ້ນຳໃຊ້ອຸປະກອນສ່ວນບຸກຄົນສຳລັບເຮັດວຽກ

ຮັບປະກັນວ່າເລື່ອງຄວາມປອດໄພຈະບໍ່ເປັນບັນຫາຫຍຸ້ງຍາກ ຖ້າຫາກວ່ານຳໃຊ້ອຸປະກອນສ່ວນບຸກຄົນ ເຊັ່ນ ຄອມພິວເຕີສ່ວນບຸກຄົນ (PCs) ແລະ ໂທລະສັບມືຖືເຂົ້າມານຳໃຊ້ໃນການເຮັດວຽກ, ເພາະມັນຫຍຸ້ງຍາກທີ່ຈະຈັດການໃຫ້ພະນັກງານຮູ້ນຳໃຊ້ມັນຢ່າງປອດໄພ. ຕ້ອງລະບຸຊັດເຈນວ່າ ອຸປະກອນສ່ວນບຸກຄົນ ສາມາດນຳໃຊ້ສຳລັບວຽກໄດ້ ຫຼື ບໍ່ ແລະ ພະຍາຍາມສ້າງກົດລະບຽບໃນການນຳໃຊ້ຢ່າງປອດໄພ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ໂດຍການສ້າງລະບົບອະນຸຍາດເພື່ອການນຳໃຊ້ອຸປະກອນສ່ວນບຸກຄົນ ເຊັ່ນ ຄອມພິວເຕີສ່ວນບຸກຄົນ (PCs) ແລະ ໂທລະສັບມືຖື ທີ່ໃຊ້ໃນການເຮັດວຽກ ແລະ ກຳນົດກົດລະບຽບສຳລັບການນຳໃຊ້ ຖ້າໄດ້ຮັບອະນຸຍາດໃຫ້ນຳໃຊ້ໃນການເຮັດວຽກ.

No. 22 ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No.22 ການຄຸ້ມຄອງຈັດການຄູ່ຮ່ວມທຸລະກິດ

ການຮ້ອງຂໍໃຫ້ຄູ່ຮ່ວມທຸລະກິດຮັກສາຄວາມລັບ.

ຫຼີກລ້ຽງຄວາມເຂົ້າໃຈວ່າ ບັນດາຄູ່ຮ່ວມທຸລະກິດ ຈະຮັກສາຄວາມລັບແນ່ນອນ ໂດຍອີງໃສ່ສະພາບຂອງຂໍ້ມູນຂ່າວສານ. ເມື່ອຫາກວ່າສະໜອງຂໍ້ມູນຂ່າວສານທີ່ເປັນຄວາມລັບໃຫ້ກັບບັນດາຄູ່ຮ່ວມທຸລະກິດ, ຈຳເປັນຕ້ອງໃຫ້ຄວາມຈະແຈ້ງວ່າຂໍ້ມູນຂ່າວສານນັ້ນຕ້ອງໄດ້ຮັກສາເປັນຄວາມລັບ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ ຮ່າງສັນຍາຢ່າງຈະແຈ້ງກ່ຽວກັບການຮັກສາຄວາມລັບ.

No. 23 ໃບປະເມີນບໍລິສັດດ້ວຍຕົນເອງ No.23 ການນຳໃຊ້ບໍລິການຈາກພາຍນອກ

ນຳໃຊ້ບໍລິການຈາກພາຍນອກທີ່ເຊື່ອຖືໄດ້

ຖ້າເລືອກນຳໃຊ້ບໍລິການຈາກພາຍນອກ ເຊັ່ນ ການບໍລິການຄລາວ (Cloud) ໃນລາຄາພິເສດ, ທ່ານອາດຈະພົບວ່າ ການບໍລິການ ອາດຈະບໍ່ໄດ້ຄວບຄຸມໃນກໍລະນີການປະຕິບັດງານລົ້ມເຫຼວ ແລະ ບັນຫາອື່ນໆ. ເມື່ອຈະນຳໃຊ້ບໍລິການຈາກພາຍນອກ ສຳລັບແອັບພິເຄຊັ່ນທີ່ມີຜົນກະທົບຮ້າຍແຮງຕໍ່ການດຳເນີນທຸລະກິດ ຄວນພິຈາລະນາຈາກ ການປະຕິບັດງານທີ່ລະອຽດຖີ່ຖ້ວນ, ຄວາມໜ້າເຊື່ອຖື, ລາຍລະອຽດການຊັດເຊີຍ ແລະ ອື່ນໆ ທີ່ກ່ຽວຂ້ອງ.

ການຈັດຕັ້ງປະຕິບັດ ດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆ ເຊັ່ນ: ການກວດກາ ສັນຍາການໃຫ້ບໍລິການ, ລາຍລະອຽດການຊັດເຊີຍ, ບັນດາມາດຕະການຄວາມປອດໄພ ແລະ ສິ່ງອື່ນໆທີ່ກ່ຽວຂ້ອງ ໃນການເລືອກຜູ້ໃຫ້ບໍລິການ.

ຄຳອະທິບາຍ

No. 24	ใบประเมินบริษัทด้วยตัวเอง No. 24 การกะกรุมสำหรับเหตการณ์ความปลอดไพของข้อมูล

ກຽມພ້ອມສຳລັບເຫດການດ້ານຄວາມປອດໄພຂໍ້ມູນຂ່າວສານທີ່ຈະເກີດຂຶ້ນ

ເມື່ອມີເຫດການເກີດຂຶ້ນ, ປົກກະຕິ ບໍ່ມີເວລາທີ່ຈະຄິດໄຕ່ຕອງ ແລະ ທຸກຄວາມລ່າຊ້າ, ໃນການແກ້ໄຂເຫດການນັ້ນ ມັກຈະມີແນວໂນ້ມເຮັດໃຫ້ຜົນກະທົບຂອງເຫດການນັ້ນເພີ່ມຂຶ້ນ. ນຳໃຊ້ເຫດການທີ່ໄດ້ຮັບການລາຍງານໃນສື່ທີ່ເກີດຂຶ້ນ ໃນການອ້າງອີງ ເພື່ອຄິດກ່ຽວກັບວ່າ ໃຜຈະເຮັດຫຍັງ ແລະ ເມື່ອໃດ ໂດຍຕັ້ງສົມມຸດຕິຖານທີ່ວ່າ ເຫດການທີ່ຄືກັນນັ້ນ ເກີດຂຶ້ນໃນບໍລິສັດຂອງທ່ານ.

ການຈັດຕັ້ງປະຕິບັດ	ดำเนินตามขั้นตอนต่างๆ เช่น: การกะกรุม คู่มือแก้ไขสำหรับ การรั่วไหล, การสูญหาย ຫຼື ຖືກລັກຂະໂມຍຂໍ້ມູນທີ່ສຳຄັນ.

No. 25	ใบประเมินบริษัทด้วยตัวเอง No. 25 การกะกรุมกฎละบรุบ

ສ້າງກົດລະບຽບສຳລັບມາດຕະການຄວາມປອດໄພຂອງຂໍ້ມູນຂ່າວສານ

ເຖິງແມ່ນວ່າ, ຜູ້ບໍລິຫານລະດັບສູງ ໄດ້ວາງນະໂຍບາຍ ເພື່ອເປັນມາດຕະການຄວາມປອດໄພຂໍ້ມູນຂ່າວສານ, ຢ່າງໜ້ອຍ ເອກະສານກົດລະບຽບຕ້ອງມີຄວາມລະອຽດຢ່າງຊັດເຈນ, ພະນັກງານ ສາມາດຂໍຄຳແນະນຳຈາກຜູ້ບໍລິຫານໄດ້ຕະຫຼອດເວລາ. ເພື່ອໃຫ້ພະນັກງານປະຕິບັດຕາມກົດລະບຽບດ້ວຍຕົວເອງ, ເອກະສານ “ກົດລະບຽບຂອງບໍລິສັດ” ທີ່ຊັດເຈນເປັນສິ່ງສຳຄັນ ເພື່ອໃຫ້ ພະນັກງານ ສາມາດນຳໃຊ້ເປັນບ່ອນອ້າງອີງໄດ້.

ການຈັດຕັ້ງປະຕິບັດ	ดำเนินตามขั้นตอนต่างๆ เช่น ลายการ No. 1-24 ของใบประเมิน ที่เป็นกฎละบรุบสำหรับมาดตะการความปอดไพของข้อมูลข่าวสาน พ้อมกับเผียแผ่พายในบริสัด และ มีการกวดสอบบันดากฎละบรุบเป็นปะจำ เพื่อปับปุงข้อบกพ่องต่างๆที่ค้นพบ

NISC National center of Incident readiness and Strategy for Cybersecurity

LaoCERT Lao Computer Emergency Response Team

IPA Information-technology Promotion Agency, Japan

2019.04