ជំពូក ១

ឯកសារបន្ថែម (ត្រូវបានរៀបចំឡើងនៅឆ្នាំ២០០៩)

ផ្នែក ទី១

គោលនយោបាយជាមូលដ្ឋានរបស់

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខជាតិ

របស់ រាជរដ្ឋាភិបាល

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល គោលនយោបាយជាមូលដ្ឋាន

១. សាថតារ

- ហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មានរបស់រដ្ឋាភិបាល បានជួបប្រទះនូវការគំរាមកំហែងផ្នែកសន្តិសុខព័ត៌មាននៅទូទាំងពិភពលោក ដែលអាចបង្កនូវការខូចខាតយ៉ាងធ្ងន់ធ្ងរដល់ធនធានព័ត៌មានរបស់រាជរដ្ឋាភិបាល។ ខាងក្រោមនេះត្រូវបានចាត់ទុកថាជាការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិត៖

- Cyber Terrorist: ជាជនដែលមានជំនាញ ចូលវាយលុកប្រព័ន្ធកុំព្យូទ័ររបស់ស្ថាប័នផ្សេងៗក្នុងគោលបំណងកែប្រែ និងបំផ្លើចបំផ្លាញព័ត៌មាន ដើម្បីផលប្រយោជន៍នយោបាយ។
- Hackers: ជាអ្នកជំនាញសរសេរកម្មវិធីចូលវាយលុកប្រព័ន្ធកុំព្យូទ័រ របស់ស្ថាប័នផ្សេងៗក្នុងគោលបំណងលួចកែប្រែ និងបំផ្លើចបំផ្លាញព័ត៌មាន។
- Cyber Thieves/Frauds: គោលបំណងរបស់ពួកគេ គឺដើម្បីរកលុយ ។

ឧក្រិដ្ឋជនអ៊ីនធឺណិត ធ្វើការវាយប្រហារហេដ្ឋារចនាសម្ព័ន្ធ ICT របស់រាជរដ្ឋាភិបាល ដើម្បីកាត់ផ្តាច់សេវាតាមប្រព័ន្ធអ៊ីនធឺណិតរបស់រដ្ឋាភិបាល (e-Government services) ដើម្បីលួចយក ឬបំផ្លាញព័ត៌មានដែលមានតម្លៃ និងមូលដ្ឋានទិន្នន័យសម្ងាត់របស់រាជរដ្ឋាភិបាល ។ ជាមួយគ្នានេះដែរ ឧក្រិដ្ឋជនទាំងនោះ នឹងផ្តោតគោលដៅទៅលើហេដ្ឋារចនាសម្ព័ន្ធ ICT របស់សង្គម ដូចជាសេវាអ៊ីនធឺណិតជាដើមក្នុងគោលបំណងបង្កការ រំខានដល់ការងាររបស់សាធារណជន ។

- គ្រោះថ្នាក់បន្ទាន់របស់រាជរដ្ឋាភិបាល
  ប្រសិនបើព័ត៌មានសំខាន់នៅក្នុងហេដ្ឋារចនាសម្ព័ន្ធរបស់រាជរដ្ឋាភិបាល ត្រូវបានពួកឧក្រិដ្ឋជនអ៊ីនធឺណិតធ្វើអោយលេចឮទៅខាងក្រៅ ឬធ្វើការផ្លាស់ប្តូរគ្នានោះ ។ ដូច្នេះ ជាការសំខាន់ បំផុតដែលរាជរដ្ឋាភិបាលត្រូវពង្រឹងសន្តិសុខព័ត៌មាន ព្រមទាំងតម្លើងប្រព័ន្ធការពារដោយផ្អែកតាមការរៀបចំ ផែនការដ៏រឹងមាំ និងប្រកបដោយយុទ្ធសាស្ត្រទៀតផង ។

២. គោលនយោបាយជាមូលដ្ឋាន

ដោយពិចារណាទៅលើបរិយាកាសគំរាមកំហែង ផ្នែកសន្តិសុខព័ត៌មាននាពេលបច្ចុប្បន្ន រាជរដ្ឋាភិបាលគួរតែណែនាំអោយមានការប្រើប្រាស់នូវដំណោះស្រាយសន្តិសុខព័ត៌មានដ៏ទូលំទូលាយ នៅតាមបណ្តាក្រសួង និងស្ថាប័ន ទាំងអស់ ក្នុងកម្រិតគុណភាពរួម ។ ដើម្បីបង្កើតនូវដំណោះស្រាយរួមដ៏រឹងមាំបែបនេះ លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មាន គួរតែត្រូវបានរៀបចំជាគោលការណ៍ណែនាំ ។ គួរតែកត់សម្គាល់ដែរថា ក្រសួង និងស្ថាប័នទាំងអស់មានភារកិច្ចទទួលខុសត្រូវក្នុងការបង្កើតដំណោះស្រាយសន្តិសុខព័ត៌មាន សម្រាប់ប្រព័ន្ធ ICT របស់ខ្លួនស្របតាមគោលការណ៍ណែនាំនេះ ។ ជាមួយគ្នានេះ ក៏ជាប្រការដ៏មានសារសំខាន់ផងដែរ ដែលត្រូវធានាអោយបាននូវសេវារដ្ឋបាលរបស់រាជរដ្ឋាភិបាលប្រកបដោយគុណភាពល្អ និងមានស្ថិរភាព។ ប្រការនេះមិនត្រឹមតែគ្រប់គ្រង ICT អោយបានល្អប៉ុណ្ណោះទេ ប៉ុន្តែថែមទាំងប្រឆាំងនឹងការគំរាមកំហែងផ្នែកសន្តិសុខព័ត៌មានដែលកាន់តែមានគ្រោះថ្នាក់ខ្លាំងឡើងៗជារៀងរាល់ថ្ងៃទៀតផង ។ ដូច្នេះលក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មាន គួរត្រូវធ្វើការត្រួតពិនិត្យ និងពិនិត្យមើលឡើងវិញ ។

(១) ការបង្កើតលក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GISSC)

រាល់ក្រសួង និងស្ថាប័នទាំងអស់ ត្រូវទទួលខុសត្រូវចំពោះការអភិវឌ្ឍប្រព័ន្ធ ICT របស់ខ្លួន ដែលរួមមានទាំងការអនុវត្តការការពារសន្តិសុខព័ត៌មានស្របតាមគោលការណ៍ណែនាំទូទៅរបស់រាជរដ្ឋាភិបាលផងដែរ ។ មជ្ឈមណ្ឌលជាតិគ្រប់គ្រងសន្តិសុខព័ត៌មាន មានភារកិច្ចទទួលខុសត្រូវជាចម្បងក្នុងការរៀបចំ និងធានាអោយបាននូវការអនុវត្តគោលការណ៍ណែនាំនេះផងដែរ ។ គោលការណ៍ណែនាំនេះ ហៅថាលក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលដែលត្រូវបានត្រួតពិនិត្យឡើងវិញ និងពណ៌នាយ៉ាងល្អិតល្អន់ជារៀងរាល់ឆ្នាំដែលឆ្លុះបញ្ចាំងដោយការវិវត្ត ផ្នែកបច្ចេកវិទ្យារបស់ឧក្រិដ្ឋជនអ៊ីនធឺណិត និងការផ្លាស់ប្តូរលក្ខណៈនៃការគំរាមកំហែង ។

ដោយពិចារណាទៅលើភាពបន្ទាន់នៃបញ្ហាសន្តិសុខព័ត៌មាន NiDA នឹងដើរតួនាទីបណ្តោះអាសន្នជាលេខាធិការដ្ឋាន NISC ក្រោយពីមានការធ្វើប្រតិភូកម្មដោយរាជរដ្ឋាភិបាលរហូតដល់មានការបង្កើត NISC ដោយយោងតាមការសម្រេចបាននូវតួនាទីមួយចំនួនដែលបានកំណត់ ។

GISSC រួមមានសមាសធាតុមួយចំនួនដូចខាងក្រោមនេះ ៖

- រចនាសម្ព័ន្ធអង្គភាព និងទំនួលខុសត្រូវ
- រដ្ឋបាល និងអធិការកិច្ច
- ការវាយតម្លៃអំពីធនធានព័ត៌មាន
- ការពិចារណាអំពីការការពារសន្តិសុខព័ត៌មានរបស់ប្រព័ន្ធអនុវត្តទាំងអស់
- ការពិចារណាអំពីការការពារសន្តិសុខព័ត៌មានសម្រាប់កុំព្យូទ័រមេ និងកុំព្យូទ័រកូនទាំងអស់
- ការពិចារណាអំពីការការពារសន្តិសុខព័ត៌មានរបស់ហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញ
- តម្រូវការសម្រាប់មុខងារសន្តិសុខព័ត៌មានទាំងអស់

(១) ការគ្រប់គ្រងការប្រើប្រាស់ យថាភាព ការដាក់លេខសម្ងាត់ ចំណុចខ្សោយ ផ្នែកសន្តិសុខ គ្រឿងបរិក្ខារ ឧបករណ៍ទូទៅសម្រាប់ប្រើប្រាស់អ៊ីនធឺណិត (ដូចជា network server (វែបសាយត៍ អ៊ីម៉ែល FTP, DNS ។ល។) ប្រព័ន្ធរបាំងការពារ (Firewall) ឧបករណ៍ភ្ជាប់បណ្តាញអ៊ីនធឺណិត (Router) ឧបករណ៍ភ្ជាប់បណ្តាញ (Switch) ...!

(២) ការត្រួតពិនិត្យឡើងវិញអំពីគោលនយោបាយសន្តិសុខព័ត៌មានរបស់ក្រសួង ដោយសារគ្រប់ក្រសួង និងស្ថាប័នទាំងអស់ មានការកិច្ចទទួលខុសត្រូវក្នុងការអភិវឌ្ឍ និងថែរក្សាប្រព័ន្ធ ICT របស់ខ្លួននោះ ជាការចាំបាច់ដែលត្រូវបង្កើតគោលនយោបាយ និងផែនការសន្តិសុខព័ត៌មានផ្ទាល់ខ្លួន ស្របតាមគោលការណ៍ណែនាំរបស់ GISSC ។ ភាពត្រឹមត្រូវ គឺជាចំណុចគន្លឹះដ៏សំខាន់នៅក្នុងបរិបទនេះ ។

(៣) ស្វ័យអធិការកិច្ច

គ្រប់ក្រសួង និងស្ថាប័នទាំងអស់ ត្រូវបានស្នើអោយធ្វើអធិការកិច្ចលើប្រព័ន្ធ ICT អោយបានទៀងទាត់យ៉ាងហោចណាស់អោយបានពីរ ឬ បីខែម្តងស្របតាម GISSC។ ប្រសិនបើរកឃើញថាមានចំណុចខ្វះខាត លើការប្រើប្រាស់មិនត្រឹមត្រូវនោះ គួរចាត់វិធានការសមស្របដែលរួមមានការកែតម្រូវជាបន្ទាន់ ។

(៤) ការត្រួតពិនិត្យឡើងវិញនូវមូលដ្ឋានវដ្ត PDCA

NISC ត្រូវត្រួតពិនិត្យឡើងវិញនូវរបាយការណ៍អធិការកិច្ចរបស់ក្រសួង ឬស្ថាប័ននីមួយៗអោយស្របតាមទស្សនៈត្រឹមត្រូវរបស់ GISSC ។ ប្រសិនបើរកឃើញថាមានភាពមិនស៊ីសង្វាក់គ្នា NISC គួរផ្តល់នូវមតិយោបល់ និងអនុសាសន៍ណែនាំអំពីរបៀប

កែតម្រូវលើភាពមិនស៊ីសង្វាក់គ្នានេះ ជូនដល់បណ្តាក្រសួង ឬស្ថាប័នទាំងនេះវិញ ។

(៥) ការជំរុញអោយមានការគាំទ្រដល់និរន្តភាពសន្តិសុខព័ត៌មាន
ជាការចាំបាច់ដែលតម្រូវអោយមានវិញ្ញាបនបត្របញ្ជាក់សន្តិសុខព័ត៌មានជាផ្លូវការ ដែល ចេញដោយអង្គការទទួលស្គាល់គុណភាពតាមនិយាមអន្តរជាតិ នៅពេលរាជរដ្ឋាភិបាលជាវផលិតផល ICT ដូចជា routers, switch, firewall, appliances ។ល។ លើសពីនេះទៅទៀតរាជរដ្ឋាភិបាលគួរតែជួលក្រុមហ៊ុនពិគ្រោះយោបល់ឬវិស្វកម្ម ICT ប្រសិនបើអាចទៅរួច ។ ជាការចាំបាច់ផងដែរ ដែលត្រូវផ្តល់ការបញ្ជាក់ដល់ក្រុមហ៊ុនសរសេរកម្មវិធី ថាតើ ក្រុមហ៊ុននេះ នឹងរក្សាកម្រិតគោលនយោបាយសន្តិសុខព័ត៌មាន និងដំណើរការគ្រប់គ្រងដូចៗគ្នាឬយ៉ាងណា ?

(៦) ការជំរុញអោយមានសន្តិសុខព័ត៌មានរបស់អង្គភាពពាក់ព័ន្ធនឹងរាជរដ្ឋាភិបាល
ជាការចាំបាច់ដែលអង្គភាពពាក់ព័ន្ធនឹងរាជរដ្ឋាភិបាល ត្រូវរក្សាកម្រិតដូចគ្នានៃដំណើរការគ្រប់គ្រងសន្តិសុខព័ត៌មានស្របតាម GISSC ។

(៧) ផែនការសម្របសម្រួលរវាង NISC ជាមួយនិងបណ្តាក្រសួង និងស្ថាប័ននានា ពាក់ព័ន្ធនឹងភាពងាយរងគ្រោះលើផ្នែក Software
NISC គួរតែមានការប្រាស្រ័យទាក់ទងល្អជាមួយបណ្តាក្រសួង និងស្ថាប័នទាំងអស់ជាពិសេសជាមួយក្រសួង ដែលគ្រប់គ្រងលើហេដ្ឋារចនាសម្ព័ន្ធ ICT សំខាន់ៗ ដើម្បីផ្លាស់ប្តូរព័ត៌មានអំពីការសិក្សា និងការវិភាគ លើភាពងាយរងគ្រោះរបស់ software ។ NISC គួរតែធ្វើការសិក្សាផងដែរអំពីវិធានការនានា និងនីតិវិធីការពារលើភាពងាយរងគ្រោះទាំងនោះ បើទទួលបាននូវព័ត៌មានចាំបាច់ពីការសិក្សានេះគឺ ត្រូវបញ្ជូនទៅគ្រប់ក្រសួង និងស្ថាប័នទាំងអស់អោយបានឆាប់បំផុតតាមដែលអាចធ្វើទៅបាន ។

(៨) ផែនការអភិវឌ្ឍន៍ធនធានមនុស្សផ្នែកសន្តិសុខព័ត៌មាន
ជាការពិបាកដែលរាជរដ្ឋាភិបាលត្រូវរក្សាចំនួនបុគ្គលិក និងវិស្វករសន្តិសុខព័ត៌មានអោយបានគ្រប់គ្រាន់ ដើម្បីអនុវត្តផែនការគ្រប់គ្រងសន្តិសុខព័ត៌មានតាមសេចក្តីត្រូវការ ។ ដូច្នេះហើយ NISC គួរតែរៀបចំផែនការសម្រាប់អភិវឌ្ឍធនធានមនុស្សផ្នែកថៃ

ទាំសន្តិសុខព័ត៌មាន ។ NISC ក៏បានតម្រូវអោយធ្វើការផ្សព្វផ្សាយគោលការណ៍ណែនាំស្តីពីការអភិវឌ្ឍ software លម្អិតសម្រាប់ការពារសន្តិសុខព័ត៌មាន ដែលនឹងចូលរួមចំណែកក្នុងការ អភិវឌ្ឍ software របស់ខ្លួនផងដែរ ។

(៩) ផែនការរយៈពេលមធ្យមសម្រាប់រាជរដ្ឋាភិបាល

NISC គួរតែរៀបចំកងកម្លាំងប្រភេទផ្សេងៗគ្នាសម្រាប់រាជរដ្ឋាភិបាលដើម្បីទប់ទល់នឹងឧប្បត្តិហេតុសន្តិសុខព័ត៌មាន ដែលអាចកើតមានឡើងជាយថាហេតុ ។ NISC ក៏ចាំបាច់ត្រូវដាក់ចេញផងដែរនូវគោលការណ៍ណែនាំស្តីពី លក្ខខណ្ឌតម្រូវផ្នែកសន្តិសុខព័ត៌មានជាមូលដ្ឋាន សម្រាប់លទ្ធកម្មពាក់ព័ន្ធនឹង ICT នៅក្នុងរាជរដ្ឋាភិបាល ដែលអនុវត្តទូទៅចំពោះគ្រប់ក្រសួង និងស្ថាប័នទាំងអស់ ។ គួរកត់សម្គាល់ផងដែរថា បេសកកម្មដ៏សំខាន់ របស់ NISC គឺត្រូវសហការ គ្រប់គ្រង សហប្រតិបត្តិការ និងសម្របសម្រួលក្នុងចំណោមក្រសួង និងស្ថាប័នពាក់ព័ន្ធនឹងបញ្ហាសន្តិសុខព័ត៌មាន ។

[ចប់គោលនយោបាយជាមូលដ្ឋានរបស់ GISSC]

មាតិកា

ផ្នែក ទី២

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មាន

របស់ រាជរដ្ឋាភិបាល (GISSC)

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល

១. មូលដ្ឋានគ្រឹះ

១.១ វិធានទូទៅ

១.១.១ ភាពចាំបាច់សម្រាប់ការរៀបចំឯកសារគ្រប់គ្រងសន្តិសុខព័ត៌មាន

តាមវិធានជាមូលដ្ឋាន គ្រប់ក្រសួង និ ងស្ថាប័នទាំងអស់មានការិច្ចទទួលខុសត្រូវ រៀបចំផែនការ និងអនុវត្តវិធានការសន្តិសុខព័ត៌មាន ដើម្បីចៀសវាងឧប្បត្តិហេតុណាមួយដែល អាចកើតមានឡើងចំពោះហេដ្ឋារចនាសម្ព័ន្ធ បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន (ICT) របស់ អង្គភាពពាក់ព័ន្ធ ។

រាជរដ្ឋាភិបាលគួរតែផ្តល់អោយគ្រប់ក្រសួង និងស្ថាប័នទាំងអស់នូវ"គោលនយោបាយ មូលដ្ឋានគ្រឹះ" និង ក្របខ័ណ្ឌរួមបញ្ចូលគ្នាមួយដែលជាគោលការណ៍ណែនាំនិយាម ដើម្បីអោយ គ្រប់ក្រសួងនិងស្ថាប័នទាំងអស់អាចអភិវឌ្ឍ និងកែលម្អនូវវិធានការសន្តិសុខព័ត៌មានអោយកាន់ តែប្រសើរឡើងប្រកបដោយភាពត្រឹមត្រូវ យោងតាមអាទិភាពផ្ទាល់ របស់អង្គភាពទាំងនោះ ។

ដោយសារមជ្ឈដ្ឋានសន្តិសុខព័ត៌មានមានការផ្លាស់ប្តូរយ៉ាងឆាប់រហ័សនោះ គោលការ ណ៍ណែនាំនេះគួរតែត្រូវបានពិនិត្យឡើងវិញអោយបានជាទៀងទាត់ ដើម្បីចៀសវាង និងបង្ការការ កើតមានឧប្បត្តិហេតុថ្មីៗផ្នែកសន្តិសុខ ។

ជាការសំខាន់យ៉ាងខ្លាំងក្នុងការកំណត់នូវបទបញ្ញត្តិនានា ស្តីពីការប្រើប្រាស់ទិន្នន័យ ដែលពណ៌នាអំពីគម្រោងការប្រើប្រាស់ធនធានព័ត៌មាន និងប្រព័ន្ធដំណើរការព័ត៌មានសម្ងាត់របស់ រាជរដ្ឋាភិបាល ។ ជាប្រការមួយដ៏ចាំបាច់ផងដែរដែលត្រូវកំណត់វិធាននានា ដើម្បីកុំអោយមាន ការរំលោភបំពានលើបទបញ្ញត្តិនានានោះ ។

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GISSC) ត្រូវបាន រៀបចំឡើងសម្រាប់គោលបំណងត្រួសត្រាយអំពីរបៀបពិចារណា និងអនុវត្តលក្ខណ្ឌតម្រូវ អប្បបរមាសម្រាប់ការគ្រប់គ្រងសន្តិសុខព័ត៌មាន នៅកម្រិតរាជរដ្ឋាភិបាលនៅក្នុងខ្លឹមសារនេះ ។

១.១.២ របៀបអនុវត្តឯកសារនេះនៅតាមគ្រប់ក្រសួង និងស្ថាប័នទាំងអស់

GISSC ត្រូវបានរៀបចំឡើងដើម្បីការពារធនធានព័ត៌មានរបស់រាជរដ្ឋាភិបាល ។ ធនធានព័ត៌មាន រួមមានដូច ខាងក្រោម ៖

- ទិន្នន័យដែលរក្សាទុកនៅក្នុងកុំព្យូទ័រ និង ប្រព័ន្ធផ្សព្វផ្សាយតាមប្រព័ន្ធអេឡិចត្រូនិច
- ឯកសារបោះពុម្ពដែលមានផ្ទុកសេចក្តីពិពណ៌នាអំពីប្រព័ន្ធ ICT
- ព័ត៌មានដែលបោះពុម្ពចេញពីកុំព្យូទ័រ ។

អ្នកប្រើប្រាស់ដែលបានគ្រោងទុករបស់ GISSC គឺរាល់បុគ្គលិករាជរដ្ឋាភិបាលទាំងអស់ រួមទាំងអ្នកពិគ្រោះយោបល់ ICT ដែលបានជួលមកបម្រើការងារជាដើមដែលមានលទ្ធភាពក្នុងការប្រើប្រាស់ទិន្នន័យ និងឯកសារសម្ងាត់នានា ។ វិធានការសន្តិសុខព័ត៌មានគួរតែត្រូវបានអនុវត្តជាអាទិភាព ។ អាទិភាពប្រែប្រួលទៅតាមសារសំខាន់ នៃធនធានព័ត៌មាន ឬផលប៉ះពាល់នៃការគំរាមកំហែងផ្នែកសន្តិសុខព័ត៌មាន ។

វិធានការសន្តិសុខព័ត៌មាន គួរតែមាននិរន្តរភាពគ្រប់គ្រាន់ ។ អាស្រ័យហេតុនេះ រាល់វិធានការទាំងអស់ គួរតែត្រូវបានពិនិត្យឡើងវិញអោយបានជាទៀងទាត់ដោយធ្វើយ៉ាងណាអោយមានភាពស៊ីសង្វាក់គ្នាជាមួយ GISSC ។

១.១.៣ ការវាយតម្លៃធនធានព័ត៌មាន និងវិធាននៃការប្រើប្រាស់ធនធានទាំងនោះ

ដើម្បីការពារព័ត៌មានស្តីពីសេវាកម្មរបស់រាជរដ្ឋាភិបាលពីឧប្បត្តិហេតុផ្សេងៗអោយមានសុវត្ថិភាព និងសន្តិសុខ ចាំបាច់ត្រូវធ្វើការវាយតម្លៃធនធានព័ត៌មានទាំងអស់នោះ ដើម្បីកំណត់លេខរៀងចំណាត់ថ្នាក់អាទិភាព (ការកំណត់អាទិភាព) ដោយយោងទៅតាមភាពងាយរងគ្រោះនៃព័ត៌មាននោះ ។ លេខរៀងទាំងនោះ ក៏ត្រូវបានប្រើប្រាស់ដើម្បីផ្តល់នូវវិធានសម្រាប់ប្រើប្រាស់ព័ត៌មានផងដែរ ។

ដើម្បីធ្វើចំណាត់ថ្នាក់ព័ត៌មានសេវាកម្មរបស់រាជរដ្ឋាភិបាល CIA ត្រូវពិចារណាទៅលើ ៖

- **C (ការសម្ងាត់) ៖** ការលេចចេញនូវទិន្នន័យ ព័ត៌មាន និងឯកសារសម្ងាត់បំផុត នឹងបណ្តាលអោយ មានការខូចខាតយ៉ាងធ្ងន់ធ្ងរដល់រាជរដ្ឋាភិបាលកម្ពុជា ។
- **I (ភាពត្រឹមត្រូវ) ៖** ការក្លែងបន្លំ ឬការធ្វើអោយខូចខាតព័ត៌មាន នឹងបណ្តាលអោយមានការខូចខាត ដល់រាជរដ្ឋាភិបាលកម្ពុជា ។
- **A (ភាពអាចមាន) ៖** ការហាមឃាត់មិនអោយចូលទៅប្រើប្រាស់ ឬការគ្មានលទ្ធភាពចូលទៅប្រើប្រាស់ព័ត៌មាន នឹងបណ្តាលអោយមានការខូចខាតដល់រាជរដ្ឋាភិបាលកម្ពុជា ។

រាល់ព័ត៌មានទាំងអស់ (ផ្នែកមូលដ្ឋានទិន្នន័យ) ត្រូវបានធ្វើចំណាត់ថ្នាក់ដោយយោងតាមភាពសំខាន់ និងភាពងាយរងគ្រោះរបស់ព័ត៌មានទាំងនេះ ។ ការប្រើប្រាស់ព័ត៌មាន ដូចជា ការថតចម្លង ការចែកចាយ ការបញ្ជូន និងការផ្ទេរព័ត៌មាន គួរតែត្រូវបានចាត់ចែងអោយបានសមស្រប ដើម្បីអោយព័ត៌មានទាំងឡាយនោះអាចត្រូវបានរឹតត្បិតត្រឹមត្រូវទៅតាមប្រភេទចំណាត់ថ្នាក់របស់ព័ត៌មានទាំងនោះ ។

១.២ ការរៀបចំ និងការអភិវឌ្ឍទំនួលខុសត្រូវ

១.២.១ ការរៀបចំ និងទំនួលខុសត្រូវ

ការរៀបចំ និងទំនួលខុសត្រូវចំពោះការគ្រប់គ្រងសន្តិសុខព័ត៌មាន គួរតែត្រូវបានពិចារណាស្របតាមចំណុចដូចខាងក្រោម ៖

(១) មន្ត្រីជាន់ខ្ពស់ផ្នែកសន្តិសុខព័ត៌មាន (GCIO) ត្រូវបានតែងតាំង ហើយមានទំនួលខុសត្រូវខ្ពស់បំផុត ចំពោះរាល់ការគ្រប់គ្រងសន្តិសុខព័ត៌មាននៅក្នុងក្រសួង ឬស្ថាប័នពាក់ព័ន្ធ ។

(២) គណៈកម្មាធិការគ្រប់គ្រងសន្តិសុខព័ត៌មាន (គណៈកម្មាធិការ ISM) ត្រូវបានរៀបចំឡើងនៅក្នុងក្រសួង ឬស្ថាប័ននីមួយៗ ដើម្បីរៀបចំផែនការអនុវត្ត ត្រួតពិនិត្យ និងពិនិត្យឡើងវិញនូវគំនិតផ្តួចផ្តើមសន្តិសុខព័ត៌មានរបស់ក្រសួង ឬស្ថាប័នពាក់ព័ន្ធ ។

(៣) អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវបានតែងតាំងនៅក្នុងក្រសួង ឬស្ថាប័ននីមួយៗដើម្បីគ្រប់គ្រងរាល់ការងារសន្តិសុខព័ត៌មានទាំងអស់ ។ អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ទទួលខុសត្រូវក្នុងការធានា និងរក្សានិរន្តរភាពនៃវិធានសន្តិសុខព័ត៌មាននានា ក្រោមការគ្រប់គ្រងរបស់ GCIO ។ កាតព្វកិច្ចដ៏សំខាន់របស់អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន គឺត្រូវរក្សាការប្រាស្រ័យទាក់ទងល្អជាមួយអ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់ក្រសួង ឬស្ថាប័នផ្សេងៗទៀត ។

(៤) ការរំលោភលើវិធាននានា

ប្រសិនបើបុគ្គលិករាជរដ្ឋាភិបាល ដឹងថាមានការរំលោភវិធានសន្តិសុខព័ត៌មាននោះ ចាំបាច់ត្រូវធ្វើការរាយការណ៍អំពីការប្រព្រឹត្តខុសឆ្គងបែបនេះទៅអ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានជាបន្ទាន់ ។ អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន នឹងចាត់វិធានការសមស្រប ។ ប្រសិនបើចាំបាច់គួររាយការណ៍ហេតុការណ៍នៃការរំលោក

លើវិធាននេះ ទៅ GCIO ។

១.២.២ ការរាយការណ៍អំពីការរំលោភលើវិធាននានា

ប្រសិនបើបុគ្គលិករាជរដ្ឋាភិបាលរកឃើញថា មានការរំលោភសន្តិសុខព័ត៌មានធ្ងន់ធ្ងរ នោះ បុគ្គលិករូបនោះត្រូវជូនដំណឹងមកកាន់អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានអំពីករណីបែបនេះ ។ អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន នឹងចាត់វិធានការសមស្របទៅតាមលទ្ធផល នៃការពិគ្រោះយោបល់ជាមួយ GCIO ។ អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ក៏ចាំបាច់ត្រូវជូនដំណឹងអំពីករណីរំលោភបំពាននេះទៅបុគ្គលិកបច្ចេកទេសសន្តិសុខព័ត៌មាន ជាបន្ទាន់រួមជាមួយនិងវិធានការដែលបានចាត់ចែងផងដែរ ។

១.២.៣ ការគ្រប់គ្រង

(១) ការអប់រំអំពីវិធានការសន្តិសុខព័ត៌មាន

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ទាំងអស់ ចាំបាច់ត្រូវរៀបចំផែនការ និងអនុវត្តការកិច្ចដូចខាងក្រោម ៖

- រៀបចំ និងថែរក្សាឯកសារនានាដែលពាក់ព័ន្ធនិងវិធានការទាំងឡាយស្តីពីសន្តិសុខព័ត៌មាន
- បង្កើតផែនការ និងបើកវគ្គបណ្តុះបណ្តាលអំពីសន្តិសុខព័ត៌មានដល់បុគ្គលិករាជរដ្ឋាភិបាលអោយបានយ៉ាងហោចណាស់មួយលើកជារៀងរាល់ឆ្នាំ ដើម្បីបង្កើនការយល់ដឹងអំពីសារសំខាន់នៃសន្តិសុខព័ត៌មាន និងការអនុវត្តសន្តិសុខព័ត៌មាននេះ ។

(២) ការដោះស្រាយការខូចខាត ឬឧប្បត្តិហេតុ

ក. ការត្រៀមលក្ខណៈចំពោះការកើតឡើងនូវការខូចខាត ឬឧប្បត្តិហេតុ

ក្រុមគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវត្រៀមលក្ខណៈរបស់ខ្លួនជានិច្ចកាល ដើម្បីឆ្លើយតបអោយបានឆាប់រហ័សទៅនឹង ឧប្បត្តិហេតុសន្តិសុខព័ត៌មានផ្សេងៗដើម្បីកាត់បន្ថយការខូចខាតមកត្រឹមកម្រិតអប្បបរមា និងស្តារឡើងវិញអោយបាននៅក្នុងរយៈពេលខ្លីបំផុត ។

ខ. ការរាយការណ៍ និងនីតិវិធីស្តារឡើងវិញបន្ទាន់នៅក្រោយពេលកើតមានការខូចខាត ឬជួបឧប្បត្តិហេតុ

នៅពេលមានការខូចខាត ឬជួបឧប្បត្តិហេតុ ត្រូវបានរកឃើញដោយបុគ្គលិករាជរដ្ឋា

កិបាល បុគ្គលិករូបនោះ ត្រូវធ្វើសេចក្តីរាយការណ៍ទៅបុគ្គលិកបច្ចេកទេសព័ត៌មានវិទ្យា(IT) ជាបន្ទាន់ដើម្បីទទួលបានការឆ្លើយតបអោយបានឆាប់ហើស ។ ស្របពេលជាមួយគ្នានោះ បុគ្គលិកបច្ចេកទេសព័ត៌មានវិទ្យា គួរតែទាក់ទង និងពិគ្រោះយោបល់ជាមួយអ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន អំពីវិធានការដែលត្រូវអនុវត្ត ។

១.២.៤ អធិការកិច្ច

គ្រប់ក្រសួង និងស្ថាប័នទាំងអស់ ត្រូវធ្វើស្វ័យអធិការកិច្ចចំពោះការគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដូចជា ការវាយតម្លៃគុណភាព និងអនុវត្តស្វ័យអធិការកិច្ចនេះពីដងក្នុងមួយឆ្នាំ ។ លទ្ធផលនៃការធ្វើស្វ័យអធិការកិច្ច គួរត្រូវរាយការណ៍ ជូន GCIO។

រាល់របាយការណ៍ស្វ័យអធិការកិច្ចទាំងអស់ នឹងត្រូវសង្ខេបដោយ NiDA ដែលទទួលខុសត្រូវអនុវត្តការងារ នេះក្នុងនាមជាលេខាធិការដ្ឋាននៃមជ្ឈមណ្ឌលជាតិគ្រប់គ្រងសន្តិសុខព័ត៌មាន ហើយបន្ទាប់មក នឹងត្រូវដាក់បញ្ចូលទៅក្នុងគេហទំព័ររបស់រាជរដ្ឋាភិបាល សម្រាប់ធ្វើការចែកចាយព័ត៌មានផ្ទៃក្នុងទាំងនេះ នៅក្នុងចំណោមបុគ្គលិករាជរដ្ឋាភិបាល ។ គ្រប់ក្រសួង និងស្ថាប័នទាំងអស់ ត្រូវបានស្នើសុំអោយកែលម្អវិធានការសន្តិសុខព័ត៌មានអោយមានលក្ខណៈកាន់តែប្រសើរឡើង ប្រសិនបើរកឃើញចំណុចខ្សោយណាមួយនៃវិធានការទាំងនោះ ។

១.២.៥ ការពិនិត្យឡើងវិញទៅលើគោលការណ៍ណែនាំ

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងបុគ្គលិកបច្ចេកទេសព័ត៌មានវិទ្យាទាំងអស់ត្រូវបានតម្រូវអោយធ្វើការពិនិត្យឡើងវិញជាប្រចាំ ទៅលើគោលការណ៍ណែនាំនានាដែលមានស្រាប់ ដើម្បីរកមើលនូវភាពមិនស៊ីសង្វាក់គ្នា ភាពមិនគ្រប់គ្រាន់ និងភាពគ្មានបច្ចុប្បន្នភាពនៃគោលការណ៍ណែនាំ នៅក្នុងភាពត្រឹមត្រូវនៃមជ្ឈដ្ឋានសន្តិសុខព័ត៌មានចុងក្រោយបង្អស់ ។ ប្រសិនបើរកឃើញថាមានចំណុចដែលមានបញ្ហាធ្ងន់ធ្ងរនោះ អាជ្ញាធរថ្នាក់លើគួរតែធ្វើការណែនាំអំពីចំណុចទាំងនោះ ។

១.២.៦ ការប្រើប្រាស់បុគ្គលិកខាងក្រៅ

នៅពេលការងារអភិវឌ្ឍន៍កម្មវិធីកុំព្យូទ័រ (software) ដំណើរការព័ត៌មាន ការអង្កេតនិងការសិក្សា ត្រូវបានធ្វើឡើងដោយប្រើប្រាស់បុគ្គលិកខាងក្រៅក្រសួង និងស្ថាប័ន គួរតែរក្សាសន្តិសុខព័ត៌មានរបស់បុគ្គលិកខាងក្រៅ ក្នុងកម្រិត ដូចគ្នានឹងការរក្សាទុកផ្ទាល់របស់ខ្លួន ។ នៅក្នុងបរិបទនេះ ក្រសួង ឬស្ថាប័នអាចផ្តល់អោយបុគ្គលិកខាងក្រៅ នូវរាល់លក្ខខណ្ឌតម្រូវទាំងអស់នៃគោលនយោបាយ និងគោលការណ៍ណែនាំស្តីពីសន្តិសុខព័ត៌មានដែលអាចមាន ។

១.៣ ការប្រើប្រាស់ធនធានព័ត៌មាន

១.៣.១ ការប្រើប្រាស់ទិន្នន័យ

(១) ការបង្កើត និងការបញ្ចូលទិន្នន័យ

បុគ្គលិករាជរដ្ឋាភិបាល ត្រូវអនុវត្តតាមវិធាននៃការប្រើប្រាស់ព័ត៌មានដែលមាននៅក្នុងមូលដ្ឋាននៃការបង្កើតទិន្នន័យ ។

(២) ការប្រើប្រាស់ទិន្នន័យ

បុគ្គលិករាជរដ្ឋាភិបាល ត្រូវចាត់ចែងព័ត៌មានអោយបានត្រឹមត្រូវ យោងទៅតាមវិធានចំណាត់ថ្នាក់ព័ត៌មាន របស់រាជរដ្ឋាភិបាល ។ នៅពេលថតចម្លងព័ត៌មាន ព័ត៌មាននោះគួរតែត្រូវបានចាត់ចែងដោយយោងតាមចំណាត់ថ្នាក់ព័ត៌មានសម្ងាត់ជាដើម ។

(៣) ការរក្សាទុកទិន្នន័យ

ការចូលប្រើប្រាស់ព័ត៌មានដែលបានរក្សាទុក ត្រូវអនុវត្តតាមវិធានដូចខាងក្រោម ៖

- ការគ្រប់គ្រងការប្រើប្រាស់
- ការគ្រប់គ្រងអត្តសញ្ញាណ និងលេខសម្ងាត់
- ការបំលែងទៅជាកូដ ប្រសិនបើចាំបាច់ ។

(៤) ការផ្ទេរទិន្នន័យ

ការផ្ទេរព័ត៌មានទៅកាន់កុំព្យូទ័រដទៃទៀត ចាំបាច់ត្រូវមានការអនុញ្ញាតពីអ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ជាមុនសិន ប្រសិនបើព័ត៌មាននោះស្ថិតក្នុងចំណាត់ថ្នាក់សន្តិសុខកម្រិតខ្ពស់។ ការការពារដោយលេខសម្ងាត់ និងការចម្លងព័ត៌មានទុក ក៏ត្រូវការជាចាំបាច់ផងដែរ ។

(៥) ការបោះពុម្ពទិន្នន័យ

នៅពេលដែលព័ត៌មានរបស់រាជរដ្ឋាភិបាលត្រូវបានបោះពុម្ពផែនការប្រើប្រាស់ព័ត៌មានគួរត្រូវបានត្រួតពិនិត្យ និងបញ្ជាក់អោយបានច្បាស់លាស់ ។ ចាំបាច់ត្រូវមានការអនុញ្ញាតពីសំណាក់អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានផងដែរ ។

(៦) ការលុបទិន្នន័យ

នៅពេលត្រូវការលុបព័ត៌មានរបស់រាជរដ្ឋាភិបាល ត្រូវធានាអោយប្រាកដថាមិនមាននរ

ណាម្នាក់អាចទាញយក ឯកសារដែលលុបហើយ មកវិញបានឡើយ ។

១.៤ វិធានការចំពោះដំណើរការព័ត៌មាន

១.៤.១ ការរឹតត្បិតចំពោះដំណើរការព័ត៌មាននៅក្រៅដួរាជរដ្ឋាភិបាល

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន គួររៀបចំ និងប្រកាន់ខ្ជាប់នូវវិធានសន្តិសុខព័ត៌មាន ចំពោះការម៉ៅការការងារអោយទៅប្រភពខាងក្រៅ។ អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ក៏គួររៀបចំ និងប្រកាន់ខ្ជាប់នូវវិធានសន្តិសុខព័ត៌មានផងដែរ ចំពោះរាល់ដំណើរការព័ត៌មានចាំបាច់របស់ រាជរដ្ឋាភិបាលដែលត្រូវបានម៉ៅការអោយទៅប្រភពខាងក្រៅដោយអន្លើ ឬទាំងស្រុងនោះ។ ការ អនុញ្ញាតពីសំណាក់ GCIO ព្រមទាំងអ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវមានជាចាំបាច់សម្រាប់ ការម៉ៅការការងារអោយទៅប្រភពខាងក្រៅ ។

១.៤.២ ការរឹតត្បិតទៅលើការប្រើប្រាស់ Saas (កម្មវិធីកុំព្យូទ័រសម្រាប់សេវាកម្ម)

ការប្រើប្រាស់ Saas អាចចាត់ទុកថាជាប្រភេទមួយនៃការម៉ៅការការងារអោយទៅ ប្រភពខាងក្រៅ ។ ក្នុងករណីនេះ ត្រូវយកកថាខណ្ឌ ១.៤.១ ខាងលើមកអនុវត្ត ។ ការបញ្ជាក់អំពីកិច្ចព្រមព្រៀងសេវាកម្ម (SA) គឺជាកត្តា សំខាន់បំផុតនៅក្នុងចំណុចនេះ ។ SA គួរតែត្រូវបានវាយតម្លៃលម្អិត ដោយ GCIO និងអ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ។

១.៥ វិធានការចំពោះប្រព័ន្ធដំណើរការព័ត៌មាន

១.៥.១ លក្ខខណ្ឌតម្រូវសម្រាប់សន្តិសុខព័ត៌មាន

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានគួរពិចារណាលើចំណុចសន្តិសុខដែលមានដូចខាង ក្រោម នៅពេលធ្វើផែនការសម្រាប់គម្រោង អភិវឌ្ឍន៍ប្រព័ន្ធព័ត៌មាន ។

- លក្ខខណ្ឌតម្រូវសម្រាប់សន្តិសុខព័ត៌មាន
- ការមានបុគ្គលិករក្សាសន្តិសុខព័ត៌មានដែលមានចំណេះដឹង និងជំនាញ គ្រប់គ្រាន់ផ្នែកសន្តិសុខព័ត៌មាន
- វិធានការសន្តិសុខព័ត៌មានដែលចាំបាច់សម្រាប់ការអភិវឌ្ឍ និងប្រតិបត្តិការ

១.៥.២ វិធានអភិវឌ្ឍន៍ និងការអនុវត្តតាមប្រព័ន្ធដំណើរការព័ត៌មាននៅកម្រិតរាជរដ្ឋាភិបាល

(១) ការរៀបចំឯកសារ និងកំណត់ត្រា

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវរៀបចំ និងថែរក្សាឯកសារដូចខាងក្រោម ៖

- បញ្ជីអ្នកប្រើប្រាស់ និងកំណត់ត្រារបស់អ្នកប្រើប្រាស់
- បញ្ជីឈ្មោះ software ជាមួយនឹងលេខសំណៅ/កំណែប្រែ និងប្រវត្តិដែលមានបច្ចុប្បន្នភាព
- លក្ខខណ្ឌតម្រូវ លក្ខណៈបច្ចេកទេស និងឯកសារគម្រោង
- សៀវភៅណែនាំអំពីលំហូរការងារសម្រាប់ការឆ្លើយតបចំពោះការខូចខាត និងឧប្បត្តិហេតុនានា ។

(២) លទ្ធកម្មសម្ភារៈបរិក្ខារ

GCIO និងអ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវរៀបចំ និងប្រកាន់ខ្ជាប់នូវនីតិវិធីលទ្ធកម្ម ដើម្បីទិញសម្ភារៈបរិក្ខារ និង ឧបករណ៍ផ្សេងៗ ផ្អែកតាមតម្រូវការសម្រាប់សន្តិសុខព័ត៌មាន ។

(៣) ការអភិវឌ្ឍកម្មវិធីកុំព្យូទ័រ (software)

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ចាំបាច់ត្រូវរៀបចំ និងប្រកាន់ខ្ជាប់នូវគោលការណ៍ណែនាំដូចខាងក្រោមសម្រាប់គម្រោង អភិវឌ្ឍកម្មវិធីកុំព្យូទ័រ (software)

- រៀបចំក្រុមអភិវឌ្ឍន៍ ដែលរួមមានបុគ្គលិកដែលអាចទទួលខុសត្រូវអនុវត្ត និងដោះស្រាយលក្ខខណ្ឌត្រូវតាមផ្នែកសន្តិសុខព័ត៌មាន
- រៀបចំឯកសារគម្រោងច្បាស់លាស់ស្តីពីការអនុវត្តសន្តិសុខព័ត៌មានដែលតម្រូវអោយមានជាចាំបាច់
- កំណត់វិសាលភាពនៃការពិនិត្យមើលឡើងវិញនូវគម្រោងនិងនីតិវិធីក្នុងការអនុវត្ត
- ផ្តល់នូវការគ្រប់គ្រងលើការចូលប្រើប្រាស់ព័ត៌មានសមស្រប និងវិធីសាស្ត្រចម្លងព័ត៌មានទុកសម្រាប់ឯកសារកូដដើម
- កំណត់វិសាលភាពនៃការពិនិត្យមើលកូដដើមឡើងវិញ និងនីតិវិធីនៃការអនុវត្ត
- កំណត់នូវចំណុចនិងនីតិវិធីក្នុងការធ្វើតេស្តសមស្របដោយយោងតាមលក្ខខណ្ឌតម្រូវសន្តិសុខព័ត៌មាន
- កត់ត្រា និងផ្សៀងផ្ទាត់ទិន្នន័យលទ្ធផលនៃការធ្វើតេស្ត ។

(៤) គោលការណ៍ណែនាំស្តង់ដារសម្រាប់ការដាក់លេខសម្ងាត់ និងហត្ថលេខាឌីជីថល

ចាំបាច់ត្រូវកំណត់ និង ប្រើប្រាស់ប្រព័ន្ធកម្មវិធីកុំព្យូទ័របំលែងទិន្នន័យទៅជាកូដសម្ងាត់របស់រាជរដ្ឋាភិបាល ។ កូដដែលប្រើប្រាស់សម្រាប់បំលែងទិន្នន័យទៅជាកូដសម្ងាត់ និងហត្ថលេខាឌីជីថល គួរត្រូវថតចម្លងទុក និងរក្សាទុក អោយមានសុវត្ថិភាព ។

(៥) ការរក្សាអោយបានល្អនូវជំនាញផ្នែកសន្តិសុខព័ត៌មាន

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវបង្កើត និង ប្រកាន់ខ្ជាប់នូវវិធានការគ្រប់គ្រាន់សម្រាប់ការទប់ស្កាត់ការរំលោភបំពានលើវិធានសន្តិសុខព័ត៌មាននៅក្នុងសកម្មភាពនានានៅក្រៅរាជរដ្ឋាភិបាល ។

(៦) វិធានសម្រាប់ការប្រើប្រាស់ឈ្មោះ domain

គ្រប់ក្រសួង និងស្ថាប័នរដ្ឋទាំងអស់ចាំបាច់ត្រូវតែប្រើប្រាស់ឈ្មោះ domain របស់រាជរដ្ឋាភិបាលខាងក្រោមនេះដោយគ្មានករណីលើកលែងឡើយ ។

បច្ចុប្បន្ននេះ ឈ្មោះ domain របស់រាជរដ្ឋាភិបាលគឺ "gov.kh" ។

(៧) ការងារប្រចាំថ្ងៃដើម្បីចៀសវាងការឆ្លងមេរោគ (malware) ចូលក្នុងកុំព្យូទ័រ

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវរៀបចំ និងប្រកាន់ខ្ជាប់នូវគោលការណ៍ណែនាំខាងក្រោមដើម្បីចៀសវាងការឆ្លងមេរោគ (malware) ចូលក្នុងកុំព្យូទ័រ ៖

- ធ្វើបច្ចុប្បន្នភាព (Update)ប្រព័ន្ធប្រតិបត្តិការអោយបានជាទៀងទាត់ ។ នៅក្នុងន័យនេះ មានន័យថា ត្រូវប្រើប្រព័ន្ធប្រតិបត្តិការដែលបានធ្វើបច្ចុប្បន្នភាពជាប្រចាំ ។
- ត្រូវប្រើកម្មវិធីរក្សាសន្តិសុខ (កម្មវិធីប្រឆាំងមេរោគ ឬកម្មវិធីប្រឆាំង spyware) ។
- ត្រូវធ្វើបច្ចុប្បន្នភាពសំណុំឯកសារកម្មវិធីប្រឆាំងមេរោគ/កម្មវិធីប្រឆាំង spyware (Anti-virus/ Anti-spyware definition file update) អោយបានជាប់ជាប្រចាំ
- មិនត្រូវទាញយក និងបើកសំណុំឯកសារដែលមានផ្ទុកមេរោគដូចជាប្រភេទ malware ឡើយ
- បើកអោយដំណើរការស្វ័យបច្ចុប្បន្នភាព (Auto update) លើកម្មវិធីរក្សាសន្តិសុខ ។

- ត្រួតពិនិត្យសំណុំឯកសារ(Virus Scan)ដោយកម្មវិធីរក្សាសន្តិសុខនៅពេលធ្វើការផ្ទេរឯកសារទាំងនោះ
- ត្រូវផ្តាច់ខ្សែបណ្តាញ (LAN) ចេញពីម៉ាស៊ីនកុំព្យូទ័រភ្លាមនៅពេលរកឃើញថាម៉ាស៊ីនកុំព្យូទ័រនោះអាចមានមេរោគ ដោយកម្មវិធីរក្សាសន្តិសុខមិនថាមានមេរោគជាក់ស្តែង ឬមិនទាន់ឃើញជាក់ស្តែងឡើយ ។

២. ការដំណើរការព័ត៌មាន

២.១ វិធានការក្នុងការរៀបចំលម្អិតអំពីលក្ខខណ្ឌតម្រូវសម្រាប់សន្តិសុខព័ត៌មាន

២.១.១ មុខងារសន្តិសុខព័ត៌មាន

(១) ការគ្រប់គ្រងអត្តសញ្ញាណកម្ម

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានគួរគ្រប់គ្រងអ្នកប្រើប្រាស់ (user) ទាំងអស់ដោយប្រើអត្តសញ្ញាណ (អត្តសញ្ញាណអ្នកប្រើប្រាស់ និងលេខសម្ងាត់) ដើម្បីចាត់ចែងអ្នកប្រើប្រាស់ទាំងឡាយអោយដំណើរការចូលប្រព័ន្ធដំណើរការព័ត៌មានប្រកបដោយសន្តិសុខ ។ គ្រប់លេខសម្ងាត់ទាំងអស់ត្រូវផ្លាស់ប្តូរជាទៀងទាត់ ។ ប្រព័ន្ធកំណត់អត្តសញ្ញាណ គួរតែត្រូវបានដំឡើង ដើម្បីផ្តល់ជាសញ្ញាដាស់តឿនដល់អ្នកប្រើប្រាស់ម្នាក់ៗអំពីភាពចាំបាច់នៃលេខសម្ងាត់ នៅចន្លោះរយៈពេលជាក់លាក់មួយ ។ ឧទាហរណ៍ បីខែម្តងជាដើម ។ កុំព្យូទ័រគួរតែត្រូវបានកំណត់មិនអោយដំណើរការដោយគ្មានការផ្លាស់ប្តូរលេខសម្ងាត់នៅ ក្នុងបរិបទនេះ ។

ជាការចាំបាច់យ៉ាងខ្លាំង ដែលត្រូវបំលែងអោយទៅជាកូដ (encryption) ទិន្នន័យអំពីអត្តសញ្ញាណ និងលេខសម្ងាត់ នៅពេលដែលទិន្នន័យទាំងនោះ ត្រូវបានរក្សាទុកនៅក្នុងកុំព្យូទ័រ ឬត្រូវបានផ្ទេរទៅកាន់កុំព្យូទ័រមួយទៀត ។ ជាអនុសាសន៍ អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានគួរតែថែរក្សានិងធ្វើបច្ចុប្បន្នភាពទិន្នន័យរបស់កុំព្យូទ័រអ្នកប្រើប្រាស់ដោយផ្អែកតាមវិធានរដ្ឋបាល និង តាមការផ្លាស់ប្តូររបស់អង្គភាព ។

(២) មុខងារគ្រប់គ្រងការប្រើប្រាស់

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវគ្រប់គ្រងការប្រើប្រាស់ ចំពោះរាល់អ្នកប្រើប្រាស់ទាំងអស់ដែលមានបំណងចូលទៅក្នុងប្រព័ន្ធដំណើរការព័ត៌មាននៅក្នុងក្រសួង ឬស្ថាប័នពាក់ព័ន្ធ ។

(៣) មុខងារគ្រប់គ្រងបុព្វសិទ្ធិ

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានចាំបាច់ត្រូវគ្រប់គ្រងបុព្វសិទ្ធិចំពោះបណ្តាអ្នកប្រើប្រាស់ដោយដាក់កូដភ្ជាប់ (extension) ទៅនឹងការគ្រប់គ្រងអត្តសញ្ញាណ និងលេខសម្ងាត់ ។ បុព្វសិទ្ធិពាក់ព័ន្ធទៅនឹងប្រតិបត្តិការគ្រប់គ្រងព័ត៌មាន ដូចជា ការបញ្ជាក់បន្ថែម ការផ្លាស់ប្តូរការធ្វើបច្ចុប្បន្នភាព ការលុបចោល និងការផ្ទេរជាដើម ។

(៤) មុខងារត្រួតពិនិត្យកំណត់ត្រា

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវពិនិត្យតាមដានប្រព័ន្ធដំណើរការព័ត៌មាន ដោយប្រើមុខងារពិនិត្យតាមដានកំណត់ត្រា សម្រាប់ការអង្កេត ។ វិសាលភាពនៃការពិនិត្យតាមដានកំណត់ត្រា និងមុខងារនៃការពិនិត្យតាមដាននេះ នឹងរួមមានដូចជា បញ្ហាវិនិច្ឆ័យ ការត្រួតពិនិត្យរបាយការណ៍ ។ល។ ដែលនឹងប្រែប្រួលយោងទៅតាមលក្ខខណ្ឌតម្រូវរបស់ប្រព័ន្ធដំណើរការព័ត៌មាន ។

(៥) មុខងារជានាវ៉ាប់រង

អ្នកគ្រប់គ្រងម៉ាស៊ីនកុំព្យូទ័រត្រូវមានវិធានការសម្រាប់មុខងារជានាវ៉ាប់រង ចំពោះរាល់ប្រព័ន្ធដំណើរការព័ត៌មានទាំងមូលដូចជា ការទាញយកឯកសារត្រឡប់មកវិញ ការចម្លងឯកសារទុក និងការរក្សាទុកឯកសារ។

(៦) លេខសម្ងាត់ និងហត្ថលេខាឌីជីថល (រួមទាំងការគ្រប់គ្រងកូដសម្ងាត់ផងដែរ)

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវធ្វើការពិចារណាអំពីការដាក់អោយប្រើប្រាស់នូវមុខងារប្រើលេខសម្ងាត់ សម្រាប់ការគ្រប់គ្រងព័ត៌មានសម្ងាត់បំផុតរបស់រាជរដ្ឋាភិបាល ។ មុខងារហត្ថលេខាឌីជីថល និងវិធីគ្រប់គ្រងកូដសម្ងាត់សុវត្ថិភាព ក៏គួរតែត្រូវបានពិចារណាក្នុងគោលបំណងដូចគ្នានេះផងដែរ ។

២.១.២ ការគំរាមកំហែងដល់សន្តិសុខព័ត៌មាន

(១) វិធានការទប់ស្កាត់ចំណុចខ្សោយផ្នែកសន្តិសុខ

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានគួរតែធ្វើការសិក្សាអំពីវិធានការនានាជាប្រចាំ ដើម្បីចៀសវាងកុំអោយមានចំណុចខ្សោយផ្នែកសន្តិសុខណាមួយនៅក្នុងប្រព័ន្ធពត៌មាន និងប្រព័ន្ធទំនាក់ទំនងដែលបានដំឡើងរួច ។ អាស្រ័យហេតុនេះ ការសិក្សា ជាប់ជាប្រចាំអំពីការប្រមូលព័ត៌មានស្តីពីការធ្វើបច្ចុប្បន្នភាពនៃចំណុចខ្សោយផ្នែកសន្តិសុខ គឺជាកិច្ចការមួយដែលចាំបាច់ត្រូវតែធ្វើជាដាច់ខាត ។

(២) វិធានការប្រឆាំងនឹងកម្មវិធីមេរោគ (malware)

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវដំឡើងកម្មវិធីរក្សាសន្តិសុខនៅក្នុងគ្រប់កុំព្យូទ័រទាំងអស់ដើម្បីការពារការឆ្លងកម្មវិធីមេរោគ (malware) ដែលរួមមានដូចជាមេរោគប្រភេទវីរុស និង spyware ជាដើម ។

(៣) វិធានការប្រឆាំងនឹងការវាយប្រហាររបស់ DDoS

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវធ្វើការសិក្សា និងត្រៀមរៀបចំគ្រប់មុខងារទាំងអស់ដែលអាចធ្វើទៅបាន ដើម្បីទប់ស្កាត់ការវាយប្រហាររបស់ DDoS (ការបដិសេធមិនចែកចាយសេវា) ដោយសម្របសម្រួលនិងសហការជាមួយក្រុមហ៊ុនផ្តល់សេវាអ៊ីនធើណែត ISPs, CSIRT ។ល។ ដែលកំពុងធ្វើការសម្រាប់ការរក្សាសន្តិសុខព័ត៌មាន នៅក្នុង និងក្រៅប្រទេសកម្ពុជា ។

(៤) វិធានការចំពោះការវាយប្រហារជាជំណាក់កាល (stepping-stone attacks)

ការវាយប្រហារតាមរយៈប្រព័ន្ធអ៊ីនធើណែត ប្រើប្រាស់ការវាយប្រហារជាជំណាក់កាលដើម្បីលាក់អត្តសញ្ញាណ ។ អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវចាត់វិធានការគ្រប់បែបយ៉ាងដែលអាចមាន ដើម្បីតាមចាប់ការវាយប្រហារប្រភេទនេះ ។ ដោយសារវិធានការទាំងនេះ ត្រូវបានសិក្សានៅក្នុងបណ្តាមន្ទីរពិសោធន៍ ក្រុមហ៊ុនរក្សាសន្តិសុខព័ត៌មាន ក្រុមហ៊ុនសារគមនាគមន៍ សាកលវិទ្យាល័យ ។ល។ នៅក្នុងប្រទេសជាច្រើន អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវលៃលកយ៉ាងណាទៅសិក្សាជាប្រចាំអំពីវិធានការអនុវត្តដើម្បីអាចបញ្ឈប់ការកើតមានសាជាថ្មីនូវសកម្មភាព hacking ឬការវាយប្រហារផ្សេងៗ និងដើម្បីកាត់បន្ថយការខូចខាតដល់ប្រព័ន្ធដំណើរការព័ត៌មានអោយនៅត្រឹមកម្រិតអប្បបរមា ។

២.២ វិធានការចំពោះសមាសធាតុប្រព័ន្ធព័ត៌មាន

២.២.១ ទីតាំង និងមជ្ឈដ្ឋាន

គួរពិចារណាអំពីកន្លែងសុវត្ថិភាពដែលល្អប្រសើរសម្រាប់ធ្វើការដំឡើងម៉ាស៊ីនកុំព្យូទ័រមេ និងឧបករណ៍ភ្ជាប់បណ្តាញកុំព្យូទ័រ ។

ក. ការគ្រប់គ្រងច្រកចូលទៅកាន់ទីតាំង

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវគ្រប់គ្រងអ្នកដែលគ្មានការអនុញ្ញាត ដែលពាក់ព័ន្ធនឹងការចូលទៅកាន់តំបន់ហាមឃាត់ ដែលនៅក្នុងតំបន់នេះមានដំឡើង

គ្រឿងបរិក្ខារដែលតម្រូវអោយមានសន្តិសុខកម្រិតខ្ពស់ ។ នៅក្នុងបរិបទនេះ ចាំបាច់ត្រូវដាក់កុំព្យូទ័រនានា ឧបករណ៍បន្ទាប់បន្សំ និងគ្រឿងកុំព្យូទ័រ អោយនៅដាច់ដោយឡែកជាលក្ខណៈរូបវន្ត និងដាច់ដោយឡែកពីកន្លែងធ្វើការងារធម្មតាផ្សេងៗទៀត ។ គួរពិចារណារៀបចំអោយមានការចាក់សោ និងប្រព័ន្ធប្រកាសអាសន្នជាលក្ខណៈរូបវន្តអោយបានគ្រប់គ្រាន់ ។ ការចូលទៅកាន់ទីតាំងទាំងនោះក៏គួរតែត្រូវបានគ្រប់គ្រង និងកត់ត្រាទុកផងដែរ ។

ខ. ការគ្រប់គ្រងភ្ញៀវ

ភ្ញៀវគួរតែចុះឈ្មោះនៅកន្លែងច្រកចូលដើម្បីជានាសន្តិសុខ ហើយប្រតិបត្តិការនេះ គួរតែត្រូវបានធ្វើឡើងដោយផ្អែកតាមវិធាននានាអោយបានត្រឹមត្រូវ ។ យ៉ាងហោចណាស់ ព័ត៌មានអំពីភ្ញៀវ (ឈ្មោះ មុខតំណែង និងគោលបំណងដែលចូលមកក្នុងអង្គភាព និងម៉ោងចូល/ចេញ) និងហត្ថលេខា របស់អ្នកអនុញ្ញាត ត្រូវបានកត់ត្រាទុកនៅក្នុងបញ្ជីកំណត់ហេតុ ហើយរបស់របរផ្ទាល់ខ្លួនរបស់ភ្ញៀវត្រូវរក្សាទុក នៅច្រកចូល ។

គ. ការការពារពីការលួច

កុំព្យូទ័រ និងឧបករណ៍គមនាគមន៍ ឧបករណ៍បន្ទាប់បន្សំ និងគ្រឿងកុំព្យូទ័រ គួរតែត្រូវបានការពារពីការលួច ដោយវិធានការគ្រប់គ្រាន់ ។

ឃ. ការគ្រប់គ្រងសន្តិសុខនៅក្នុងតំបន់ហាមឃាត់

បុគ្គលិករូបណាក៏ដោយ ត្រូវកាន់ប័ណ្ណសម្គាល់ខ្លួន ។ បើគ្មានប័ណ្ណសម្គាល់ខ្លួនទេ គ្មានបុគ្គលណាម្នាក់ត្រូវបាន អនុញ្ញាតអោយចូលទៅក្នុងតំបន់ហាមឃាត់បានឡើយ ។

ង. ការគ្រប់គ្រងគ្រោះមហន្តរាយ និងការខូចខាត

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវធ្វើការការពារជារូបវន្តសម្រាប់កុំព្យូទ័រ និងឧបករណ៍ភ្ជាប់បណ្តាញកុំព្យូទ័រ ព្រមទាំងឧបករណ៍ បន្ទាប់បន្សំ និងគ្រឿងកុំព្យូទ័រ ដើម្បីចៀសវាង ឬកាត់បន្ថយអោយនៅត្រឹមអប្បបរមា នូវការខូចខាតដែលបណ្តាលមកពីកាលៈទេសៈមើលមិនឃើញជាមុន ដូចជាគ្រោះមហន្តរាយ

ជាដើម ។ ចាំបាច់ត្រូវបិទចរន្តអគ្គិសនីដែលផ្គត់ផ្គង់ទីតាំងផងដែរ ដោយយកចិត្តទុកដាក់ចំពោះសុវត្ថិភាពរបស់បុគ្គលិកទាំងអស់ ដែលធ្វើការងារនៅពេលដែលកើតមានឧប្បត្តិហេតុបែបនេះ ។

២.២.២ កុំព្យូទ័រ

(១) ការរៀបចំផែនការសមត្ថភាព

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវធ្វើការសិក្សាអំពីការរៀបចំផែនការអោយបានត្រឹមត្រូវសម្រាប់សមត្ថភាពប្រព័ន្ធកុំព្យូទ័រ ត្រួតពិនិត្យការបញ្ចូលទិន្នន័យទៅក្នុងប្រព័ន្ធកុំព្យូទ័រ ចរាចរណ៍បណ្តាញ និងការកើតមាននូវកំហុសរបស់មនុស្ស ។ល។

(២) ការរៀបចំកម្មវិធីសម្រាប់កុំព្យូទ័រកូន (client)

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវចាត់ចែងរាល់ការដំឡើងកម្មវិធីកុំព្យូទ័រកូនទាំងអស់ ។ ទាំងកុំព្យូទ័រលើតុ និងកុំព្យូទ័រយួរដៃ គួរតែត្រូវបានរក្សាក្នុងកម្រិតរៀបចំសន្តិសុខព័ត៌មានដូចគ្នាក្នុងករណីអង្គភាពដូចគ្នា ទោះបីជាកុំព្យូទ័រយួរដៃអាច ត្រូវបានប្រើប្រាស់នៅក្រៅការិយាល័យរដ្ឋាភិបាលក៏ដោយ ។ ការដំឡើងកម្មវិធីសម្រាប់អនុវត្ត P2P (កម្មវិធីទំនាក់ទំនងគ្នាតាមប្រព័ន្ធអ៊ីនធើរណែត) ត្រូវបានរឹតត្បិត ។ ប្រសិនបើគ្មានការអនុញ្ញាតពីអ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានទេ ការប្រើប្រាស់កម្មវិធីកុំព្យូទ័របែបនេះ នឹងត្រូវហាមឃាត់ទាំងស្រុងក្នុងករណីការិយាល័យរដ្ឋាភិបាល ។

(៣) តំហែទាំកុំព្យូទ័រមេ

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវពិចារណាអំពីការរៀបចំអោយមានការចូលទៅប្រើប្រាស់ព័ត៌មានប្រកបដោយសន្តិសុខ តឹងរ៉ឹងបំផុតដែលរួមមានការប្រើប្រាស់ប្រព័ន្ធលេខសម្ងាត់នៅពេលមានការអនុវត្តតំហែទាំកុំព្យូទ័រមេ តាមរយៈខ្សែបណ្តាញពីខាងក្រៅជួររាជរដ្ឋាភិបាល។

២.២.៣ កម្មវិធីកុំព្យូទ័រសម្រាប់ការអនុវត្ត

(១) អ៊ីម៉ែល (e-mail)

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវធ្វើការរៀបចំអោយបានល្អនូវ e-mail server ដោយចៀសវាងការប្រើប្រាស់អ៊ីម៉ែល ដែលមានបញ្ជូនតដោយ hackers។ ជាការចាំបាច់ផងដែរក្នុងការប្រើប្រាស់មុខងារយថាភាព (authentication function) តាមរយៈការត្រួតពិនិត្យការ

កំណត់អត្តសញ្ញាណ និងលេខសម្ងាត់ ។

(២) គេហទំព័រ

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ចាំបាច់ត្រូវចៀសវាងការវាយប្រហារនានាពីសំណាក់ hackers ដែលប៉ុនប៉ងយាយីដល់ គេហទំព័ររបស់រាជរដ្ឋាភិបាល ។ ត្រូវចាត់រាល់វិធានការបង្ការ និងការពារគ្រប់បែបយ៉ាងដែលអាចធ្វើទៅបាន ដើម្បីទប់ទល់និងបោះបង់ចោលការចូលទៅកាន់គេហទំព័រដែលមិនស្របច្បាប់ និងដែលមិនត្រឹមត្រូវបែបនេះ ។ រាល់ប្រព័ន្ធដំណើរការព័ត៌មានគួរតែត្រូវបានបង្កើតឡើងអោយបានតឹងរ៉ឹងប្រឆាំងនឹងការចូលទៅកាន់ប្រព័ន្ធនេះដោយមិនស្របច្បាប់ កុំអោយអាចទាញយកព័ត៌មានរបស់រដ្ឋាភិបាលពីកុំព្យូទ័រមេមកបាន ក្នុងនោះរួមទាំងការទាញយកសំណុំឯកសារពីប្រព័ន្ធអ៊ីនធើណែតផងដែរ ។

(៣) ប្រព័ន្ធគ្រប់គ្រងឈ្មោះអាស័យដ្ឋានគេហទំព័រ (DNS)

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវរៀបចំដំឡើង DNS server(s) អោយបានត្រឹមត្រូវដើម្បីផ្តល់សេវាដំណោះស្រាយ ឈ្មោះជាប់លាប់ (ការបំលែងពីឈ្មោះ domain ទៅជា IP address) ។ អាចចាត់ទុកថាជាការសំខាន់ផងដែរ ចំពោះប្រតិបត្តិការ និងតំហែទាំប្រព័ន្ធកុំព្យូទ័រមេដែលមានផ្ទុក DNS ដើម្បីថែទាំដំណើរការគ្រប់គ្រង ដែលមានភាពស៊ីសង្វាក់គ្នា ។

ការវាយប្រហារពីសំណាក់ hackers គួរតែត្រូវបានការពារដូចខាងក្រោម ៖

- ការដំឡើង DNS Cache Server ដើម្បីចៀសវាងការទទួលយកការស្នើសុំឈ្មោះ domain ពីខាងក្រៅ
- ការការពារការលេចចេញព័ត៌មាន នៅពេលផ្តល់សេវាកម្មឈ្មោះ domain ។

២.២.៤ ខ្សែគមនាគមន៍

(១) វិធានការចំពោះខ្សែគមនាគមន៍ទូទៅ

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវគ្រប់គ្រងធាតុមួយចំនួនដូចខាងក្រោម ៖

- ការផលិតផ្នែករឹង (hardware) និងផ្នែកទន់ (software) របស់កុំព្យូទ័រដែលមានការបញ្ជាក់ និងផ្ទៀងផ្ទាត់ត្រឹមត្រូវ គួរតែត្រូវបាន ជ្រើសរើសសម្រាប់ការភ្ជាប់បណ្តាញជាប្រចាំ និងបិតបៀរ ។
- ក៏ចាំបាច់ត្រូវធ្វើការបែងចែកកុំព្យូទ័រទៅតាមក្រុមអោយបានល្អផងដែរ ដែលត្រូវបានតភ្ជាប់ទៅនឹង ឧបករណ៍ភ្ជាប់បណ្តាញកុំព្យូទ័រ

- ត្រូវកំណត់លក្ខខណ្ឌត្រឹមត្រូវក្នុងការប្រើប្រាស់ការតភ្ជាប់បណ្តាញ ដើម្បីផ្តល់អោយនូវមុខងារគ្រប់គ្រងការដំណើរការទិន្នន័យ (access and route control functions) ដ៏សមរម្យ ។

(២) ការគ្រប់គ្រងប្រព័ន្ធបណ្តាញកុំព្យូទ័រផ្ទៃក្នុង (Intranet)

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវផ្តល់មុខងារអនុញ្ញាតអោយប្រើប្រាស់ទិន្នន័យសម្រាប់ការតភ្ជាប់តាមប្រព័ន្ធបណ្តាញកុំព្យូទ័រផ្ទៃក្នុង នៅពេលដែលមានការចូលទៅប្រើប្រាស់ខ្សែបណ្តាញ ។

មុខងារខាងក្រោមនេះ គួរតែត្រូវធ្វើការសិក្សា និងអនុវត្ត ដែលមានដូចជា ៖

- ពិនិត្យមើលឡើងវិញជាទៀងទាត់នូវព័ត៌មានស្តីអំពីការគ្រប់គ្រងលើការប្រើប្រាស់ទិន្នន័យ
- ពិនិត្យតាមដានគុណភាពនៃការបញ្ជូនការប្រាស្រ័យទាក់ទង ដើម្បីរកអោយឃើញនូវដំណើរការខុសប្រក្រតី នៃឧបករណ៍ភ្ជាប់បណ្តាញកុំព្យូទ័រ
- ពិនិត្យតាមដានបរិមាណនៃការប្រាស្រ័យទាក់ទង

(៣) ការគ្រប់គ្រងការតភ្ជាប់ពីខាងក្រៅទៅនឹងប្រព័ន្ធបណ្តាញកុំព្យូទ័រផ្ទៃក្នុង (Extranet)

អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវផ្តល់មុខងារអនុញ្ញាតអោយប្រើប្រាស់ទិន្នន័យសម្រាប់ការតភ្ជាប់តាមប្រព័ន្ធ Extranet នៅពេលដែលមានការស្នើសុំអោយមានការតភ្ជាប់ខ្សែបណ្តាញពីខាងក្រៅជួរាជរដ្ឋាភិបាល ។

ក៏តម្រូវអោយមានការបំពេញលក្ខខណ្ឌតម្រូវអប្បបរមាផ្នែកសន្តិសុខព័ត៌មានផងដែរ សម្រាប់ការតភ្ជាប់ពីខាងក្រៅ ។ ប្រសិនបើមិនមានសន្តិសុខគ្រប់គ្រាន់ទេនោះ ត្រូវដំឡើងខ្សែបណ្តាញមួយផ្លូវទៀត ។

មុខងារខាងក្រោមនេះ គួរតែត្រូវធ្វើការសិក្សា និងអនុវត្ត ដែលមានដូចជា ៖

- ពិនិត្យមើលឡើងវិញជាទៀងទាត់នូវទិន្នន័យគ្រប់គ្រងការប្រើប្រាស់ទិន្នន័យ
- ពិនិត្យតាមដានគុណភាពនៃការបញ្ជូនការប្រាស្រ័យទាក់ទង ដើម្បីរកអោយឃើញនូវដំណើរការខុសប្រក្រតី នៃឧបករណ៍ភ្ជាប់បណ្តាញកុំព្យូទ័រ
- ពិនិត្យតាមដានបរិមាណនៃការប្រាស្រ័យទាក់ទង

[ចប់ GISSC]

ជំពូក ២

GISMS1.0 (**ចេញផ្សាយនៅក្នុងឥណ្ឌា ឆ្នាំ២០០៨**)

ផ្នែក ទី១

ផ្នែក ទី២

ផ្នែក ទី៣ ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល

កំណត់សម្គាល់អំពី GISSC នេះ ៖

ឯកសារនេះ គឺជាផ្នែកមួយនៃ GISSC (ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល) ដែលត្រូវបានបង្កើតឡើងដោយ NiDA និង JICA ដើម្បីពង្រឹងសន្តិសុខព័ត៌មានរបស់ការិយាល័យរាជរដ្ឋាភិបាលកម្ពុជា ។

ប្រការដែលមានចែងនៅក្នុងឯកសារនេះ បង្ហាញអំពីលក្ខខណ្ឌតម្រូវអប្បបរមាដែលក្រសួង ឬ ស្ថាប័នពាក់ព័ន្ធគួរតែពិចារណាតាមរយៈការពង្រឹងសន្តិសុខព័ត៌មានរបស់អង្គភាព ។

ប្រភេទផ្សេងៗនៃឯកសារពាក់ព័ន្ធទាំងឡាយ ដូចជា គោលការណ៍ណែនាំ និងសៀវភៅវិធានផ្សេងៗ គួរតែត្រូវបានបង្កើតឡើងដោយក្រសួង និងស្ថាប័នពាក់ព័ន្ធនីមួយៗ ។

ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល
សំណៅ ១.0 កំណែប្រែលើកទី ១

ខែធ្នូ ឆ្នាំ២00៩

ទីស្តីការគណៈរដ្ឋមន្ត្រី
អាជ្ញាធរជាតិឧទ្ធលបន្ទុកកិច្ចការអភិវឌ្ឍន៍វិស័យបច្ចេកវិទ្យា
គមនាគមន៍ ព័ត៌មានវិទ្យា

ទីភ្នាក់ងារសហប្រតិបត្តិការអន្តរជាតិនៃប្រទេសជប៉ុន