អារម្ភកថា

ក្រោយពីបានឆ្លងកាត់សង្គ្រាមស៊ីវិលអស់ជាច្រើនទសវត្សន៍មក ព្រះរាជាណាចក្រកម្ពុជាបាន នឹងកំពុងធ្វើដំណើរលើផ្លូវដ៏វែងឆ្ងាយមួយ ក្នុងកិច្ចការស្តារនិងអភិវឌ្ឍន៍ប្រទេសជាតិឡើងវិញ។ ក្នុងពេលដែលប្រទេសជាតិកំពុងរក្សាបានស្ថិរភាព នយោបាយជាបន្តបន្ទាប់ គួបផ្សំនឹងកំណើនវិនិយោគ ដ៏ច្រើនសន្ធឹកសន្ធាប់ពីបរទេស ធ្វើឲ្យប្រទេសកម្ពុជាបច្ចុប្បន្នទទួលបាននូវអត្រា កំណើនសេដ្ឋកិច្ចយ៉ាងខ្ពស់ដែលមានជាមធ្យម ៩,១% ក្នុងមួយឆ្នាំ ក្នុងរយៈពេល៥ឆ្នាំកន្លងមកនេះ។ ក៏ប៉ុន្តែនៅមានការលំបាកមួយចំនួនក្នុងចំណោមការលំបាក ដទៃទៀតដូចជាសមត្ថភាពធនធានមនុស្សនៅមានកំរិត និងកង្វះខាតហេដ្ឋារចនាសម្ព័ន្ធ ដែលមិនមានអំណោយផលពេញលេញ ដល់ការទាក់ទាញការវិនិយោគ មួយចំនួនពីបរទេស។ បច្ចេកវិទ្យាគមនាគមន៍ ព័ត៌មានវិទ្យា (ICT) បានដើរតួនាទីយ៉ាងសំខាន់ក្នុងការរក្សានូវល្បឿននៃការអភិវឌ្ឍន៍តាមរយៈ ការបង្កើននូវការពឹងពាក់គ្នាទៅវិញទៅមក ក្នុងក្របខណ្ឌសេដ្ឋកិច្ចពិភពលោក។ យើងជឿជាក់ថាហេដ្ឋារចនាសម្ព័ន្ធ បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា លំដាប់ពិភពលោក គឺជាបុរេលក្ខខណ្ឌសំខាន់មួយសំរាប់អ្នកវិនិយោគបរទេស។ ប្រទេសកម្ពុជាបានជ្រើសរើសយកវិធីសាស្ត្រមួយដែលអនុញ្ញាតឲ្យវិស័យឯកជនចូលរួមនៅក្នុងការកសាងហេដ្ឋារចនាសម្ព័ន្ធ បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា ដែលជាកត្តាមួយ នាំឲ្យវិស័យសំណង់នៅទីក្រុងសំខាន់ៗ មានការរីកចំរើនយ៉ាងឆាប់រហ័ស។ យ៉ាងណាមិញយើងក៏ពឹងផ្អែកទៅលើការដាក់ឲ្យប្រើប្រាស់ បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យានៅក្នុងរាជរដ្ឋាភិបាល ដើម្បីជំរុញឲ្យមានការកែលំអរថែមទៀតដល់សេវានានា របស់រដ្ឋប្រព្រឹត្តទៅដោយប្រសិទ្ធភាព និងតម្លាភាពជាងមុន។ បច្ចុប្បន្នយើងកំពុងរៀបចំបង្កើតប្រព័ន្ធបណ្តាញកុំព្យូទ័រផ្ទៃក្នុង (Intranet) សំរាប់ រដ្ឋាភិបាល ដែលជាហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មានវិទ្យាថ្នាក់ជាតិ (NII) សំរាប់បង្កើតបរិស្ថានការងារផ្តល់សេវាអេឡិចត្រូនិច (e-Services)។ យើងត្រូវធ្វើជាបន្តបន្ទាប់ទៀតនូវការងារបង្កើតឲ្យមាននូវព័ត៌មាននានាអំពីរដ្ឋាភិបាល និងសេវាផ្សេងៗ ក្នុងការធ្វើ ប្រតិបត្តិការប្រព័ន្ធអ៊ីនធឺណិតដើម្បីធ្វើឲ្យប្រសើរឡើងនូវសេវាសាធារណៈ និងបរិយាកាសវិនិយោគ។

ការសិក្សារៀបចំឯកសារស្តីពីសន្តិសុខព័ត៌មាន គឺមានសារៈសំខាន់ និងត្រូវចំពេលក្នុងកាលៈទេសៈនេះ។ ផែនទីបង្ហាញផ្លូវដែលអាចកំណត់ទិសដៅបានត្រឹមត្រូវមួយ ត្រូវបានគូរជាលើកដំបូងសំរាប់ប្រទេសកម្ពុជា។ ផែនការនេះបានឆ្លុះ បញ្ចាំងនូវតថភាពនៃការប្រើប្រាស់ បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា នៅក្នុងរដ្ឋាភិបាល យោងទៅតាមរបកគំហើញជាក់ស្តែងផ្សេងៗ ដែលទទួលបានពីទីភ្នាក់ងារផ្នែកនីតិប្រតិបត្តិទាំងអស់របស់រដ្ឋាភិបាល។ ឯកសារនេះបានបង្ហាញនូវទិដ្ឋភាពសន្តិសុខនៃការប្រើប្រាស់បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា នៅក្នុងការិយាល័យនានានៃរដ្ឋាភិបាល រួមជាមួយនឹងកម្រងកម្មវិធី (Application) ដែលកំពុងដាក់ឲ្យប្រើប្រាស់ គ្រោងនឹងបង្កើត និងដែលត្រូវការសំ

រាប់សេវារដ្ឋាភិបាលអេឡិចត្រូនិច (e-Government)។ អនុសាសន៍ដែលបានផ្តល់ឲ្យទាំងអស់ អាចនឹងយកទៅអនុវត្តបានប្រកបដោយប្រសិទ្ធភាព និងជោគជ័យដោយសារ ការប្រើប្រាស់នូវវិធីសាស្ត្រជាដំណាក់ៗ យ៉ាងត្រឹមត្រូវដោយផ្តោតការយកចិត្តទុកដាក់ទៅលើការគ្រប់គ្រងបញ្ហាផ្សេងៗ ដែលត្រូវការនូវដំណោះស្រាយជាចំបងមុនគេ ដើម្បីងាយស្រួលដល់ការដោះស្រាយប្រកបដោយប្រសិទ្ធិភាពខ្ពស់ នូវរាល់បញ្ហាដែលមានភាពស្មុគស្មាញជាង ហើយធ្វើការ អនុវត្តន៍ជាបន្តនូវកិច្ចការសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន។

នេះជាកាលៈទេសៈដ៏សំខាន់មួយដែលរាជរដ្ឋាភិបាល ត្រូវប្រឈមមុខនឹងការពិតនានាដូចបានបង្ហាត់បង្ហាញនៅក្នុងឯកសារនេះ។ មិនតែប៉ុណ្ណោះត្រូវការបង្កើតនូវបរិយាកាស ដែលផ្តល់អំណោយផលដល់ការប្រើប្រាស់បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា នៅក្នុងការិយាល័យនានារបស់ រដ្ឋាភិបាល ប្រកបដោយសុវត្ថិភាព និងធ្វើការអភិវឌ្ឍន៍សេវាអេឡិចត្រូនិចឲ្យបាន មុនឆ្នាំ ២០២០។ ដូច្នេះខ្ញុំមានសេចក្តីសោមនស្សរីករាយណាស់ ក្នុងការរៀបចំឲ្យមានឡើងនូវឯកសារពាក់ព័ន្ធនឹងបញ្ហាសន្តិសុខព័ត៌មាននេះ ហើយក៏សូមសំដែងនូវអំណរគុណ ដល់ទីភ្នាក់ងារសហប្រតិបត្តិការអន្តរជាតិនៃប្រទេសជប៉ុនដែលបានជួយឧបត្ថម្ភគាំទ្រ និង អគ្គលេខាធិការដ្ឋានអាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា (NiDA) ដែលបានសិក្សា និងរៀបចំឯកសារសន្តិសុខព័ត៌មាននេះឡើង សំរាប់ រាជរដ្ឋាភិបាលកម្ពុជា។ កិច្ចខិតខំប្រឹងប្រែងក្នុងការបំពេញការងារទាំងអស់នេះ កំពុងនឹងរង់ចាំយើងទាំងអស់គ្នាហើយយើងសង្ឃឹមថា នឹងផ្តល់អត្ថប្រយោជន៍ជាច្រើន ដល់ការអភិវឌ្ឍន៍សង្គម និងសេដ្ឋកិច្ចរបស់ប្រទេសកម្ពុជា។

ខ្ញុំសូមថ្លែងអំណរគុណ និងជូនពរដល់ទីភ្នាក់ងារសហប្រតិបត្តិការអន្តរជាតិនៃប្រទេសជប៉ុន (JICA) និង អគ្គលេខាធិការដ្ឋានអាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា (NiDA) សូមបានទទួលនូវជោគជ័យដ៏ឧត្តុង្គឧត្តម រាល់ការសិក្សាស្រាវជ្រាវ នាពេលអនាគត។

រាជធានីភ្នំពេញ, ថ្ងៃទី ខែ សីហា ឆ្នាំ ២០០៩

សុខ អាន
ឧបនាយករដ្ឋមន្ត្រី
រដ្ឋមន្ត្រីទទួលបន្ទុកទីស្តីការគណៈរដ្ឋមន្ត្រី និងជា
អនុប្រធានអាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍
បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា

មាតិកា

ផ្នែក ទី១

គោលនយោបាយ នៃប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន

របស់ រាជរដ្ឋាភិបាល

គោលនយោបាយ នៃប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់ រាជរដ្ឋាភិបាល

[គោលបំណង]

គោលបំណងនៃសកម្មភាពការពារសន្តិសុខព័ត៌មាន គឺដើម្បីរក្សានិរន្តរភាព នៃការគ្រប់គ្រងព័ត៌មាន របស់រាជរដ្ឋាភិបាលកម្ពុជា និងដើម្បីកាត់បន្ថយហានិភ័យនៃការខូចខាច តាមរយៈការបង្ការមិនឲ្យកើតមាននូវឧប្បត្តិហេតុអាក្រក់ផ្សេងៗ និងកាត់បន្ថយផលប៉ះពាល់ ដែលអាចនឹងកើតមានឡើង។

[គោលនយោបាយ]

- គោលដៅនៃគោលនយោបាយរបស់ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល គឺដើម្បីការពារសម្ភារៈបរិក្ខាព័ត៌មាន របស់រាជរដ្ឋាភិបាលកម្ពុជាទប់ទល់នឹងសកម្មភាព យាយីដោយចេតនា ឬអចេតនាពីខាងក្នុង និងខាងក្រៅ។

- គោលនយោបាយរក្សាសន្តិសុខព័ត៌មាននឹងធ្វើឲ្យប្រាកដថា៖
  - ព័ត៌មាននានានឹងត្រូវបានការពារទប់ទល់នឹងការលួចប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត
  - ការសម្ងាត់របស់ព័ត៌មាននឹងត្រូវបានរក្សាការពារ
  - លក្ខណៈរួមរបស់ព័ត៌មាននឹងត្រូវបានរក្សាការពារ
  - លទ្ធភាពផ្តល់ព័ត៌មានសំរាប់ដំណើរការគ្រប់គ្រងនឹងត្រូវបានអនុវត្ត
  - តម្រូវការផ្នែកនិតិបញ្ញត្តិ និងបទបញ្ញត្តិនឹងត្រូវបានបំពេញ
  - ការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មាននឹងត្រូវបានផ្តល់ជូនមន្ត្រីរាជការទាំងអស់
  - រាល់ការបំពារបំពានជាក់ស្តែង ឬដែលគួរឲ្យសង្ស័យប៉ះពាល់ដល់សុវត្ថិភាពព័ត៌មាន នឹងត្រូវបានរាយការណ៍ទៅកាន់ប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន ហើយនឹងត្រូវបានស៊ើបអង្កេតដោយហ្មត់ចត់ ។

- នីតិវិធីដែលបានបង្កើតឡើងគាំទ្រដល់គោលនយោបាយនានា រួមទាំងដំណោះស្រាយក្នុងការគ្រប់គ្រងមេរោគ និងពាក្យ/លេខសម្ងាត់ (Passwords)។
- តម្រូវការផ្នែករដ្ឋបាលដើម្បីអាចទទួលបាននូវព័ត៌មាន និងប្រើប្រាស់នូវប្រព័ន្ធផ្សេងៗ នឹងត្រូវ

បានបំពេញ។

- ក្នុងកំឡុងពេលអនុវត្តការងារ ប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន មានការកិច្ចទទួលខុសត្រូវចំពោះការថែរក្សាគោលនយោបាយ ព្រមទាំងផ្តល់ការគាំទ្រ និងដំបូន្មានផ្សេងៗ។
- ប្រធានគ្រប់គ្រងទាំងអស់មានការកិច្ចទទួលខុសត្រូវ ដោយផ្ទាល់ចំពោះការអនុវត្តន៍គោលនយោបាយ និងធ្វើឲ្យបុគ្គលិកនៅក្នុងនាយកដ្ឋានរបស់ខ្លួនគោរពតាមគោលនយោបាយទាំងនេះ។
- ការគោរពតាមគោលនយោបាយស្តីអំពីសន្តិសុខព័ត៌មាននេះ គឺជាភារកិច្ចចាំបាច់ដែលត្រូវ អនុវត្ត។

អគ្គលេខាធិការដ្ឋាន អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការ
អតិវឌ្ឍន៍បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា

ផ្នែក ទី២

ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រង
សន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល

អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា
គមនាគមន៍ ព័ត៌មានវិទ្យា

- ពង្រាងដោយលោក យូស៊ូកេ តាណាកា (Yusuke Tanaka) អ្នកជំនាញ
នៃទីភ្នាក់ងារសហប្រតិការអន្តរជាតិនៃប្រទេសជប៉ុន (JICA)

- កែសម្រួល និងរៀបរៀងដោយក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការ
សន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន

១.សេចក្តីផ្តើម

ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រដ្ឋាភិបាល (GISMS) ត្រូវបានកំណត់នូវលក្ខខណ្ឌដែលរាជរដ្ឋាភិបាលកម្ពុជាត្រូវបំពេញរួមមាន ការបង្កើត ការអនុវត្តន៍ ការត្រួតពិនិត្យ និងការចាត់វិធានការក្នុងនាមជា អង្គភាពទទួលបន្ទុកប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាលស្ថិតក្នុងគោលនយោបាយស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GISMS) ដែលបានប្រកាសដោយនាយករដ្ឋមន្ត្រីដែលជាថ្នាក់ដឹកនាំរាជរដ្ឋាភិបាល។

២. វិសាលភាព

ឯកសារណែនាំ ស្តីអំពី GISMS ត្រូវបានរៀបរៀងឡើង ដោយរួមបញ្ចូល នូវក្រសួង ស្ថាប័ន នៃរាជរដ្ឋាភិបាលទាំង៣១ ដូចមានខាងក្រោម៖

១. ទីស្តីការគណៈរដ្ឋមន្ត្រី

២. ក្រសួងកសិកម្ម រុក្ខាប្រម៉ាញ់ និង នេសាទ

៣. ក្រសួងពាណិជ្ជកម្ម

៤. ក្រសួងវប្បធម៌ និង វិចិត្រសិល្បៈ

៥. ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ

៦. ក្រសួងអប់រំ យុវជន និង កីឡា

៧. ក្រសួងបរិស្ថាន

៨. ក្រសួងកិច្ចការបរទេស និង សហប្រតិបត្តិការអន្តរជាតិ

៩. ក្រសួងសុខាភិបាល

១០. ក្រសួងឧស្សាហកម្ម រ៉ែ និង ថាមពល

១១. ក្រសួងព័ត៌មាន

១២. ក្រសួងមហាផ្ទៃ

១៣. ក្រសួងយុត្តិធម៌

១៤. ក្រសួងការងារ និង បណ្តុះបណ្តាលវិជ្ជាជីវៈ

១៥. ក្រសួងរៀបចំដែនដី នគរូបនីយកម្ម និង សំណង់

១៦. ក្រសួងការពារជាតិ

១៧. ក្រសួងទំនាក់ទំនងសភា និង អធិការកិច្ច

១៨. ក្រសួងផែនការ

១៩. ក្រសួងប្រៃសនីយ៍ និង ទូរគមនាគមន៍

២០. ក្រសួងសាធារណការ និង ដឹកជញ្ជូន

២១. ក្រសួងធម្មការ និង សាសនា

២២. ក្រសួងអភិវឌ្ឍន៍ជនបទ

២៣. ក្រសួងសង្គមកិច្ច អតីតយុទ្ធជន និង យុវនិតិសម្បទា

២៤. ក្រសួងទេសចរណ៍

២៥. ក្រសួងធនធានទឹក និង ឧតុនិយម

២៦. ក្រសួងកិច្ចការនារី

២៧. សាលាក្រុងភ្នំពេញ

២៨. រដ្ឋលេខាធិការដ្ឋានមុខងារសាធារណៈ

២៩. រដ្ឋលេខាធិការដ្ឋានអាកាសចរណ៍ស៊ីវិល

៣០. អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា (អ.អ.ប.គ.ព)

៣១. គណៈប្រតិភូអចិន្ត្រៃយ៍តំណាងឲ្យព្រះរាជាណាចក្រកម្ពុជាប្រចាំនៅអង្គការសហប្រជាជាតិ

៣. ឯកសារយោង ពាក្យ និងនិយមន័យ

៣.១. ឯកសារយោង

ឯកសារយោងខាងក្រោមមានសារៈសំខាន់យ៉ាងខ្លាំងសំរាប់ការចងក្រងឯកសារណែនាំនេះ ISO/ISE 27001: 2005 បច្ចេកវិទ្យាព័ត៌មាន – វិធីសាស្ត្រការពារសន្តិសុខ – ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន– តម្រូវការ

៣.២. ពាក្យ និងនិយមន័យ

ខាងក្រោមនេះគឺជាពាក្យទាំងឡាយដែលត្រូវបានប្រើប្រាស់នៅក្នុង GISMS រួមជាមួយនឹងអត្ថន័យនីមួយៗរបស់ពួកវា។

- **ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GISMS)៖**

ជាប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន (ISMS) សំរាប់រាជរដ្ឋាភិបាលកម្ពុជា។ GISMS ត្រូវបានបង្កើតឡើង ដោយយោងទៅតាម ISO/ISE 27001។

- **ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (ការិយាល័យ GIS)៖**

ត្រូវបានបង្កើតឡើង ដោយមានតួនាទីជា លេខាធិការរបស់គណៈកម្មាធិការនាយកផ្នែករបស់រាជរដ្ឋាភិបាល (GCIO) ហើយ អ.អ.ប.គ.ព ជាអង្គភាពដែលទទួលខុសត្រូវ ក្នុងការបំពេញតួនាទីរបស់ការិយាល័យ GIS នេះ។ ស្ថាប័ននេះទទួលខុសត្រូវ ក្នុងការបង្កើតគោលនយោបាយ បទដ្ឋាន និងសេចក្តីណែនាំរបស់ GISMS និងទទួលខុសត្រូវផងដែរ ចំពោះការងារទាំងឡាយ ដែលពាក់ព័ន្ធនឹង GISMS នៅក្នុងរាជរដ្ឋាភិបាលកម្ពុជា។ *និយមន័យនេះ គឺជាសេចក្តីព្រាងប៉ុណ្ណោះ។*

ការឧបត្ថម្ភគាំទ្រសំរាប់ GCIO នឹងត្រូវបានចាត់ចែងនៅក្នុងគំរោងអភិវឌ្ឍន៍ GCIO។

- **នាយកផ្នែកសន្តិសុខព័ត៌មាន (CISO)៖**

មន្ត្រីម្នាក់នៃស្ថាប័ននីមួយៗនឹងត្រូវតែងតាំងសំរាប់មុខងារនេះហើយទំនួលខុសត្រូវផ្សេងៗ ត្រូវបានកំណត់ដោយជាក់លាក់នៅក្នុង ឯកសារណែនាំស្តីអំពី GISMS និងឯកសារវិធានស្តីអំពី សន្តិសុខព័ត៌មាន។

- **នាយកគ្រប់គ្រងសន្តិសុខព័ត៌មាន (IS Manager)៖**

មុខងារនេះត្រូវបានផ្តល់ដោយសាមីស្ថាប័ន។ ទំនួលខុសត្រូវផ្សេងៗត្រូវបានកំណត់ដោយជាក់លាក់នៅក្នុងឯកសារណែនាំស្តីអំពី GISMS និងឯកសារវិធានស្តីអំពីសន្តិសុខព័ត៌មាន។

- **ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ៖**

ជាឯកសារសំរាប់កំណត់ និងវាយតំលៃអំពីសំការៈព័ត៌មាន ព្រមទាំងសំរាប់កំណត់ និងវាយតំលៃមើលហានិភ័យដែលអាចនឹងកើតមាន។

- **ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GIS Rule Book)៖**

ជាឯកសារដែលកំណត់នូវវិធាន និងនីតិវិធីសំរាប់រក្សាសន្តិសុខដល់សំការៈព័ត៌មាននីមួយៗ។ ឯកសារនេះនឹងត្រូវបានចងក្រងដោយសាមីស្ថាប័ន ដើម្បីការពារសន្តិសុខព័ត៌មានរបស់ខ្លួនដោយយោងទៅតាម ឯកសារគំរូដែលបង្កើតឡើងដោយ អ.អ.ប.ត.ព។ វាជាការប្រសើរបំផុតដែលសាមីស្ថាប័នត្រូវយកគំរូតាមឯកសារគំរូនេះក្នុងកំរិតមួយជាអប្បបរមា។

៤. ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GISMS)

GISMS មានតួនាទីកំនត់ផែនការអនុវត្ត ត្រួតពិនិត្យ និងចាត់វិធានការជាប្រាំ ដូចបានកំនត់ ISO27001 (PDCA Cycle) បានអនុវត្តទៅតាមវដ្តដែលមានលក្ខណៈជាការរៀបចំផែនការ ការអនុវត្តន៍ ការត្រួតពិនិត្យ និងសកម្មភាព (The Plan, Do, Check And Action (PDCA) Cycle) ដូចបានចែងនៅក្នុង ISO27001។ ជំពូកនេះនឹងធ្វើការនិយាយអំពីដំណើរការការងាររបស់ GISMS ការគ្រប់គ្រងឯកសារ និងបញ្ជីព័ត៌មាន។

៤.១. <u>ការបង្កើតផែនការ</u>

ដំណើរនៃការបង្កើតផែនការត្រូវបានចែកជា ៥ ផ្នែកផ្សេងៗគ្នារួមមាន៖

- ការពិនិត្យមើលគោលនយោបាយ និងឯកសារណែនាំ
- ការកំណត់វិសាលភាពនៃ GISMS
- ការវាយតំលៃអំពីហានិភ័យ
- ការបង្កើតឯកសារណែនាំស្តីអំពី GIS
- ការស្នើសុំការអនុម័ត ។

៤.១.១.<u>ការពិនិត្យមើលគោលនយោបាយនិងឯកសារណែនាំស្តីអំពី GISMS</u>

ជាបឋមត្រូវមើលអំពីគោលនយោបាយរបស់ GISMS ដែលបានប្រកាសអំពីគោលដៅ និងគោលនយោបាយរបស់ GISMS នៃព្រះរាជាណាចក្រកម្ពុជា។ ម៉្យាងវិញទៀតត្រូវមើលឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសុវត្ថិភាពព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GISMS Manual) ដែលឯកសារនេះ នឹងត្រូវយកទៅអនុវត្តនៅគ្រប់ស្ថាប័នរដ្ឋទាំងអស់ក្នុងព្រះរាជាណាកម្ពុជា និងសំរាប់កំណត់នូវវិធានទាំងឡាយ ដើម្បីរៀបចំបង្កើតGISMS ។

៤.១.២. <u>ការកំណត់វិសាលភាពនៃ GISMS</u>

នៅពេលដែលស្ថាប័នណាមួយចាប់ផ្តើមបង្កើត GISMS ស្ថាប័នមួយនេះត្រូវកំណត់ នូវវិសាលភាពសំរាប់វដ្តនៃ PDCA ជាក់លាក់មួយ។ ជាទូទៅវាអាចប្រព្រឹត្តទៅបានចំពោះការកំណត់ វិសាលភាពដោយយោងទៅលើសេវាកម្ម ឬបរិក្ខារូបវន្តដូចជា ព្រំដី ឬអាគារជាដើម។ ការកំណត់ វិសាលភាពនេះ ក៏អាចអនុវត្តទៅបានដោយយោងទៅលើបណ្តាញកុំព្យូទ័រប្រព័ន្ធព័ត៌មាន ដើម្បី កំណត់ឲ្យបាននូវការគ្រប់គ្រង និងដំណោះស្រាយប្រកបដោយប្រសិទ្ធិភាពទប់ទល់នឹង បញ្ហាគំរាមផ្សេងៗ។ សាមីស្ថាប័នក៏ត្រូវមានការប្រុងប្រយ័ត្នផង ដៃរចំពោះការកំណត់វិសាលភាព ដោយយោង ទៅលើតារាងចេនាសម្ព័ន្ធដោយហេតុថាការប្រព្រឹត្តបែបនេះពេលខ្លះនឹងធ្វើឲ្យ ការអនុវត្តជាក់ស្តែង មានការលំបាក។

ឯកសារបឋមស្តីអំពី GISMS ផ្តោតតែទៅលើម៉ាស៊ីនកុំព្យូទ័រ (Client PC) ដែល ជាបរិក្ខារ កំរិតទាបបំផុតនៃ GISMS ដែលត្រូវបានកំណត់វិសាលភាពត្រឹមត្រូវ ហើយនឹងត្រូវបាន បង្កើតឡើងនាពេលអនាគតប៉ុណ្ណោះ ។

៤.១.៣. <u>ការវាយតំលៃអំពីហានិភ័យ</u>

ដំណើរការនៃការវាយតំលៃអំពីហានិភ័យត្រូវបានចែកចេញជា ៥ ដំណាក់កាល រួមមាន៖

- ការកំណត់សំការៈព័ត៌មាន
- ការវាយតំលៃអំពីសំការៈព័ត៌មាន
- ការពិនិត្យមើលអំពីហានិភ័យដែលអាចនឹងកើតមាន
- ការវាយតំលៃអំពីហានិភ័យ
- ការកំណត់ហានិភ័យ ។

ដំណើរការលំអិតត្រូវបានកំណត់នៅក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ។
សូមមើលសេចក្តីណែនាំនៅក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ
(ឧបសម្ព័ន្ធទី១៖ ឯកសារសំរាប់ ពិនិត្យមើលហានិភ័យ)។

<u>ដំណាក់កាលទី១៖ ការកំណត់សំការៈព័ត៌មាន</u>

ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ បានបញ្ចូលសំការៈព័ត៌មានចំនួន ៦ប្រភេទ ក្នុងនោះសំការៈព័ត៌មាន ៤ប្រភេទរួមមាន សេវាកម្ម ឬបរិក្ខារកុំព្យូទ័រ ក្រដាសឯកសារ បណ្តាញកុំព្យូទ័រ និងម៉ាស៊ីនកុំព្យូទ័រមេ (Server) នឹងត្រូវ កំណត់ដោយនាយកដ្ឋាននីមួយៗដែលទទួលបន្ទុក ពិនិត្យមើល ដោយខ្លួនឯង ។

<u>ដំណាក់កាលទី២៖ ការវាយតំលៃអំពីសំការៈព័ត៌មាន</u>

ដំណាក់កាលបន្ទាប់នេះគឺការវាយតំលៃអំពីសំការៈព័ត៌មាន។ ចំនុចបីយ៉ាង

នៃការវាយតំលៃរួម គឺការសម្ងាត់ ផលប៉ះពាល់ (Integrity) លទ្ធភាព (ផ្តល់សេវាកម្ម ឬបរិក្ខារ)។

សូមជ្រើសរើសចំនុចមួយក្នុងចំណោមចំណាត់ថ្នាក់មួយ ពីចំនុចទាំងបីនៃការវាយតំលៃយោងតាមលក្ខណៈវិនិច្ឆ័យដែលបានបង្ហាញដូចខាងក្រោម៖

១.ការសម្ងាត់				
ល.រ	ចំណាត់ថ្នាក់	ពិន្ទុ		សេចក្តីអធិប្បាយ
C១	១.សាធារណៈ	១		សំការៈព័ត៌មានដែលបើកចំហសំរាប់សាធារណៈជន
C២	២.ផ្ទៃក្នុង	២		ព័ត៌មានដែលប្រើប្រាស់សំរាប់តែការប្រតិបត្តិការងារ របស់រាជរដ្ឋាភិបាល
C៣	៥.សម្ងាត់	៥		ជាការសម្ងាត់ក្នុងចំណោមបុគ្គលមួយចំនួនដែលទទួលការអនុញ្ញាត
២.ផលប៉ះពាល់				
ល.រ	ចំណាត់ថ្នាក់	ពិន្ទុ		សេចក្តីអធិប្បាយ
I១	១.ទាប	១		ការក្លែងបន្លំពុំមានផលប៉ះពាល់ដល់និរន្តរភាពការងារ
I២	៣.មធ្យម	៣		ការក្លែងបន្លំមានផលប៉ះពាល់ដល់ការចំណាយលើការប្រតិបត្តិការការងារ
I៣	៥.ខ្ពស់	៥		ការក្លែងបន្លំមានផលប៉ះពាល់ដល់នយោបាយ
៣.លទ្ធភាព(ផ្តល់សេវាកម្ម ឬបរិក្ខារ)				
ល.រ	ចំណាត់ថ្នាក់	ពិន្ទុ		សេចក្តីអធិប្បាយ
A១	១.ទាប	១		មិនដំណើរការ ឬមិនមានប្រតិបត្តិការលើសពី២៤ម៉ោង

A២	៣.មធ្យម	៣		មិនដំណើរការ ឬមិនមានប្រតិបត្តិការរហូតដល់២៤ ម៉ោង
A៣	៥.ខ្ពស់	៥		មិនដំណើរការ ឬមិនមានប្រតិបត្តិការរហូតដល់៤ម៉ោង

លទ្ធផលចុងក្រោយនៃការវាយតំលៃ អំពីសំភារៈព័ត៌មានណាមួយឆ្លុះឲ្យឃើញតាមរយៈពិន្ទុសរុបទទួលបានពីចំនុចទាំងបី។ ប្រសិនបើលោកអ្នកគិតថាលទ្ធផលសរុបនៃការវាយតំលៃអំពីសំភារៈព័ត៌មានមានលក្ខណៈខុសពីការពិតជាក់ស្តែងសូមធ្វើការពិនិត្យ និងកែសម្រួលឡើងវិញ នូវចំនួនពិន្ទុនៅក្នុងចំនុចវាយតំលៃទាំងបីនោះ។

៤.ការវាយតំលៃអំពីសំភារៈព័ត៌មាន(ពិន្ទុសរុប=ការសម្ងាត់+ផលប៉ះពាល់+លទ្ធភាព)				
ល.រ	ចំណាត់ថ្នាក់	ពិន្ទុ	ពិន្ទុសរុប	សេចក្តីអធិប្បាយ
As១	១.ទាប	១	៣ ដល់ ៦	សំភារៈព័ត៌មានមានផល់ប៉ះពាល់ មធ្យមលើប្រតិបត្តិការការងារ
As២	២.មធ្យម	២	៧ ដល់ ១២	សំភារៈព័ត៌មានមានផល់ប៉ះពាល់ យ៉ាងខ្លាំងលើប្រតិបត្តិការការងារ
As៤	៣.ខ្ពស់	៣	១៣ ដល់ ១៥	សំភារៈព័ត៌មានមានផល់ប៉ះពាល់យ៉ាងខ្លាំងលើអភិបាលកិច្ច

<u>ជំណាក់កាលទី៣៖ ការពិនិត្យមើលអំពីសំភារៈព័ត៌មាន</u>

ក្នុងការពិនិត្យមើលអំពីសំភារៈព័ត៌មានលោកអ្នកគ្រាន់តែជ្រើសរើសពាក្យបានអនុវត្ត ឬមិនបាន អនុវត្តសំរាប់ចំនុចត្រួតពិនិត្យនីមួយៗ។

(ចំនុចត្រួតពិនិត្យជាគំរូមួយចំនួនទាក់ទងនឹងកុំព្យូទ័រ)

- បង្កើតឈ្មោះអ្នកប្រើប្រាស់ម្នាក់យ៉ាងតិច នៅគ្រប់កុំព្យូទ័រទាំងអស់ ។

- ប្រើប្រាស់នូវពាក្យ ឬលេខសម្ងាត់ដែលពិបាកលួចចំលង និងធ្វើការផ្លាស់ប្តូរវាជាទៀងទាត់ ។
- ហាមឃាត់ការចែករំលែកការប្រើប្រាស់រួមគ្នាដោយប្រើគណនី (User ID , Password) តែមួយ។
- បង្ហាញលើកញ្ចក់កុំព្យូទ័រដោយស្រីនសេវឺ (Screen Saver) ដែលមានដាក់ពាក្យ ឬលេខសម្ងាត់។
- ធ្វើការរុករកមេរោគកុំព្យូទ័រ (Scan) នៅក្នុងឧបករណ៍ផ្ទុកទិន្នន័យជាប្រចាំដោយប្រើបាស់កម្មវិធីកំចាត់មេរោគ។
- កំណត់មុខងារចាប់មេរោគដោយស្វ័យប្រវត្តិ។
- ធ្វើអោយកម្មវិធីប្រឆាំងមេរោគទាន់សម័យ (Update Definition) យ៉ាងតិចចំនួន មួយដង ក្នុងមួយសប្តាហ៍ ។
- រក្សាទុកបញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ និង ធ្វើអោយកម្មវិធីប្រឆាំងមេរោគទាន់សម័យ (Update Definition) ។
- តភ្ជាប់កុំព្យូទ័រទាំងអស់ទៅកាន់ឧបករណ៍សំរាប់រក្សាទុកចរន្តអគ្គិសនីបម្រុង (UPS)។
- ត្រូវលុបសម្អាតទិន្នន័យរូបវន្ត (Physical Formatting) ក្នុងឧបករណ៍ផ្ទុកទិន្នន័យនៃកុំព្យូទ័រដោយមិនបន្សល់ទុកនូវទិន្នន័យ ឬព័ត៌មានដែលអាចទាញមកវិញបាន។

<u>ជំណាក់កាលទី៤៖ ការវាយតំលៃអំពីហានិភ័យ</u>

ធ្វើការវាយតំលៃអំពីបញ្ហាគំរាម និងអំពីភាពងាយទទួលរងនូវផែលប៉ះពាល់ដោយយោងទៅតាមលក្ខណៈវិនិច្ឆ័យដែលបានផ្តល់ជូន។ ដើម្បីបង្កលក្ខណៈងាយស្រួលក្នុងការកំណត់នូវបញ្ហាគំរាមជាក់លាក់ទាំងឡាយ ចំនុចត្រួតពិនិត្យនីមួយៗ

ត្រូវបានផ្តល់ជូននូវឧទាហរណ៍ទាក់ទង នឹងបញ្ហាគំរាម ដែលបានរៀបរាប់នៅក្នុងជួរបន្ទាត់ «សេចក្តីអធិប្បាយ»។

៦.បញ្ហាគំរាម				
ល.រ	ចំណាត់ថ្នាក់	ពិន្ទុ		សេចក្តីអធិប្បាយ
T១	១.ទាប	១		លទ្ធភាពកើតមានបញ្ហាគំរាមក្នុងកំរិតទាប
T២	២.មធ្យម	២		លទ្ធភាពកើតមានបញ្ហាគំរាមក្នុងកំរិតមធ្យម
T៣	៣.ខ្ពស់	៣		លទ្ធភាពកើតមានបញ្ហាគំរាមក្នុងកំរិតខ្ពស់
៧.ភាពងាយទទួលរងផលប៉ះពាល់				
ល.រ	ចំណាត់ថ្នាក់	ពិន្ទុ		សេចក្តីអធិប្បាយ
V១	១.ទាប	១		ត្រូវបានគ្រប់គ្រងដោយត្រឹមត្រូវដើម្បីការពារប្រឆាំងនឹងបញ្ហាគំរាម
V២	២.មធ្យម	២		ត្រូវបានគ្រប់គ្រង ប៉ុន្តែត្រូវការការកែលំអ
V៣	៣.បង្គួរ	៣		ត្រូវបានគ្រប់គ្រងប្រកបដោយតុល្យភាព ប៉ុន្តែត្រូវការការកែលំអ
V៤	៤.ខ្ពស់	៤		គ្មានវិធានការគ្រប់គ្រង ដើម្បីទប់ទល់និងបញ្ហាគំរាម

លទ្ធផលសរុបនៃការវាយតំលៃអំពីហានិភ័យត្រូវបានកំណត់ដោយយោងទៅតាមការគណនាខាងក្រោម៖

៨.ការវាយតំលៃអំពីហានិភ័យ(ពិន្ទុសរុប=(សំភារៈព័ត៌មាន+បញ្ហាគំរាម)*ភាពងាយទទួលរងផលប៉ះពាល់)				
ល.រ	ចំណាត់ថ្នាក់	ពិន្ទុ	ពិន្ទុសរុប	សេចក្តីអធិប្បាយ

R១	១.ទាប	១	២ ដល់ ៦	ហានិភ័យដែលអាចកើតឡើងបាន
R២	២.ខ្ពស់	២	៨ ដល់ ២៤	ហានិភ័យដែលអាចកើតឡើងបាន និងត្រូវការការគ្រប់គ្រង

<u>ជំណាក់កាលទី៥៖ កំណត់ការគ្រប់គ្រង</u>

រាល់ចំនុចត្រួតពិនិត្យទាំងអស់ ដែលត្រូវបានវាយតំលៃថាមានហានិភ័យ « ខ្ពស់» គួរត្រូវបានគ្រប់គ្រងដោយម៉ត់ចត់។ ជាទូទៅស្ថាប័នទាំងឡាយត្រូវអនុវត្តតាមវិធាន និងនីតិវិធីនានាដើម្បីកាត់បន្ថយហានិភ័យទាំងនេះ។ ការប្រព្រឹត្តបែបនេះនាំឲ្យយើងអាចបង្កើតបាន នូវឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន សំរាប់រាជរដ្ឋាភិបាល។ បន្ទាប់ពីបានកំណត់ការគ្រប់គ្រង និងដោះស្រាយរាល់បញ្ហាទាក់ទងនឹងហានិភ័យរួចមក សូមធ្វើការវាយតំលៃអំពីហានិភ័យទាំងនេះម្តងទៀត ដើម្បីឲ្យប្រាកដថា រាល់ចំនុចត្រួតពិនិត្យទាំងអស់ ត្រូវបានវាយតំលៃក្នុងកំរិតមួយ «ទាប» (ឧទាហរណ៍៖ ធ្វើការកំណត់វិធាន និងនីតិវិធីនៅក្នុងឯកសារវិធានស្តីពី GIS)។

<u>៤.១.៤. ការបង្កើតឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល</u>

ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ត្រូវបានចងក្រងដោយស្ថាប័ននីមួយៗ។ យោងតាមលទ្ធផលនៃការវាយតំលៃអំពីហានិភ័យដំណោះស្រាយដ៏ចម្បងនោះ គឺការកំណត់វិធាន និងនីតិវិធីដើម្បីកាត់បន្ថយហានិភ័យដែលកើតឡើង។ ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលត្រូវបានចែកចេញជាប្រាំផ្នែកគឺ៖

១)វិសាលភាព ជាផ្នែកដែលត្រូវបានកំណត់នៅក្នុងចំនុចទី ៤.១.២ ស្តីអំពីការកំណត់វិសាលភាពនៃ GISMS

២) ការរៀបចំសន្តិសុខព័ត៌មាន

៣) វិធាន និងនីតិវិធី

៤) ការបណ្តុះបណ្តាលស្តីអំពីសន្តិសុខព័ត៌មាន

៥) ការប៉ាន់ប្រមាណអំពីកំរិតនៃការត្រួតពិនិត្យ និងការអនុវត្តន៍។

ស្ថាប័ននីមួយៗត្រូវបានតម្រូវឲ្យប្រើប្រាស់ ឯកសារវិធានគំរូអំពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ផ្តល់ជូនដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មារបស់រាជរដ្ឋាភិបាល ដែលតួនាទីរបស់ការិយាល័យនេះនឹងត្រូវបានរៀបរាប់នៅក្នុងជំពូកទី៥ ស្តីអំពីទំនួលខុសត្រូវក្នុងការគ្រប់គ្រង។ ដំណាក់កាលចំនួនបីខាងក្រោមពន្យល់អំពីគន្លឹះក្នុងការចងក្រងឯកសារវិធានស្តីអំពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

<u>៤.១.៤.១.ការកំណត់វិសាលភាពនៃ GISMS នៅក្នុងឯកសារវិធានស្តីពី GIS</u>

វិសាលភាពនៃ GISMS ដែលបានកំណត់នៅក្នុងចំនុចទី ៤.១.២ ត្រូវបានកត់ត្រាចូល ទៅក្នុងឯកសារវិធានស្តីពី GIS ដែលមានការផ្តល់ អនុសាសន៍ឲ្យមានការបញ្ជាក់បន្ថែម អំពីសំភារៈព័ត៌មានព្រមជាមួយនឹងមន្ត្រី ឬអង្គភាព ឬទីតាំងជារូបវន្តែ៣ក់ព័ន្ធនឹងសំភារៈទាំងនោះដូចមាន បង្ហាញតាមរយៈឧទាហរណ៍នៅក្នុងឯកសារវិធានគំរូ។

<u>៤.១.៤.២.ការកំណត់នីតិវិធី ឬវិធានដែលមិនស្ថិតក្នុងក្របខ័ណ្ឌនៃការអនុវត្ត នៅក្នុងឯកសារវិធានគំរូ</u>

នៅក្នុងវិសាលភាពនៃស្ថាប័ននីមួយៗ វិធាននិងនីតិវិធីនានាអាស្រ័យទៅលើ សំភារៈព័ត៌មានជាក់ស្តែងនិងការសម្ងាត់របស់ពួកគេ។ វាមិនមានការចាំបាច់ក្នុងការកំណត់វិធាន និងនីតិវិធីទាំងនេះទេ លើកលែងតែមានសំភារៈ

ព័ត៌មានជាក់លាក់ដែលបានរួមបញ្ចូលនៅក្នុងវិសាលភាពនេះ។

៤.១.៤.៣. <u>ការកែតម្រូវវិធាន និង នីតិវិធីនៅក្នុងឯកសារវិធានគំរូ</u>

វិធាន និងនីតិវិធីទាំងនេះគួរត្រូវបានកំណត់ថា «មានសន្តិសុខជាងមុន» ប្រសិនបើ ព័ត៌មានដែលបានប្រើប្រាស់នៅក្នុងស្ថាប័នមួយកាន់តែមានលក្ខណៈសម្ងាត់ ដោយយោងទៅតាមលទ្ធផលនៃការវាយតំលៃអំពីហានិភ័យ។ ប្រសិនបើ ឯកសារវិធានគំរូពុំមានសំការៈព័ត៌មាន ដែលបានបញ្ចូលទៅក្នុងវិសាលភាពនោះទេ សូមសរសេរថាវិធាន និងនីតិវិធីទាំងនេះ«នឹងត្រូវ បានកំណត់»។ ក្នុងករណីនេះវាជាប្រការសំខាន់មួយ ដែលត្រូវពិភាក្សាជាមួយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល មុននឹងចាប់ផ្តើមកំណត់វិធាន និងនីតិវិធីនានា ដើម្បីធ្វើការសម្រេចអំពីអ្នកដែល នឹងត្រូវបង្កើតបទដ្ឋាននៃសំការៈព័ត៌មានថ្មីរបស់រាជរដ្ឋាភិបាលកម្ពុជា ដែលត្រូវបញ្ចូលទៅក្នុងវិសាលភាព។

៤.១.៥. <u>ការស្នើសុំការអនុម័ត</u>

ការផ្តល់ការអនុម័តត្រូវបានចែកចេញជាពីរដំណាក់កាលៈ

- ការអនុម័តដោយថ្នាក់ដឹកនាំកំពូលនៃស្ថាប័ន
- ការអនុម័តដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

នៅពេលដែលដំណាក់កាលទាំងពីរដូចបានរៀបរាប់ពីចំនុច ៤.១.១ ដល់ចំនុច ៤.១.៤ ត្រូវបានបញ្ចប់ និងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ ឯកសារវិធានស្តីពី សន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ដែលក្នុងនោះស្តីអំពី ការតែងតាំងអ្នកគ្រប់គ្រង CISO និង IS ត្រូវបានចងក្រងរួចរាល់ ដំណើរការរៀបចំផែនការ និងឯកសារទាំងនេះគួរត្រូវបានពិនិត្យឡើងវិញនិងទទួលបានការអនុម័តពីការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាលជាមុនសិន ដើម្បីឲ្យប្រាកដថាពួកវាត្រូវបានបង្កើតឡើងដោយស្របទៅតាម

គោលការណ៍របស់ GISMS។

ឆ្លងតាមការវាយតំលៃដោយស្វ័យប្រវត្តិនៅក្នុង ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យមានករណីលើកលែងមួយដែលអនុញ្ញាតឲ្យមានការទទួលយកហានិភ័យ ដែលមិនធ្លាប់ជួបប្រទះ ទោះបីជាវាស្ថិតនៅក្នុងកំរិតមួយដែលហួសពីការដែលអាចទទួលយកបាន នេះជាហេតុផលចាំបាច់ច្បាស់លាស់ និងជំ្រមត្រូវមួយក្នុងការសម្រេចចិត្ត ដើម្បីទទួលបាននូវការអនុម័តពីការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

ការទទួលបានការអនុម័តពីថ្នាក់ដឹកនាំកំពូលនៃស្ថាប័ន គឺជាការចាំបាច់បំផុតសំរាប់ការអនុវត្តន៍ការងារនៅក្នុងស្ថាប័នឲ្យបានពេញលេញ និងប្រកបដោយប្រសិទ្ធិភាព។

៤.២. <u>ការអនុវត្តន៍ និងប្រតិបត្តិការ</u>

នៅពេលអនុវត្ត GISMS នៅក្នុងស្ថាប័នមួយ ត្រូវបង្កើតការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានដោយនាយកផ្នែកនេះត្រូវធ្វើការចាត់តាំងសមាជិកមួយចំនួនសំរាប់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាននោះដើម្បីរៀបចំ និងផ្តល់ការបណ្តុះបណ្តាល។

ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន គឺជាប្រព័ន្ធ «គ្រប់គ្រង» មួយ ហេតុដូចនេះមន្ត្រីដែលមានឋានៈខ្ពស់ជាងគួរត្រូវបានបណ្តុះបណ្តាលមុនគេ ដើម្បីឲ្យពួកគាត់មានចំណេះដឹង ទាក់ទងនិងប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងអាចដឹកនាំមន្ត្រីក្រោមឪវាទក្នុងការអនុវត្តន៍ប្រព័ន្ធនេះ។

៤.៣. <u>ការតាមដាន និងពិនិត្យមើលឡើងវិញ</u>

ដើម្បីឲ្យការប្រើប្រាស់ ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានចាក់គ្រឹះទៅក្នុងអង្គភាពរដ្ឋយើងត្រូវធ្វើដំណើរនៅលើផ្លូវដ៏វែងឆ្ងាយមួយជាចាំបាច់ក្នុងការខិតខំប្រឹងប្រែង និងកែលំអជាបន្តបន្ទាប់។ ដើម្បីយល់អំពីគោលដៅ និងពិភាក្សាអំពីការកែលំអនានា វាត្រូវការនូវឧបករណ៍សំរាប់វាស់កំរិតការងារទាំងនេះដែល នឹងត្រូវបានកំណត់នៅក្នុងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

- ការធ្វើសវនកម្មផ្ទៃក្នុង ដើម្បីអង្កេតអំពីប្រសិទ្ធិភាពនៃប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន

ដែលបានអនុវត្ត ក៏ត្រូវបានស្នើឡើង ដើម្បីស្វែងរកបញ្ហានានាសំរាប់ការកំណត់កំរិតនៃហានិភ័យក្នុងដំណើរការរៀបចំផែនការ និង/ឬ សំរាប់ពិនិត្យឡើងវិញនូវកំរិតហានិភ័យដែលអាចទទួលយកបាន។

- លទ្ធផលថ្មីៗនៃការវាយតំលៃអំពីហានិភ័យ គួរត្រូវបានបញ្ចូលទៅក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ។
- ចំនួនដងនៃការត្រួតពិនិត្យ និងសកម្មភាពអនុវត្តន៍គួរត្រូវបានកំណត់នៅក្នុងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។
- សកម្មភាពទាំងនេះគួរតែត្រូវបានអនុវត្តយ៉ាងហោចណាស់លើសពីមួយដងក្នុងមួយឆ្នាំ។

<u>៤.៤. ធ្វើការថែទាំ និងលើកកំពស់</u>

លទ្ធផលនៃការវាស់កំរិត និងការធ្វើសវនកម្មផ្ទៃក្នុងការងារ នាំឲ្យយើងអាចធ្វើការសម្រេចចិត្តអំពីសកម្មភាពនានា ដើម្បីលើកកំពស់ប្រសិទ្ធិភាពនៃប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងជៀសវាងពីហានិភ័យនានា។ សកម្មភាពទាំងនេះមិនត្រឹមតែជួយបង្កើនប្រសិទ្ធភាពនៃវិធាន និងនិតិវិធីនានាប៉ុណ្ណោះទេ ពួកវាថែមទាំងជួយផ្តល់ជំណោះស្រាយក្នុងការដំឡើងកម្មវិធី និងឧបករណ៍ផ្នែករឹងកុំព្យូទ័រសំរាប់ការពារបណ្តាញកុំព្យូទ័រ ឬប្រព័ន្ធផងដែរ។ សកម្មភាពទាំងនេះក៏អាចរួមបញ្ចូល នូវការលុបបំបាត់វិធាននិងនីតិវិធីមួយចំនួនដើម្បីតម្រូវទៅនឹងបំលាស់ប្តូរតួនាទី និងប្រតិបត្តិការការងារនៃស្ថាប័ននីមួយៗ។

<u>៤.៥. ការគ្រប់គ្រងឯកសារ</u>

ផ្នែកនេះនឹងធ្វើការកំណត់ អំពីរចនាសម្ព័ន្ធ ការអនុញ្ញាត ការកែសម្រួល ការចែកចាយ លទ្ធកម្ម និងការរក្សាទុកឯកសារ។

<u>៤.៥.១. រចនាសម្ព័ន្ធឯកសារ និងការអនុញ្ញាត</u>

ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលមានឯកសារសំខាន់ៗ ចំនួន

បួនប្រភេទគឺ៖

១) <u>គោលនយោបាយស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល</u>

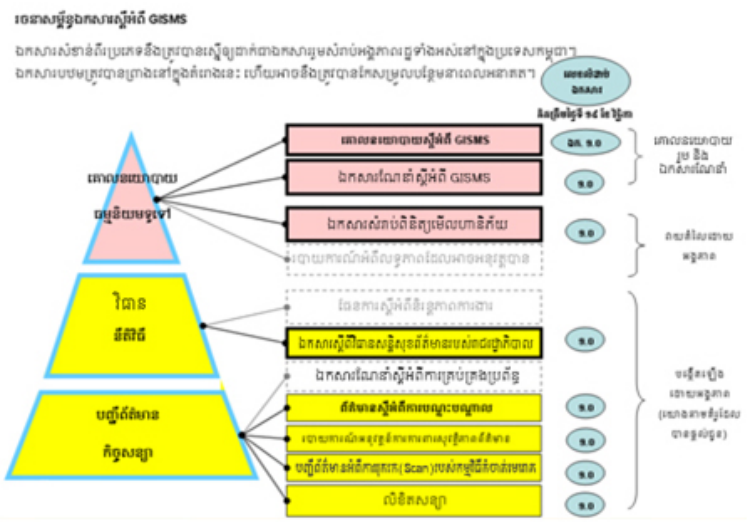
២) <u>ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល</u>

ឯកសារទាំងនេះ ត្រូវបានធ្វើសេចក្តីព្រាង ដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ពិនិត្យឡើងវិញដោយ គណៈកម្មាធិការនាយកផ្នែកព័ត៌មានរបស់រាជរដ្ឋាភិបាល (ជាឈ្មោះបណ្តោះអាសន្នរហូតទាល់តែមានឈ្មោះជាផ្លូវការមួយត្រូវបានបង្កើតឡើងសំរាប់ជំនួស) និងផ្តល់ការអនុញ្ញាតដោយប្រធាន GCIO (ជាឈ្មោះបណ្តោះអាសន្ន)។ គោលនយោបាយស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល គួរត្រូវបានប្រកាសដោយប្រមុខនៃរាជរដ្ឋាភិបាលកម្ពុជា។ *ឯកសារបឋមលេខ ១.០ ត្រូវបានចងក្រងជាលើកទីមួយ ដោយ អ.អ.ប.គ.ព ក្រោមការឧបត្ថម្ភគាំទ្រដោយ JICA។*

៣) <u>ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ</u>

ចំនុចត្រួតពិនិត្យត្រូវបានព្រាងដោយ ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលពិនិត្យឡើងវិញ និងផ្តល់ការអនុញ្ញាតដោយគណៈកម្មាធិការ GCIO (ជាឈ្មោះបណ្តោះអាសន្នរហូតទាល់តែមានឈ្មោះជាផ្លូវការមួយត្រូវបានបង្កើតឡើងជំនួស)។ ឯកសារមិនទាន់បំពេញព័ត៌មានក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ ផ្តល់នូវចំលើយជ្រើសរើសជាស្រេចសំរាប់ការវាយតំលៃអំពីហានិភ័យ ហើយឯកសារដែលបានបំពេញរួចទាំងនេះ នឹងត្រូវបានវាយតំលៃ និងកែតម្រូវដោយសាមីស្តាប័ន។ សូមបំពេញឈ្មោះស្តាប័ននៅក្នុងឯកសារទាំងនេះ

បន្ទាប់ពីបានវាយតំលៃរួច។



៤) ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល

ឯកសារនេះត្រូវបានចងក្រងដោយស្ថាប័ននីមួយៗ។ ឯកសារវិធានគំរូមួយស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលត្រូវបានធ្វើសេចក្តីព្រាងដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ដោយយោងទៅតាមចំលើយជ្រើសរើសសំរាប់វាយតំលៃ អំពីហានិភ័យពីឯកសារមិនទាន់បំពេញព័ត៌មានក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ។ ការចងក្រងឯកសារនេះគួរត្រូវបានទទួលការអនុញ្ញាតដោយថ្នាក់ដឹកនាំស្ថាប័ន។ សូមបញ្ចូលឈ្មោះស្ថាប័ននីមួយៗទៅក្នុងឯកសារនេះ។ ឯកសារបន្ថែមដ៏ទៃទៀតត្រូវបានបង្កើត និងប្រើប្រាស់ដោយស្ថាប័ននីមួយៗ។

៤.៥.២. <u>ការកែសម្រួល ការចែកចាយ លទ្ធកម្ម និងការរក្សាទុកឯកសារ</u>

<u>ការកែសម្រួល</u>

គោលនយោបាយស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល គួរត្រូវបានប្រកាសដោយប្រមុខនៃរាជរដ្ឋាភិបាលកម្ពុជា។ ដូច្នេះបែបបទនៃការកែសម្រួលត្រូវកំណត់ដោយវិធានដ៏ទៃទៀតដែលបង្កើតឡើងដោយរាជរដ្ឋាភិបាលកម្ពុជា។ (បញ្ហានេះគួរត្រូវកំណត់ក្នុងក្រិតមួយជាក់លាក់នាពេលអនាគត) ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល និងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យត្រូវបានកែសម្រួលជារៀងរាល់ឆ្នាំដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល យោងទៅតាមមតិយោបល់ ឬសំណើរសុំពីស្ថាប័ននានាដែលនឹងកំពុងអនុវត្តប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន។ ឯកសារព្រាងទាំងនេះត្រូវបានផ្តល់ការអនុញ្ញាតដោយយោងតាមបែបបទដូចគ្នា ដូចបានកំណត់នៅក្នុងចំនុចទី ៤.៥.១ ស្តីអំពីរចនាសម្ព័ន្ធឯកសារ និងការផ្តល់ការអនុញ្ញាត។

ការកែសម្រួលឯកសារដ៏ទៃទៀត ទាក់ទងនឹងប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលត្រូវបានកំណត់ដោយស្ថាប័ននីមួយៗ ដោយយោងទៅតាមវដ្តដូចបានរៀបរាប់នៅក្នុងចំនុចទី៤.៣ស្តីអំពីការត្រួតពិនិត្យនិងចំនុចទី ៤.៤(សកម្មភាពអនុវត្តន៍)។

ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ និងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល ត្រូវមានប្រវត្តិនៃការកែសម្រួលដើម្បីឲ្យដឹងប្រាកដថា មួយណាដែលអ្នកអានយកជាឯកសារយោង។

<u>ការចែកចាយ លទ្ធកម្ម និងការរក្សាទុក</u>

កំរិតនៃភាពសម្ងាត់របស់ឯកសារទាក់ទងនឹងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលមានការ ប្រែប្រួល ទៅតាមឯកកសារនីមួយៗ ដូចបានកំណត់ខាងក្រោម៖

១. គោលនយោបាយ និងឯកសារណែនាំស្តីអំពីសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល ត្រូវបានចាត់ទុកជាឯកសារ «សាធារណៈ» ដែលមានន័យថាឯកសារទាំងនេះអាចនឹងត្រូវបាន បោះពុម្ពផ្សាយហើយប្រជាពលរដ្ឋកម្ពុជាទាំងអស់អាចរកអានបានដោយសេរី។

២. ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យដែលមិនទាន់បានវាយតំលៃ មានកត់ត្រានូវហានិភ័យដែលមិនទាន់បានកំណត់ក្នុងស្តាប់ននីមួយៗ ហើយវាត្រូវបានចាត់ទុកជាឯកសារ «សាធារណៈ» ។ ឯកសារដែលបានវាយតំលៃរួចមានកត់ត្រានូវហានិភ័យដែលបានកំណត់ជាក់លាក់ (ដូចជាបញ្ហាគំរាម និងភាពងាយទទួលរងនូវផលប៉ះពាល់)។ ដូចនេះ វាត្រូវបានចាត់ទុកជាឯកសារ «ផ្ទៃក្នុង» ដែលតម្រូវឲ្យមានការប្រុងប្រយ័ត្នក្នុងការចែកចាយ លទ្ធកម្ម និងការរក្សាទុក និងសំរាប់ ប្រើប្រាស់តែក្នុងប្រតិបត្តិការការងាររបស់រាជរដ្ឋាភិបាលប៉ុណ្ណោះ ។

៣. ឯកសារវិធានស្តីពី GIS រួមមាននូវវិធាន និងនីតិវិធីការងារផ្ទៃក្នុង ហើយវាត្រូវបានចាត់ទុកជាឯកសារ «ផ្ទៃក្នុង» ។

ត្រូវបញ្ជូនវិធានចំលងនៃឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ ឯកសារវិធានស្តីអំពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលដែលបានកែសម្រួលនិងវាយតំលៃរួច និងឯកសារមិនទាន់ បំពេញព័ត៌មានទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល និងរក្សាទុកឯកសារទាំងនេះរយៈពេលប្រាំឆ្នាំ។
ការចែកចាយលទ្ធកម្ម និងការរក្សាទុកឯកសារដ៏ទៃទៀតត្រូវបានកំណត់ដោយ

ស្ថាប័ននីមួយៗ វាជាការសំខាន់ដែលត្រូវមានការប្រុងប្រយ័ត្នខ្ពស់ក្នុងការទុកដាក់ឯកសារដែលមានផ្ទុកនូវព័ត៌មានសម្ងាត់ (ដូចជា IP address របស់ម៉ាស៊ីនកុំព្យូទ័រមេ (server) និងព័ត៌មានផ្ទាល់ខ្លួនជាដើម)។

៤.៦. <u>ការគ្រប់គ្រងបញ្ជីព័ត៌មាន</u>

វាជាការចាំបាច់ដែលត្រូវគ្រប់គ្រងបញ្ជីព័ត៌មាន (Records) សំរាប់ការអនុវត្តន៍តាមវិធាន និងនីតិវិធីនានា។ ការគ្រប់គ្រងលើការអនុញ្ញាតការកែសម្រួលការចែកចាយលទ្ធកម្មនិងការរក្សាទុកឯកសារមិនទាន់បំពេញព័ត៌មានអាច ត្រូវបានកំណត់នៅក្នុងឯកសារវិធានស្តីអំពីសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល។

ជាទូទៅបញ្ជីព័ត៌មានត្រូវបានបញ្ជូនដោយមន្ត្រីដែលបានចាត់តាំងត្រូវតម្កល់ និងបំរុងទុកដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន។សូមរក្សាការចុះលំដាប់លេខរៀងលើកំណត់ត្រាព័ត៌មាននីមួយៗ ដោយប្រើប្រាស់លេខសំគាល់ដាច់ដោយឡែកពីគ្នា។ រយៈពេលកំណត់សំរាប់ការរក្សាទុកបញ្ជីព័ត៌មានទាំងនេះគឺមួយឆ្នាំ និងប្រែប្រួលទៅតាមការកំណត់ដាក់ស្តែង។

បញ្ជីព័ត៌មានតែងតែផ្ទុកនូវព័ត៌មានសម្ងាត់ដូចជា IP Address របស់ម៉ាស៊ីនកុំព្យូទ័រមេ (Server) និងព័ត៌មានផ្ទាល់ខ្លួនជាដើម ដែលតម្រូវឲ្យមានការរក្សាទុកដោយយកចិត្តទុកដាក់និងប្រុងប្រយ័ត្ន។

៥. ចំនួលខុសត្រូវក្នុងការងារគ្រប់គ្រង

៥.១. <u>កិច្ចប្រឹងប្រែងក្នុងការងារគ្រប់គ្រង</u>

តាមរយៈសេចក្តីប្រកាសស្តី អំពីគោលនយោបាយរបស់ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ថ្នាក់ដឹកនាំរាជរដ្ឋាភិបាលកម្ពុជាមាននាទីទទួលខុសត្រូវក្នុងការបង្កើតការអនុវត្តន៍ ការតាមដាន និងការថែទាំប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដើម្បីរក្សាឲ្យបាននូវនិរន្តរភាពផ្នែករដ្ឋបាល នៃរាជរដ្ឋាភិបាលកម្ពុជា និងដើម្បីកាត់បន្ថយហានិភ័យនៃការខូចខាត

តាមរយៈការបង្ការនូវឧប្បត្តិហេតុផ្សេងៗ និងតាមរយៈការកាត់បន្ថយផលប៉ះពាល់ នៃឧប្បត្តិហេតុទាំងនេះដែលអាចនឹងកើតមានឡើង។ ថ្នាក់ដឹកនាំនៅតាមនាយកដ្ឋាននីមួយៗមាននាទីទទួលខុសត្រូវដោយផ្ទាល់ចំពោះការអនុវត្តន៍ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងជាពិសេសចំពោះការធ្វើឲ្យបុគ្គលិកក្រោមឪវាទទាំងអស់អនុវត្តតាម។

<u>៥.២. អង្គភាពការពារសន្តិសុខព័ត៌មានវិទ្យារបស់រាជរដ្ឋាភិបាល</u>

គ្រប់ស្ថាប័នទាំងអស់របស់រាជរដ្ឋាភិបាលកម្ពុជាត្រូវតែងតាំង នាយកផ្នែកព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GCIO) សំរាប់ស្ថាប័នរបស់ខ្លួន។ ប្រមុខរាជរដ្ឋាភិបាលកម្ពុជាត្រូវបង្កើតគណៈកម្មាធិការនាយកផ្នែកព័ត៌មានរបស់រាជរដ្ឋាភិបាល (គណៈកម្មាធិការ GCIO)។ ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (ការិយាល័យ GIS) ត្រូវបានបង្កើតឡើងដោយមានតួនាទី ជាលេខាធិការរបស់គណៈកម្មាធិការនាយកផ្នែកព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GCIO) ហើយអ.អ.ប.គ.ពទទួលខុសត្រូវក្នុងការបំពេញទួនាទីជាការិយាល័យគ្រប់គ្រង សន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលនេះ។ *សូមបញ្ជាក់ថាការកំណត់នេះគឺជាសេចក្តីព្រាងប៉ុណ្ណោះ។ ការឧបត្ថម្ភគាំទ្រសំរាប់ GCIO នឹងត្រូវបានចាត់ចែងនៅក្នុងគំរោងអភិវឌ្ឍន៍ GCIO។*

ថ្នាក់ដឹកនាំ របស់អង្គភាពរដ្ឋនីមួយៗ ត្រូវតែងតាំងនាយកផ្នែកសន្តិសុខព័ត៌មាន (CISO) ដែលទទួលបានសិទ្ធិបង្កើតនូវការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន។

<u>៥.៣. ការអភិវឌ្ឍន៍សមត្ថភាព</u>

សមត្ថភាពគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវបានកំណត់ដូចខាងក្រោម ហើយសមត្ថភាពទាំងនេះ ត្រូវបានលើកកំពស់តាមរយៈ ការគ្រប់គ្រងរបស់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដែលជាមជ្ឈមណ្ឌលកំរិតឧត្តមមួយ។

ប្រភេទសមត្ថភាពគ្រប់គ្រងសន្តិសុខព័ត៌មាន៖

១. ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន

២. សន្តិសុខហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញ កុំព្យូទ័រ

៣. សន្តិសុខរបស់កម្មវិធី

៤. សន្តិសុខរបស់ប្រព័ន្ធប្រតិបត្តិការ (OS)

៥. ប្រព័ន្ធការពារសុវត្ថិភាពបណ្តាញកុំព្យូទ័រ (Firewall)

៦. ការរារាំងការចូលបំផ្លិចបំផ្លាញ

៧. មេរោគ (Virus)

៨. វិធីសាស្ត្រ Programming ប្រកបដោយសន្តិសុខ

៩. ប្រតិបត្តិការ ការពារសន្តិសុខ

១០. Protocol សំរាប់ការពារសន្តិសុខ

១១. ការបញ្ជាក់តាមយថាភូត (Authentication)

១២. ហេដ្ឋារចនាសម្ព័ន្ធគន្លឹះដែលអាចប្រើប្រាស់កូនសោសាធារណៈ (PKI)

១៣. បន្លាស់ប្តូរទំរង់ដើមនៃព័ត៌មានរបស់កុំព្យូទ័រ (Encryption)

១៤. ហត្ថលេខាអេឡិចត្រូនិច (Electronic Signature)

១៥. ការចូលក្នុងប្រព័ន្ធកុំព្យូទ័រដោយគ្មានការអនុញ្ញាត

១៦. នីតិកម្ម និងធម្មនិយម

<u>៥.៤. ការពិនិត្យមើលអំពីការគ្រប់គ្រង</u>

GCIO ត្រូវបានតម្រូវឲ្យពិនិត្យឡើងវិញ រាល់ដំណើរការទាំងអស់នៃ GISMS របស់អង្គភាពរដ្ឋនានា ហើយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ត្រូវបានអនុញ្ញាតឲ្យជាក់សំណើរទៅកាន់អង្គភាពរដ្ឋទាំងអស់ឲ្យរាយការណ៍អំពីស្ថានភាព GISMS របស់ពួកគេ។

ការិយាល័យរបស់ CISO និងការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន នៅតាមអង្គភាពរដ្ឋនីមួយៗ ត្រូវបានតម្រូវឲ្យធ្វើប្រតិបត្តិការដូចគ្នាក្នុងការងារពិនិត្យឡើងវិញរាល់ដំណើរការនៃ

GISMS ដែលជាការបំពេញនូវតម្រូវការនានារបស់ការិយាល័យ GIS និងចំនុចទី ៤.៣ ស្តីអំពីការត្រួតពិនិត្យ (ធ្វើការតាមដាន និងពិនិត្យមើលឡើងវិញ)។

៦. ការគ្រប់គ្រង និងដំណោះស្រាយ

៦.១. ប្រភេទនៃការគ្រប់គ្រង

ការគ្រប់គ្រងត្រូវបានចែកជាបួនផ្នែកសំខាន់ រួមមាន ការកាត់បន្ថយហានិភ័យ ការផ្ទេរហានិភ័យ ការចៀសវាងហានិភ័យ និងការទទួលយកហានិភ័យ (ដោយចេតនានិងតាមតថភាពជាក់ស្តែង)។

ការកាត់បន្ថយហានិភ័យ គឺជាចំណាត់ការក្នុងការគ្រប់គ្រងដ៏សំខាន់មួយប្រឆាំងនឹង ហានិភ័យដែលបានរកឃើញ។ ឧទាហរណ៍កុំព្យូទ័រមួយគ្រឿងដែលងាយទទួលរងនូវការវាយលុកដោយមេរោគ ត្រូវដំឡើងនិងប្រតិបត្តិការកម្មវិធីប្រឆាំងមេរោគ ដែលជាវិធានការមួយក្នុងការគ្រប់គ្រង។

ការផ្ទេរហានិភ័យ គឺជាវិធានការគ្រប់គ្រងមួយដែលអាចអនុវត្តបានតាមបែបរដ្ឋបាល។ ឧបមាថាកុំព្យូទ័រមួយគ្រឿងផ្ទុកនូវព័ត៌មានដ៏មានតំលៃ ហើយវាងាយទទួលរងនូវគ្រោះថ្នាក់អគ្គីភ័យ ដូច្នេះការចំលងទិន្នន័យបំរុងទុក (Data Backup) នៅទីកន្លែងដាច់ដោយឡែកមួយ គឺជាវិធានការគ្រប់គ្រងមួយដែលមានលក្ខណៈជាការកាត់បន្ថយហានិភ័យ។ ការទិញប័ណ្ណធានារ៉ាប់រងអគ្គីភ័យ និងការធានាការខូចខាតនៃទិន្នន័យដែលបាត់បង់ គឺជាការគ្រប់គ្រងតាមរយៈការផ្ទេរហានិភ័យ។

ការជៀសវាងហានិភ័យគឺជាជម្រើសមួយទៀតក្នុងការបំបាត់នូវប្រភពនៃហានិភ័យ។ ជាក់ស្តែងការស្រាវជ្រាវពីមុនៗបានប្រមែប្រមូលនូវព័ត៌មានសម្ងាត់ជាច្រើន ដែលមិនទាក់ទងនឹងការងារសំខាន់ៗ ហើយងាយនឹងធ្លាយចេញទៅខាងក្រៅ ដូច្នេះការលុបបំបាត់នូវព័ត៌មានទាំងនេះប្រកបដោយសន្តិសុខ គឺជាវិធានគ្រប់គ្រងមួយក្នុងការចៀសវាងនូវហានិភ័យ។

ការទទួលយកហានិភ័យដោយចេតនា និងតាមភាពជាក់ស្តែង គឺជាជម្រើសចុងក្រោយ។ ឧទាហរណ៍ជាទូទៅយើងត្រូវបង្កើតប្រព័ន្ធការពារសុវត្ថិភាពបណ្តាញកុំព្យូទ័រ (Firewall) ដើម្បីការពារសន្តិសុខបណ្តាញកុំព្យូទ័រខាងក្នុង (LAN) ក្នុងខណៈដែលម៉ាស៊ីនកុំព្យូទ័រមេគេហទំព័រ (Web Server) សំរាប់អ្នកប្រើប្រាស់ខាងក្រៅត្រូវបានបង្កើតឡើងដោយស្ថិតនៅក្រៅ ប្រព័ន្ធការពារសុវត្ថិភាពបណ្តាញកុំព្យូទ័រ(Firewall)។ វាជាករណីដែលអាចទទួលយកបានចំពោះម៉ាស៊ីនកុំព្យូទ័រមេគេហទំព័រ (Web Server) លើបណ្តាញអ៊ីនធឺណិតដែលងាយទទួលរងការវាយលុកពីខាងក្រៅ ទោះបីវាត្រូវការនូវកិច្ចប្រឹងប្រែងមួយចំនួនសំរាប់ការជួសជុលឡើងវិញក្តីនៅពេលដែលមានការវាយលុកកើតឡើង។ ការទទួលយកហានិភ័យគួរត្រូវបានគ្រប់គ្រងដោយប្រុងប្រយ័ត្ន និងតែងតែទាមទារនូវការពិនិត្យឡើងវិញ និងការផ្តល់ការអនុញ្ញាតពីថ្នាក់ដឹកនាំកំពូល។

៦.២. <u>ការគ្រប់គ្រង និងដំណោះស្រាយតាមរយៈសំការៈព័ត៌មាន</u>

ការគ្រប់គ្រង និងដំណោះស្រាយភាគច្រើន គឺជាវិធានការក្នុងការកាត់បន្ថយហានិភ័យទាំងអស់។ ការគ្រប់គ្រង និងដំណោះស្រាយសំខាន់ៗ ត្រូវបានរៀបរាប់តាមលំដាប់នៅក្នុងឯកសារ សំរាប់ពិនិត្យមើលហានិភ័យ និងឯកសារវិធានគំរូស្តីអំពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។ វិធានការក្នុងការគ្រប់គ្រង និងដំណោះស្រាយថ្មីៗគួរត្រូវបានដាក់ឲ្យអនុវត្តដោយស្តាប់ននីមួយៗ និងត្រូវបានរាយការណ៍អោយបានច្បាស់លាស់ ក្នុងកំឡុងពេលទទួលបានការអនុម័តពីការិយា ល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

ឧបសម្ព័ន្ធទី១៖ សេចក្តីណែនាំអំពីការពិនិត្យមើលហានិភ័យ

សេចក្តីណែនាំរបស់ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ
ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យត្រូវបានប្រើប្រាស់នៅក្នុងដំណាក់កាលរៀបចំផែនការ GISMS ។ សូមធ្វើតាមសេចក្តីណែនាំខាងក្រោមជាដំណាក់ៗ៖

ដំណាក់កាលទី ១	ធ្វើការកំណត់អត្តសញ្ញាណរបស់សំភារៈព័ត៌មាន។
ដំណាក់កាលទី ១.១	សូមពិនិត្យមើលសំភារៈព័ត៌មានទាំងនេះដែលបានចុះក្នុងជួរបន្ទាត់ C
	នៃបញ្ជីសំរាប់ពិនិត្យមើលហានិភ័យ។ សំភារៈព័ត៌មានវិទ្យាប្រាំមួយ ប្រភេទដែលត្រូវបានកំណត់ រួមមាន៖ ព័ត៌មានវិទ្យា បុគ្គលិក សេវាកម្ម ឬបរិក្ខារ ក្រដាសឯកសារ ឧបករណ៍ផ្នែករឹង ឬកម្មវិធីកុំព្យូទ័រ និង បណ្តាញម៉ាស៊ីនកុំព្យូទ័រមេ (Server) ។
ដំណាក់កាលទី ១.២	បែងចែកសំភារៈទាំងនេះដោយយោងទៅតាមរចនាសម្ព័ន្ធរបស់ អង្គភាព ។
	លក្ខណៈរបស់សំភារៈពីរប្រភេទ គឺព័ត៌មាន និងបុគ្គលិកត្រូវបានកំណត់ នៅថ្នាក់ ស្តាប័ន យោងទៅតាមលក្ខ័ណទូទៅនៃអភិបាលកិច្ច ។
	លក្ខណៈរបស់សំភារៈដ៏ទៃទៀតដូចជា សេវាកម្ម ឬបរិក្ខារ ក្រដាសឯក សារ ឧបករណ៍ផ្នែករឹង ឬកម្មវិធីកុំព្យូទ័រ និងបណ្តាញកុំព្យូទ័រ ឬម៉ាស៊ីន កុំព្យូទ័រមេ (Server) ត្រូវបានកំណត់នៅថ្នាក់នាយកដ្ឋាននីមួយៗដែល ជាស្តាប័នអាចធ្វើការត្រួតពិនិត្យដោយខ្លួនឯងបាន។
ដំណាក់កាលទី ១.៣	ធ្វើការកែតម្រូវព័ត៌មាននៅក្នុងជួរបន្ទាត់ C និង D ដោយយោងទៅតាម ការបែងចែក ដែលបានអនុវត្តនៅក្នុងដំណាក់ទី១.២។
	លោកអ្នកអាចចំលង (Copy) និងបញ្ចូល (Paste) ប្រភេទសំភារៈ ព័ត៌មាននីមួយៗទៅក្នុងជួរបន្ទាត់នៃនាយកដ្ឋានមួយៗដើម្បីងាយស្រួល ក្នុងការត្រួតពិនិត្យ ដោយសារសំភារៈព័ត៌មាននីមួយៗ មានចំនុចត្រួត ពិនិត្យលើសពីពីរ សំរាប់កំណត់នូវហានិភ័យនានាសូមធ្វើការចំលង (Copy) ដោយប្រុងប្រយ័ត្ន ដើម្បីឲ្យបានគ្រប់ចំនុចដែលមានចុះក្នុងជួរ បន្ទាត់ទាំងអស់។
ដំណាក់កាលទី ២	ធ្វើការវាយតំលៃអំពីសំភារៈ។
ដំណាក់កាលទី ២.១	ធ្វើការវាយតំលៃអំពីការសម្ងាត់ផលប៉ះពាល់ និងលទ្ធភាព (ផ្តល់សេវា

	កម្ម ឬបរិក្ខារ) ដើម្បីបំពេញនូវលក្ខណៈវិនិច្ឆ័យ ដែលបានរៀបរាប់នៅក្នុងបញ្ជីតារាងវាយតំលៃ។
	លោកអ្នកអាចធ្វើការជ្រើសរើសផ្នែកណាមួយពីបញ្ជីជ្រើសរើសនៅក្នុងជួរបន្ទាត់ G H និង I។
	សូមប្រើប្រាស់ពិន្ទុដែលបានកំណត់ស្រាប់ ប្រសិនបើលោកអ្នកគិតថាវាមានការលំបាកក្នុងការវាយតំលៃ។
ដំណាក់កាលទី ២.២	បញ្ជីសំរាប់ពិនិត្យមើលហានិភ័យបង្ហាញដោយស្វ័យប្រវត្តិនៅក្នុងជួរបន្ទាត់ J នូវពិន្ទុសរុបទទួលបានពីការវាយតំលៃនៃសំភារៈនីមួយៗ។
	ធ្វើការពិនិត្យឡើងវិញនូវលទ្ធផលទទួលបាន និងធ្វើការពិនិត្យផ្ទៀងផ្ទាត់ជាមួយនឹងលក្ខណៈវិនិច្ឆ័យដែលបានចុះនៅក្នុងបញ្ជីតារាងវាយតំលៃ។ ធ្វើការកែសម្រួលការវាយតំលៃអំពីការសម្ងាត់ ផលប៉ះពាល់ និងលទ្ធភាព ប្រសិនបើលោកអ្នកគិតថាកំរិតនៃពិន្ទុវាយតំលៃសរុបអំពីសំភារៈព័ត៌មាននីមួយៗ ខុសពីការពិតជាក់ស្តែង។
ដំណាក់កាលទី ៣	ធ្វើការត្រួតពិនិត្យសំភារៈ។
ដំណាក់កាលទី ៣.១	សូមមើលពាក្យក្នុងជួរបន្ទាត់ L និង M ហើយធ្វើការជ្រើសរើសពាក្យបានអនុវត្ត ឬមិនបានអនុវត្តនៅក្នុងជួរបន្ទាត់ N។
ដំណាក់កាលទី ៤	ធ្វើការវាយតំលៃអំពីហានិភ័យ។
ដំណាក់កាលទី ៤.១	ធ្វើការវាយតំលៃអំពីបញ្ហាគំរាមនិងភាពងាយទទួលរងផលប៉ះពាល់ដើម្បីបំពេញនូវលក្ខណៈវិនិច្ឆ័យ ដែលបានរៀបរាប់នៅក្នុងបញ្ជីតារាងវាយតំលៃ។
	លោកអ្នកអាចធ្វើការជ្រើសរើសផ្នែកណាមួយពីបញ្ជីជ្រើសរើសនៅក្នុងជួរបន្ទាត់ P និង R។
	សូមមើលសេចក្តីអធិប្បាយអំពីបញ្ហាគំរាមនីមួយៗនៅក្នុងជួរបន្ទាត់ Q សំរាប់ជាជំនួយក្នុងការសម្រេចលើការវាយតំលៃអំពីបញ្ហាគំរាម។

	សូមប្រើប្រាស់ពិន្ទុដែលបានកំណត់ជូនស្រាប់ ប្រសិនបើលោកអ្នកគិតថាវាមានការលំបាកក្នុងការវាយតំលៃ។
ដំណាក់កាលទី ៤.២	បញ្ជីសំរាប់ពិនិត្យមើលហានិភ័យបង្ហាញដោយស្វ័យប្រវត្តិនូវពិន្ទុវាយតំលៃសរុបនៅក្នុងជួរបន្ទាត់ T ។
	ធ្វើការពិនិត្យឡើងវិញនូវលទ្ធផលទទួលបាន និងធ្វើការពិនិត្យផ្ទៀងផ្ទាត់ជាមួយនឹងលក្ខណៈវិនិច្ឆ័យ ដែលបានចុះនៅក្នុងបញ្ជីតារាងវាយតំលៃ។ ធ្វើការកែសម្រួលការវាយតំលៃអំពីបញ្ហាគំរាមនិងភាពទទួលងនូវផែលប៉ះពាល់ ប្រសិនបើលោកអ្នកគិតថាកំរិតនៃពិន្ទុវាយតំលៃសរុបអំពីហានិភ័យខុសពីការពិតជាក់ស្តែង។
	សូមចូលទៅកាន់ដំណាក់កាលទី៥ ប្រសិនបើពិន្ទុសរុបនៃការវាយតំលៃអំពីហានិភ័យមានកំរិតខ្ពស់។ ប្រសិនបើពិន្ទុសរុបនៃការវាយតំលៃអំពីហានិភ័យមានកំរិតទាប សូមពិចារណាបង្កើតនូវលក្ខណៈរួមសំរាប់ GISMS និងបង្កើតនូវការរៀបចំជាក់លាក់មួយប្រសិនបើចាំបាច់ ឧទាហរណ៍៖ ធ្វើការបញ្ចូលទិន្នន័យបន្ថែម (Update) ទៅក្នុងឯកសារវិធានដែលមានស្រាប់ឬបញ្ចូលទិន្នន័យបន្ថែម (Update) ទៅក្នុងជួរបន្ទាត់ V ស្តីអំពីឯកសារយោង។
ដំណាក់កាលទី ៥	ធ្វើការកំណត់វិធានការក្នុងការគ្រប់គ្រង។
ដំណាក់កាលទី ៥.១	សូមមើលសេចក្តីអធិប្បាយអំពីវិធានការគ្រប់គ្រងដែលមានផ្តល់ជូនស្រាប់នៅក្នុងជួរបន្ទាត់ U។
ដំណាក់កាលទី ៥.២	សូមមើលសេចក្តីអធិប្បាយអំពីឯកសារយោងដែលជាឯកសារច្បាប់គំរូស្តីអំពី សន្តិសុខព័ត៌មាននៅក្នុងជួរបន្ទាត់ V។
ដំណាក់កាលទី ៥.៣	កំណត់នូវលទ្ធភាពក្នុងការអនុវត្តន៍វិធាន និងនីតិវិធីនានានៅក្នុងឯកសារវិធានគំរូស្តីអំពីសន្តិសុខព័ត៌មាន។ ធ្វើការរិះរកនូវលទ្ធភាពដែលជាជម្រើសដ៏ទៃទៀត ប្រសិនបើមិនអាចកំណត់ បាននូវលទ្ធភាពសំរាប់

	អនុវត្តបានទេ។
ដំណាក់កាលទី ៥.៤	ធ្វើការបញ្ចូលទិន្នន័យបន្ថែម (Update) ទៅក្នុងជួរបន្ទាត់ U ស្តីអំពីសេក្តីអធិប្បាយពីវិធានការគ្រប់គ្រង ជួរបន្ទាត់ V ស្តីអំពីឯកសារយោង និងធ្វើការបញ្ចូលទិន្នន័យបន្ថែម (Update) ទាក់ទងនឹងបញ្ញត្តិ និងនីតិវិធីដែលអាចប្រើប្រាស់ និងអនុវត្តបាននៅក្នុងអង្គភាព។
ដំណាក់កាលទី ៦	ធ្វើការវាយតំលៃអំពីហានិភ័យបន្ទាប់ពីបានចាត់វិធានការគ្រប់គ្រងបញ្ហាទាំងនេះ។
ដំណាក់កាលទី ៦.១	ធ្វើការវាយតំលៃអំពីបញ្ហាគំរាមនិងភាពងាយទទួលរងផលប៉ះពាល់ដើម្បីបំពេញនូវលក្ខណៈវិនិច្ឆ័យ ដែលបានរៀបរាប់នៅក្នុងបញ្ជីតារាងវាយតំលៃ។
	លោកអ្នកអាចធ្វើការជ្រើសរើសផ្នែកណាមួយពីបញ្ជីជ្រើសរើសនៅក្នុងជួរបន្ទាត់ W និង Y។
	ប្រើបាស់នូវពិន្ទុដែលបានកំណត់ជូនស្រាប់ ប្រសិនបើលោកអ្នកមិនបានផ្លាស់ប្តូរវិធានការក្នុងការគ្រប់គ្រងវិធាននិងនីតិវិធីនៅក្នុងឯកសារស្តីអំពីសន្តិសុខព័ត៌មាននោះទេ។
ដំណាក់កាលទី ៦.២	បញ្ជីសំរាប់ពិនិត្យមើលហានិភ័យបង្ហាញដោយស្វ័យប្រវត្តិនូវពិន្ទុវាយតំលៃសរុបនៅក្នុងជួរបន្ទាត់ AA។
	ធ្វើការពិនិត្យឡើងវិញនូវលទ្ធផលទទួលបាននិងធ្វើការពិនិត្យផ្ទៀងផ្ទាត់ជាមួយនឹងលក្ខណៈវិនិច្ឆ័យដែលបានចុះនៅក្នុងបញ្ជីតារាងវាយតំលៃ។ ធ្វើការកែសម្រួលការវាយតំលៃអំពីបញ្ហាគំរាម និងភាពងាយទទួលរងនូវផលប៉ះពាល់ប្រសិនបើលោកអ្នកគិតថាកំរិតនៃពិន្ទុវាយតំលៃសរុបអំពីហានិភ័យខុសពីការពិតជាក់ស្តែង។
ដំណាក់កាលទី ៦.៣	ត្រូវប្រាកដថាពិន្ទុសរុបនៃការវាយតំលៃអំពីហានិភ័យនីមួយៗដែលទទួលបានមានកំរិតទាប។ ធ្វើការសម្រេចចិត្តក្នុងការចាត់វិធានការ

	បន្ថែមដើម្បីកាត់បន្ថយនូវហានិភ័យឬធ្វើការរៀបរាប់អំពីលក្ខ័ណដែលអាចទទួលយកនូវហានិភ័យដែលមិនទាន់ជួបប្រទះ។

ផ្នែក ទី៣

ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន

របស់រាជរដ្ឋាភិបាល

អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា
គមនាគមន៍ ព័ត៌មានវិទ្យា

- ពង្រាងដោយលោក យូស៊ូកេ តាណាកា (Yusuke Tanaka) អ្នកជំនាញ
នៃទីភ្នាក់ងារសហប្រតិការអន្តរជាតិនៃប្រទេសជប៉ុន (JICA)

- កែសម្រួល និងរៀបរៀងដោយក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការ
សន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន

១. សេចក្តីផ្តើម

ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (ឯកសារវិធានស្តីពី GIS) ត្រូវបានកំណត់នូវលក្ខខណ្ឌដែល អ.អ.ប.គ.ព ត្រូវអនុវត្តនូវប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ក្រោមគោលនយោបាយស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (ឯកសារណែនាំស្តីអំពី GISMS)។

២. វិធានជាមូលដ្ឋានបីប្រភេទសំរាប់រក្សាសន្តិសុខព័ត៌មាន

[វិធានទី១] ជានិច្চកាលត្រូវធ្វើការពិចារណាឲ្យបានជិតដល់ ក្នុងការទទួលយកដំណើរការ ឬរក្សាទុកនូវព័ត៌មានសម្ងាត់នានាឲ្យបានគ្រប់ពេលវេលា។ ត្រូវចៀសវាងនូវហានិភ័យមួយចំនួន ដែលប៉ះពាល់ដល់ព័ត៌មានទាំងនេះ ដូចជាការធ្វើឲ្យលេចធ្លាយ ការលួចបន្លំ និងលទ្ធភាពដែលមិនអាចប្រើប្រាស់បាន។

[វិធានទី២] ត្រូវចាក់សោច្រកចេញចូលទូឯកសារ និងថតតុនៅការិយាល័យធ្វើការ មុនពេលដែលលោកអ្នកចាកចេញទៅក្រៅ។

[វិធានទី៣] ត្រូវបើកអោយកម្មវិធីកំចាត់មេរោគ ដំណើរការនូវមុខងារចាប់មេរោគដោយស្វ័យប្រវត្តិ ព្រមទាំងធ្វើឲ្យកម្មវិធីនេះមានភាពទាន់សម័យយ៉ាងតិច១ដងក្នុងមួយសប្តាហ៍។ ត្រូវរុករកមេរោគ (Scan) ឧបករណ៍ផ្ទុកទិន្នន័យក្នុងកុំព្យូទ័ររបស់លោកអ្នកជារៀងរាល់សប្តាហ៍ រួមជាមួយនឹងឧបករណ៍ផ្ទុកទិន្នន័យដ៏ទៃទៀត ដែលភ្ជាប់ពីខាងក្រៅកុំព្យូទ័រ (DVD/ CD/ FD/ Memory-Stick/ HDD) រាល់ពេលតភ្ជាប់ទៅកាន់កុំព្យូទ័ររបស់លោកអ្នក។

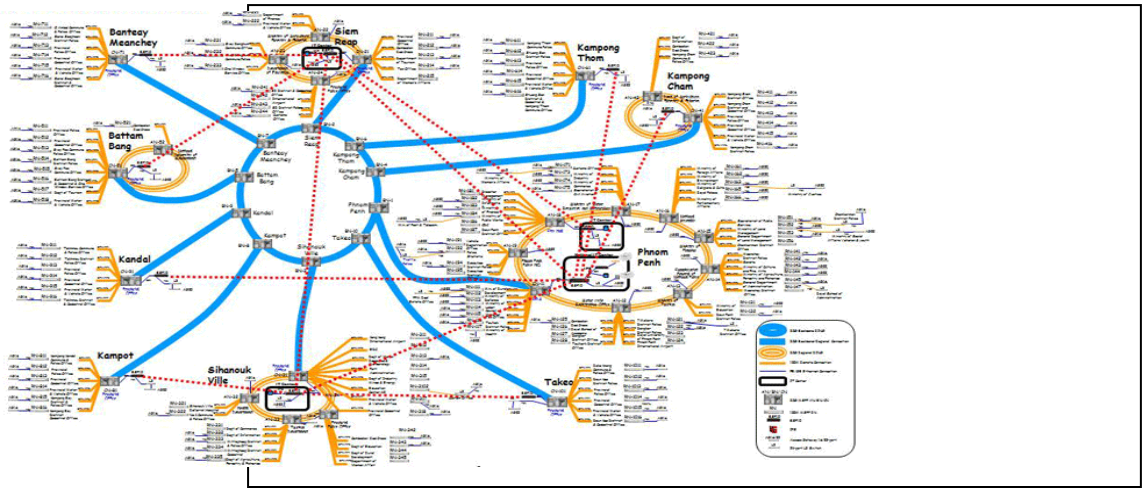
៣. វិសាលភាព

វិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ដែលមាននៅក្នុងឯកសារនេះ សំរាប់អនុវត្តនៅក្នុង អាជ្ញាធរជាតិទទួលបន្ទុកកិច្চការអភិវឌ្ឍន៍បច្চេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា ដែលក្នុង

នោះមានផ្នែកក្រោមចំណុះផ្សេងៗដូចជា *ផ្នែករដ្ឋបាលទូទៅ ផ្នែកហេដ្ឋារចនាសម្ព័ន្ធ ផ្នែកបណ្តាញ ផ្នែកសហគ្រាស ផ្នែកមាតិកា និងកម្មវិធី (Applications) ផ្នែកអភិវឌ្ឍន៍សមត្ថភាពធនធានមនុស្ស និង កូដចំហរ (FOSS) ផ្នែកគោលនយោបាយ* ព្រមទាំងផ្នែកផ្សេងៗទៀតដូចជា *ក្រុមការងារជាតិកម្ពុជាទប់ទល់បញ្ហាបន្ទាន់នៃកុំព្យូទ័រ (CamCERT) កម្មវិធីបណ្តុះបណ្តាល CISCO និងក្រុមការងារគ្រប់គ្រងកន្សោមអាទិភាព។*

ជារួម ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល សំរាប់អនុវត្តនៅលើកុំព្យូទ័រដែលមាននៅក្នុងប្រព័ន្ធបណ្តាញ (Network System) ប៉ុណ្ណោះ។ នាពេលអនាគត វិសាលភាពរបស់ឯកសារនេះនឹងត្រូវបានពង្រីក ដើម្បីរួមបញ្ចូលម៉ាស៊ីនកុំព្យូទ័រមេ (Servers) និងប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យា ខេត្ត ក្រុង។

អ.អ.ប.ត.ព បានយកចិត្តទុកដាក់លើការអភិវឌ្ឍន៍ វិស័យបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន ដោយបានអនុវត្តលើគំរោងប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យា ខេត្ត ក្រុង ដោយធ្វើការតភ្ជាប់ ជាលក្ខណៈបណ្តាញទៅតាមបណ្តាខេត្ត ក្រុង ទាំងអស់។



៤. ឯកសារយោង ពាក្យបច្ចេកទេស និង និយមន័យ

៤.១. ឯកសារយោង

ឯកសារយោងខាងក្រោម មានសារៈសំខាន់យ៉ាងខ្លាំងសំរាប់ការចងក្រងឯកសារនេះ៖

១) ISO/ISE 27001: 2005 បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន – វិធីសាស្ត្រការពារសន្តិសុខ – ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន – តម្រូវការ

២) ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល(GISMS)

៤.២. ពាក្យបច្ចេកទេស និង និយមន័យ

កុំព្យូទ័រ (Client PC)៖

វាជាប្រភេទកុំព្យូទ័រ សំរាប់ប្រើប្រាស់ក្នុងការិយាល័យដូចជា កុំព្យូទ័រលើតុ កុំព្យូទ័រយួរដៃ ឬ កុំព្យូទ័រចល័ត។

ពាក្យដ៏ទៃទៀតត្រូវបានយោងទៅតាមពាក្យ និង និយមន័យ នៅក្នុងឯកសារណែនាំស្តីអំពី GISMS ឬ ISO/ISE 27001។

៥. អង្គភាពការពារសន្តិសុខព័ត៌មាន

៥.១. និយមន័យរបស់អង្គភាពការពារសន្តិសុខព័ត៌មាន

អ.អ.ប.គ.ព បានកំណត់តួនាទី និងការទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន ដោយបង្កើតផ្នែកមួយចំនួនដូចខាងក្រោម៖

ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន (ISO)៖

ការិយាល័យនេះ ត្រូវបានបង្កើតឡើងនៅ អ.អ.ប.គ.ព មានតួនាទីអភិវឌ្ឍន៍ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន។ សមាជិករបស់ការិយាល័យនេះរួមមាន នាយកផ្នែកសន្តិសុខព័ត៌មាន (CISO) ប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន ដែលត្រូវបានផ្តល់និយមន័យដូចខាងក្រោម៖

នាយកផ្នែកសន្តិសុខព័ត៌មាន (CISO)៖

មន្ត្រីមួយរូបនៅក្នុងក្រសួង ត្រូវបានចាត់តាំងឲ្យទទួលមុខដំណែងនេះ។ មន្ត្រីរូបនេះក៏ជា

សមាជិកម្នាក់ នៃការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GISO) ផងដែរ ដែលត្រូវបានកំណត់នៅក្នុងប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

ប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន (IS Manager)៖

មន្ត្រីមួយរូបនៅក្នុងនាយកដ្ឋាន ត្រូវបានចាត់តាំងឲ្យទទួលមុខដំណែងនេះ។ ការទទួលខុសត្រូវ ផ្សេងៗ ត្រូវបានកំណត់នៅក្នុងឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល និងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល។

មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន (មន្ត្រីទទួលខុសត្រូវផ្នែក IS)៖

មន្ត្រីមួយរូបនៅក្នុងនាយកដ្ឋានត្រូវបានចាត់តាំងឲ្យទទួលមុខដំណែងនេះ។ ការទទួលខុសត្រូវផ្សេងៗ ត្រូវបានកំណត់នៅក្នុងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

មន្ត្រីធម្មតា៖

សំដៅទៅលើនិយោជិតដ៏ទៃទៀតទាំងអស់ ដែលបិតនៅក្នុងក្របខ័ណ្ឌនៃអង្គភាព។

៥.២. បញ្ជីសមាជិកការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន

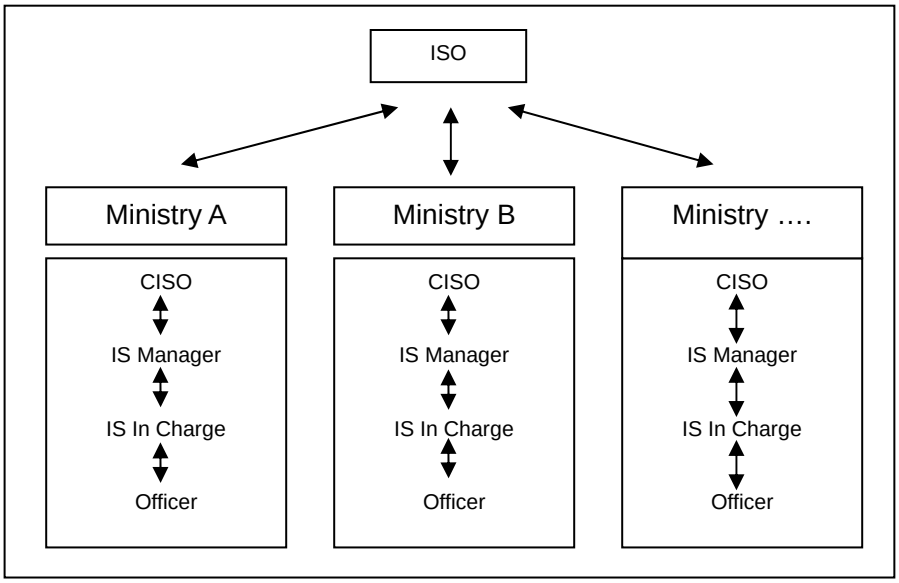
សមាសភាពមន្ត្រីការិយាល័យសុវត្ថិភាពព័ត៌មាន និងត្រូវតែងតាំងដោយអគ្គលេខាធិការ នៃអគ្គលេខាធិការដ្ឋាន អាជ្ញាធរជាតិ អ.អ.ប.គ.ព។

៥.៣. បណ្តាញទំនាក់ទំនងសំរាប់គ្រាអាសន្ន

បែបបទនៃការរាយការណ៍ ជាទូទៅត្រូវបានអនុវត្តតាមឋានានុក្រម គឺពីមន្ត្រីធម្មតា ទៅមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន ពីមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន ទៅប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងពីប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន ទៅការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ឬនាយកផ្នែកសន្តិសុខព័ត៌មាន។ ផ្ទុយទៅវិញ បែបបទនៃការផ្តល់ការណែនាំ គឺអនុវត្តពីការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ឬនាយកផ្នែកសន្តិសុខព័ត៌មាន ទៅប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន ពី

ប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន ទៅមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន និងពីមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មានទៅមន្ត្រីធម្មតា។

រចនាសម្ព័ន្ធការិយាល័យគ្រប់គ្រងសុវត្ថិភាពព័ត៌មាន៖



៦. វិធាន និង នីតិវិធី

៦.១. <u>វិធាន និង នីតិវិធីលើផ្នែកព័ត៌មាន</u>

(ក) វិធាន

(ក១) ព័ត៌មានដែលត្រូវបានប្រើប្រាស់នៅក្នុងប្រតិបត្តិការការងាររបស់រាជរដ្ឋាភិបាល ត្រូវបានចែកចេញជាបីប្រភេទ រួមមាន៖

១. ព័ត៌មានសាធារណៈ៖

ជាព័ត៌មានដែលបើកចំហសំរាប់សាធារណជន។

២. ព័ត៌មានផ្ទៃក្នុង៖

ជាព័ត៌មានដែលត្រូវបានប្រើប្រាស់ សំរាប់តែក្នុងប្រតិបត្តិការការងាររបស់

រាជរដ្ឋាភិបាលប៉ុណ្ណោះ។

៣. ព័ត៌មានសម្ងាត់៖

ជាព័ត៌មាន ដែលមានតែបុគ្គលមួយចំនួនប៉ុណ្ណោះអាចដឹងបាន ។

(ក២) នៅពេលទទួលបាននូវព័ត៌មាន លោកអ្នកត្រូវចាត់ព័ត៌មានទាំងនេះ ចូលក្នុងប្រភេទណាមួយខាងលើ ហើយវាជាការប្រសើរបំផុតដែលប្រភេទព័ត៌មាននីមួយៗ ត្រូវបានគូសសំគាល់ ឬដាក់ជាសញ្ញាចំណាំ។

(ក៣) ជានិច្ចកាល ត្រូវគ្រប់គ្រងព័ត៌មានដោយប្រុងប្រយ័ត្នយោងទៅតាមចំណាត់ថ្នាក់នីមួយៗ ។

(ក៤) ជានិច្ចកាល ត្រូវចាត់ព័ត៌មានឯកជនចូលក្នុងប្រភេទព័ត៌មានសម្ងាត់។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.២. <u>វិធាន និង នីតិវិធី លើនិយោជិត</u> (នឹងត្រូវកំណត់នាពេលអនាគត)

(ក) ន័យធន

(ផ្នែកនេះ នឹងធ្វើការកំណត់នូវតម្រូវការសន្តិសុខ ទាក់ទងនឹងការជ្រើសរើសនិយោជិត ដូចជាការពិនិត្យមើលអំពីគុណសម្បត្តិរបស់បេក្ខជន កំឡុងពេលជ្រើសរើសបុគ្គលិកថ្មី ការពិពណ៌នាអំពីការងារទាក់ទងនឹងបញ្ហាសន្តិសុខព័ត៌មាន និងតម្រូវការផ្សេងៗ នៅពេលបញ្ចប់ការជួលឲ្យបំរើការងារ)។

៦.៣. <u>វិធាន និង នីតិវិធី សន្តិសុខបរិក្ខារ</u>

៦.៣.១. <u>អគារ និងបន្ទប់ការិយាល័យ</u>

(ក) ន័យធន

(ក១) ត្រូវកំណត់នូវបុគ្គល ដែលមានសិទ្ធិចេញចូលអគារ ឬបន្ទប់។

(ក២) ត្រូវអនុវត្តនូវប្រព័ន្ធសម្ងាត់សមរម្យមួយ សំរាប់ការចេញចូលអគារ ឬបន្ទប់។

(ក៣) ត្រូវបែងចែកឲ្យដាច់រវាងការិយាល័យធ្វើការ និងទីកន្លែងដ៏ទៃទៀត ដែលសំរាប់ប្រើប្រាស់រួម។

(ក៤) ត្រូវចាត់បុគ្គលិកដែលមានការយល់ដឹងការងារផ្ទៃក្នុង ឲ្យអមភ្ញៀវដែលមកពីខាងក្រៅ។

ចំនុចព្យួរទុកបណ្តោះអាសន្ន

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៣.២. <u>ទូតម្កល់ឯកសារ និងតុធ្វើការ</u>

(ក) ខិចខាន

(ក១) ត្រូវរក្សាទុកសំការៈព័ត៌មាន ដោយសម្ងាត់ក្នុងទូតម្កល់ឯកសារ ដែលបានចាក់សោត្រឹមត្រូវ។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៣.៣. <u>ម៉ាស៊ីនទូរសារ និងម៉ាស៊ីនបោះពុម្ព</u>

(ក) ខិចខាន

(ក១) ត្រូវបោះចោលដោយប្រុងប្រយ័ត្ន នូវឯកសារដែលបានបោះពុម្ព និងបញ្ជូនតាមទូរសារនានា។

(ក២) ត្រូវរក្សាទុកបញ្ជីព័ត៌មានស្តីអំពីការបញ្ជូនទូរសារ(ទៅ ឬមក)។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៤. <u>សន្តិសុខព័ត៌មានរូបវន្ត</u>

៦.៤.១. <u>ក្រដាសឯកសារ</u>

(ក) និយាន

(ក១) ជានិច្ចកាល ត្រូវធ្វើការកំណត់អំពីព័ត៌មានសម្ងាត់ដោយប្រុងប្រយ័ត្ន នៅក្នុងក្រដាស ឬឯកសារនីមួយៗ។

(ក២) ត្រូវរក្សាទុកក្រដាស ឬឯកសារសម្ងាត់ទាំងនេះនៅកន្លែងសន្តិសុខមួយ ដើម្បីជៀសវាងនូវការលួចប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត។

(ក៣) មន្ត្រីពាក់ព័ន្ធ ត្រូវដុតចោលដោយខ្លួនឯង នូវឯកសារដែលលែងប្រើប្រាស់ ឬប្រើប្រាស់នូវម៉ាស៊ីនច្រៀក ដើម្បីកាត់ក្រដាសឯកសារដែលមានផ្ទុកព័ត៌មានសម្ងាត់ទាំងនេះជាចម្រៀកតូចៗ។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៤.២. <u>ឧបករណ៍ផ្ទុកឯកសារ (Digital Archives) (DVD/CD/FD/Tape)</u>

(ក) វិធាន

(ក១) ជានិច្ចកាល ត្រូវធ្វើការកំណត់អំពីព័ត៌មានសម្ងាត់ ដោយប្រុងប្រយ័ត្ននៅក្នុងឧបករណ៍ផ្ទុកឯកសារនីមួយៗ។

(ក២) ត្រូវរក្សាទុកឧបករណ៍ផ្ទុកឯកសារសម្ងាត់ទាំងនេះ នៅកន្លែងសន្តិសុខមួយ ដើម្បីជៀសវាងនូវការលួចប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត។

(ក៣)បំផ្លាញចោលនូវឧបករណ៍ផ្ទុកឯកសារ ដែលលែងប្រើប្រាស់(DVD/CD/FD/Tape)។

(ខ) នីតិវិធី

(មិននីតិវិធីណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៥. <u>វិធាន និង នីតិវិធី សន្តិសុខកុំព្យូទ័រ</u>

៦.៥.១. <u>កុំព្យូទ័រលើតុ</u>

(ក) ទិដ្ឋាន

ទិដ្ឋភាពទូទៅ

(ក១) ការការពារសន្តិសុខជារូបវន្តនៃកុំព្យូទ័ររបស់លោកអ្នក គឺជាការទទួលខុសត្រូវផ្ទាល់ខ្លួនរបស់លោកអ្នក។ ដូចនេះសូមមានការប្រុងប្រយ័ត្នខ្ពស់ក្នុងការថែរក្សាកុំព្យូទ័ររបស់លោកអ្នក។ ម្យ៉ាងវិញទៀត លោកអ្នកក៏ត្រូវមានសុកនិនិច្ឆ័យ និងប្រុងប្រៀបជានិច្ចដើម្បីទប់ទល់នឹងហានិភ័យនានាផងដែរ។

(ក២) រាល់កុំព្យូទ័រនីមួយៗត្រូវស្ថិតក្រោមការទទួលខុសត្រូវរបស់មន្ត្រីម្នាក់ៗជាក់លាក់ ទោះបីជាកុំព្យូទ័រទាំងនេះត្រូវបានប្រើប្រាស់ដោយមន្ត្រីច្រើនគ្នាក៏ដោយ។

(ក៣) លោកអ្នកត្រូវទទួលខុសត្រូវដោយផ្ទាល់ ចំពោះការប្រើប្រាស់កុំព្យូទ័រ លើបណ្តាញតាមរយៈអត្តសញ្ញាណ (User ID) ផ្ទាល់ខ្លួន។ ដូច្នេះ សូមថែរក្សាលេខ ឬពាក្យសម្ងាត់ (Password) របស់លោកអ្នកដោយប្រុងប្រយ័ត្ន និងសម្ងាត់បំផុត។ លេខ ឬពាក្យសម្ងាត់ (Password) នេះត្រូវតែមានលក្ខណៈស្មុគស្មាញ ដែលមិនងាយនឹងលួចប្រើប្រាស់បានហើយ វាត្រូវតែផ្លាស់ប្តូរជាទៀងទាត់។ លោកអ្នកមិនត្រូវចែករំលែកការប្រើប្រាស់ លេខ ឬពាក្យសម្ងាត់នេះជាមួយអ្នកដ៏ទៃឡើយ ទោះបីជាសមាជិកគ្រួសារ មិត្តភក្តិ ឬអ្នកបច្ចេកទេសដែលធ្វើការជាមួយលោកអ្នកក៏ដោយ។

(ក៤) ត្រូវជៀសវាងទុកនិងបើកកុំព្យូទ័រចោលដោយមិនបានប្រើប្រាស់។ ជានិច្ចកាល មុនពេលលោកអ្នកចាកចេញពីកុំព្យូទ័រ ត្រូវបិទ ឬឡក់ឌីស (Logoff) ឬដាក់លេខ ឬពាក្យសម្ងាត់ នៅលើស្ក្រីនសេវើ (Screensaver) នៃកុំព្យូទ័ររបស់លោកអ្នក។

បង្ការការឆ្លងមេរោគ

(ក៥) ការឆ្លងមេរោគក្នុងកុំព្យូទ័រ គឺជាបញ្ហាដ៏ចំបងមួយ សំរាប់ អ.អ.ប.ត.ព ក្នុងការដោះស្រាយ ដោយសារកុំព្យូទ័រនានា ងាយនឹងទទួលរងការឆ្លងមេរោគ ប្រសិនបើកម្មវិធីប្រឆាំងមេរោគរបស់កុំព្យូទ័រទាំងនោះ មិនត្រូវបានធ្វើអោយទាន់សម័យ (Update Definition) យ៉ាងតិចចំនួនមួយដងក្នុងមួយសប្តាហ៍។ វិធីសាស្ត្រ ដែលងាយស្រួលបំផុតសំរាប់អនុវត្តការងារនេះ គឺត្រូវបើកអោយកម្មវិធីកំចាត់មេរោគដំណើរការនូវមុខងារធ្វើអោយទាន់សម័យដោយស្វ័យប្រវត្តិ ដោយតភ្ជាប់កុំព្យូទ័ររបស់លោកអ្នកទៅនឹង បណ្តាញអ៊ីនធឺណិត។ ប្រសិនបើលោកអ្នកមិនអាចធ្វើបែបនេះបាន ដោយសារប្រការណាមួយ សូមទំនាក់ទំនងទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដើម្បីទទួលបាននូវសេចក្តីណែនាំ ពីនីតិវិធីក្នុងការដំឡើងកម្មវិធីកំចាត់មេរោគកុំព្យូទ័រ។

(ក៦) ជានិច្ចកាល ត្រូវរុករក (Scan) មេរោគ នូវរាល់ឯកសារទាំងឡាយដែលបានទាញយក (Download) មកទុកក្នុងកុំព្យូទ័ររបស់លោកអ្នកពីប្រភពផ្សេងៗ ដូចជា (CD/DVD /USB/Hard Disk/Memory Stick) ឯកសារបញ្ជូនតាមបណ្តាញកុំព្យូទ័រ ឯកសារជូនភ្ជាប់ក្នុងសារអេឡិចត្រូនិច (E-mail Attachments) ឬឯកសារពីបណ្តាញអ៊ីនធឺណិត)។ ដើម្បីអោយងាយស្រួល ត្រូវបើកអោយកម្មវិធីកំចាត់មេរោគដំណើរការនូវមុខងារចាប់មេរោគដោយស្វ័យប្រវត្តិ និងចាំបាច់កំណត់កាលវិភាគ សំរាប់ការរុករកមេរោគ ដោយត្រូវអនុវត្តយ៉ាងតិចមួយដងជារៀងរាល់សប្តាហ៍។

(ក៧) ត្រូវរាយការណ៍ជាបន្ទាន់ ទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន អំពីហេតុការណ៍ទាក់ទងទៅនិងសន្តិសុខព័ត៌មាន ដូចជាហេតុការនៃការឆ្លងមេរោគចូលក្នុងប្រព័ន្ធកុំព្យូទ័រដើម្បីកាត់បន្ថយនូវការខាតបង់នានា។

(ក៨) ត្រូវឆ្លើយតបជាបន្ទាន់ ទៅនឹងសារព្រមានអំពីលទ្ធភាពឆ្លងមេរោគនានា ក្នុងកុំព្យូទ័ររបស់លោកអ្នក។ ប្រសិនបើមានការសង្ស័យ អំពីមេរោគណាមួយ ឧទាហរណ៍ឯកសារដែលមានលក្ខណៈមិនប្រក្រតី សូមទាក់ទងទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន មិនត្រូវបញ្ជូនបន្ត (Forward) នូវឯកសារណាមួយ ឬបញ្ចូល (Upload) ទិន្នន័យទៅលើបណ្តាញកុំព្យូទ័រទេ ប្រសិនបើសង្ស័យថាកុំព្យូទ័ររបស់លោកអ្នកបានឆ្លងមេរោគ។

(ក៩) ត្រូវមានការប្រុងប្រយ័ត្នជាពិសេសក្នុងការរុករកមេរោគ នៅក្នុងប្រព័ន្ធកុំព្យូទ័ររបស់លោកអ្នក មុនពេលផ្ញើចេញនូវឯកសារណាមួយ។ ឯកសារទាំងនេះរួមមាន ឯកសារជូនភ្ជាប់ក្នុងសារអេឡិចត្រូនិច (E-mail Attachments) និងឯកសារដែលបានពីCD/DVD។

(ក១០) រាល់កុំព្យូទ័រលើតុទាំងអស់ ត្រូវតភ្ជាប់ទៅកាន់ឧបករណ៍រក្សាចរន្តអគ្គីសនី (UPS) ដើម្បីចៀសវាងការបាត់បង់ទិន្នន័យ។

ការសម្អាតទិន្នន័យ

(ក១១) ត្រូវលុបសម្អាតទិន្នន័យរូបវន្ត (Physical Formatting) ក្នុងឧបករណ៍ផ្ទុកទិន្នន័យនៃកុំព្យូទ័រដោយមិនបន្សល់ទុកនូវទិន្នន័យ ឬព័ត៌មានដែលអាចទាញយកមកវិញបាន។

(ខ) នីតិវិធី(សំរាប់មន្ត្រីគ្រប់រូប)

បង្ការការឆ្លងមេរោគ

(ខ១) ដើម្បីអនុវត្តតាមនីតិវិធីខាងក្រោមនេះបាន លោកអ្នកត្រូវប្រាកដថា រាល់កម្មវិធីកំចាត់មេរោគ នៅក្នុងកំព្យូទ័រទាំងអស់ត្រូវធ្វើអោយទាន់សម័យតាមចំនួនដងជាក់លាក់។

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	ណែនាំឲ្យមានការផ្តល់ជូននូវបញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.២	អនុវត្តការរុករកមេរោគ	អ្នកប្រើប្រាស់	មិនមាន
ខ១.៣	ធ្វើការបោះពុម្ព និងដាក់ជូននូវបញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ	អ្នកប្រើប្រាស់	បញ្ជីព័ត៌មានស្តីអំពីការរុករកមេរោគ (Scan) របស់កម្មវិធីប្រឆាំងមេរោគ
ខ១.៤	តម្កល់ទុកបញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ និងរក្សាទុកសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.៥	ពិនិត្យតាមដានមន្ត្រីដែលមិនបានរុករកមេរោគ និងដាក់ជូននូវបញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

ចំណាត់ការក្នុងការចាប់មេរោគ

(ខ២) នីតិវិធីខាងក្រោម ត្រូវបានបង្កើតឡើងដើម្បីចាត់វិធានការណ៍ ចាប់មេរោគផ្សេងៗ។

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ២.១	អនុវត្តនូវសកម្មភាពការពារសន្តិសុខព័ត៌មាន ដូចជា	អ្នកប្រើប្រាស់	មិនមាន

	សកម្មភាពចាប់មេរោគជាដើម		
ខ២.២	ត្រូវផ្តាច់ប្រព័ន្ធកុំព្យូទ័រ ជាបន្ទាន់ពីបណ្តាញកុំព្យូទ័រ	អ្នកប្រើប្រាស់	មិនមាន
ខ២.៣	ជូនដំណឹងទៅការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានជាបន្ទាន់ នៅពេលដែលចាប់បានមេរោគ	អ្នកប្រើប្រាស់	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន
ខ២.៤	ធ្វើការវិភាគអំពីផលវិបាកនៃហេតុការណ៍នីមួយៗ និងចាត់វិធានការសមរម្យដើម្បីដោះស្រាយ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.៥	ប្រសិនបើមានការចាំបាច់ ត្រូវបញ្ឈប់ប្រព័ន្ធដំណើរការបណ្តាញកុំព្យូទ័រ (Network Application)	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.៦	ប្រសិនបើមានការចាំបាច់ ត្រូវអនុវត្តជាបន្ទាន់នូវវិធីសាស្ត្របង្ការការឆ្លងមេរោគ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.៧	សរសេរចូលក្នុងរបាយការណ៍អំពីការវិភាគ និងវិធានការនីមួយៗ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន(ដែលបានបញ្ចូលព័ត៌មានថ្មី)
ខ២.៨	តម្កល់ទុករបាយការណ៍ទាំងនេះ និងរក្សាទុកសំរាប់ រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

៦.៥.២. <u>កុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័ត</u>

(ក) និយាន

និដ្ឋតាពទូទៅ

វិធានមួយចំនួនខាងក្រោម ត្រូវបានប្រើប្រាស់សំរាប់តែកុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តប៉ុណ្ណោះ។ បញ្ហាទាក់ទងនឹងកុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តនេះ ក៏ត្រូវតែអនុវត្តតាមវិធាន និងនីតិវិធី ដែលបានកំណត់នៅក្នុងចំនុចទី **៦.៥.១. កុំព្យូទ័រលើតុ** ផងដែរ។

(ក១) គ្រប់ពេលបើអាចធ្វើទៅបាន ត្រូវរក្សាទុកកុំព្យូទ័រយួរដៃរបស់លោកអ្នក នៅជាប់នឹងខ្លួនជានិច្ច ប្រៀបដូចនឹងកាបូបដាក់ហោប៉ៅ កាបូបយួរដៃ ឬទូរស័ព្ទចល័តរបស់លោកអ្នក។ ជាពិសេស ត្រូវរក្សាទុកវាដោយប្រុងប្រយ័ត្នបំផុត នៅទីសាធារណៈ ដូចជា អាហារដ្ឋានជាដើម (សូមបញ្ជាក់ថា វាប្រើរយៈពេលដ៏ខ្លីបំផុត សំរាប់អ្នកដែលមានបំណងលួចទិន្នន័យនៅក្នុងកុំព្យូទ័រយួរដៃ ដែលម្ចាស់របស់វាមិនបានប្រុងប្រយ័ត្ន)។

(ក២) ប្រសិនបើលោកអ្នកមានការចាំបាច់ ត្រូវទុកកុំព្យូទ័រចោលបណ្តោះអាសន្ន នៅក្នុងការិយាល័យ បន្ទប់ប្រជុំ ឬបន្ទប់សណ្ឋាគារ សូមប្រើប្រាស់ខ្សែសន្តិសុខរបស់កុំព្យូទ័រយួរដៃ ឬឧបករណ៍ស្រដៀងគ្នានេះ ដើម្បីចងភ្ជាប់កុំព្យូទ័រទៅនឹងតុ ឬគ្រឿងសង្ហារឹមដែលធ្ងន់ៗ ទោះបីក្នុងរយៈពេលមួយខ្លីក៏ដោយ។ ការការពារបែបនេះមិនសូវជាមានសន្តិសុខ ប៉ុន្តែវាអាចបង្ការនូវការបាត់បង់កុំព្យូទ័រដោយថាហេតុ។

(ក៣) នៅពេលដែលលោកអ្នកលែងត្រូវការប្រើប្រាស់កុំព្យូទ័រ សូមរក្សាទុកកុំព្យូទ័រ ក្នុងទីកន្លែងដែលមានសុវត្ថិភាពខ្ពស់ ដែលអាចប្រព្រឹត្តទៅបាននៅ គេហដ្ឋាន ការិយាល័យឬសណ្ឋាគារ។ មិនត្រូវទុកចោលកុំព្យូទ័រយួរដៃរបស់លោកអ្នកនៅក្នុងយានយន្ត ដែលបុគ្គលដ៏ទៃអាចមើលឃើញដោយងាយឡើយ។ ប៉ុន្តែប្រសិនបើមានការចាំបាច់បំផុតដែលត្រូវធ្វើបែបនេះ សូមចាក់សោវាទុកនៅក្នុងផ្នែកខាងក្រោយនៃរថយន្ត ឬប្រអប់ដាក់សម្ភារៈក្បែរអ្នកបើកបរ វាមានសន្តិសុខច្រើនជាងប្រសិនបើលោកអ្នកយកវាទៅតាមខ្លួន។

(ក៤) យកទៅតាមខ្លួននូវកុំព្យូទ័រយួរដៃរបស់លោកអ្នក ដែលបានទុកដាក់យ៉ាងត្រឹមត្រូវនៅក្នុងកាបូបដែលមានទ្រនាប់អាចការពារការប៉ះទង្គិចជាយថាហេតុ ឬកាបូបកុំព្យូទ័រដែលមានលក្ខណៈមាំទាំ ដើម្បីចៀសវាងនូវការខូចខាតដល់កុំព្យូទ័រ។ មិនត្រូវទំលាក់ ឬធ្វើអោយប៉ះទង្គិចកុំព្យូទ័ររបស់លោកអ្នកជាមួយនឹងវត្ថុរឹងឡើយ។ ការវេចខ្ចប់កុំព្យូទ័រយួរដៃរបស់លោកអ្នកជាមួយនឹងបន្ទះផ្លាស្ទិក (ដែលបង្កើតដោយថង់ខ្យល់តូចៗជាច្រើនសំរាប់ជាទ្រនាប់) អាចការពារការប៉ះទង្គិចបាន។ កាបូបដាក់កុំព្យូទ័រដែលមានរូបរាងសាមញ្ញទំនងជាមានភាពទាក់ទាញចោរលួច តិចជាងកាបូបដែលមានភាពលេចធ្លោ។

(ក៥) កុំព្យូទ័រយួរដៃរបស់រដ្ឋ ត្រូវបានប្រគល់ជូននិយោជិត ដែលមានសិទ្ធិត្រឹមត្រូវ សំរាប់ប្រើប្រាស់ក្នុងលក្ខណៈផ្លូវការ។ មិនត្រូវឲ្យកុំព្យូទ័រយួរដៃរបស់លោកអ្នកទៅអ្នកដ៏ទៃ ដូចជាក្រុមគ្រួសារ ឬមិត្តភក្តិ ឬប្រើប្រាស់ឡើយ។

(ក៦) ត្រូវកត់ត្រាទុកនូវព័ត៌មានទាក់ទងនឹងម៉ាក ម៉ូដែល លេខស៊េរី (Serial Number) និងស្លាកសម្គាល់ម្ចាស់កម្មសិទ្ធិ (ឧទាហរណ៍ អ.អ.ប.គ.ព) នៃកុំព្យូទ័រយួរដៃរបស់ លោកអ្នក ប៉ុន្តែមិនត្រូវរក្សាទុកព័ត៌មាននេះក្នុង ឬជាប់នឹងកុំព្យូទ័ររបស់លោកអ្នកឡើយ។ ប្រសិនបើវាបាត់បង់ ឬត្រូវបានលួច ត្រូវប្តឹងទៅមន្ត្រីនគរបាលជាបន្ទាន់ ហើយត្រូវជូនដំណឹងទៅការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានវិទ្យាភ្លាមៗ តាមលទ្ធភាពដែលអាចធ្វើបាន (សូមអនុវត្តបែបនេះ បន្ទាប់ពី១ ឬ២ម៉ោងក្រោយមក មិនមែន១ ឬ២ថ្ងៃក្រោយមកទេ)។

ការគ្រប់គ្រងការប្រើប្រាស់កុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តដោយពុំមាន ការអនុញ្ញាត

(ក៧) វាជាការប្រសើរបំផុត ដែលរាល់កុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តទាំងអស់ ប្រើប្រាស់នូវកម្មវិធីសំរាប់ផ្លាស់ប្តូរទំរង់ដើមរបស់ព័ត៌មាន (Encryption) ដែលមានការទទួលស្គាល់ត្រឹមត្រូវ។ ក្នុងករណីនេះត្រូវជ្រើសប្រើប្រាស់នូវឃ្លា ឬលេខ ឬពាក្យសម្ងាត់ដែលវែង និង

មិនងាយលួចប្រើប្រាស់បាន ហើយត្រូវរក្សាទុកវាឲ្យមានសន្តិសុខ។ ត្រូវទំនាក់ទំនងទៅកាន់ ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដើម្បីទទួលបានព័ត៌មានបន្ថែមអំពី ការផ្លាស់ប្តូរ ទំរង់ដើមរបស់ព័ត៌មាន (Encryption) របស់កុំព្យូទ័រយួរដៃ។ ប្រសិនបើកុំព្យូទ័រយួរដៃ ឬ កុំព្យូទ័រចល័តណាមួយបានបាត់ ឬត្រូវបានលួច ការផ្លាស់ប្តូរទំរង់ដើមរបស់ព័ត៌មាន (Encryption) ផ្តល់ការការពារយ៉ាងមានប្រសិទ្ធិភាពជាទីបំផុត ទប់ទល់ទៅនឹងការលួចចូលក្នុងកុំព្យូទ័រដើម្បីប្រើប្រាស់ទិន្នន័យ។

(ក៨) មិនត្រូវរក្សាទុកព័ត៌មានសម្ងាត់នៅក្នុងកុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តរបស់លោកអ្នក ជំនួសការផ្លាស់ប្តូរទំរង់ដើមរបស់ព័ត៌មាន (Encryption) ដូចបានរៀបរាប់នៅក្នុងប្រយោគខាងលើឡើយ។

(ខ) នីតិវិធី (សំរាប់មន្ត្រីគ្រប់រូប)

វិធានការគ្រប់គ្រងសម្ភារៈដែលបានបាត់បង់ ឬត្រូវបានលួច

(ខ១) ប្រសិនបើកុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តណាមួយបានបាត់ ឬត្រូវបានលួច សូមធ្វើតាមបែបបទដូចខាងក្រោម ៖

ជំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	ពិនិត្យមើលហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន ដូចជា ការបាត់បង់ ឬការលួចទ្រព្យសម្បត្តិ	អ្នកប្រើប្រាស់	មិនមាន
ខ១.២	ដាក់បណ្តឹងទៅមន្ត្រីនគរបាល	អ្នកប្រើប្រាស់	មិនមាន
ខ១.៣	ក្នុងរយៈពេលមួយម៉ោងបន្ទាប់ពីកើតហេតុ ត្រូវផ្តល់ព័ត៌មានទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	អ្នកប្រើប្រាស់	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន

ខ១.៤	ធ្វើការវិភាគអំពីផលវិបាកនៃហេតុការណ៍នេះ និងចាត់វិធានការសមរម្យដើម្បីដោះស្រាយភ្លាម។ កត់ត្រាអំពីហេតុការណ៍ចូលក្នុងរបាយការណ៍។	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន(ដែលបានបញ្ចូលព័ត៌មានថ្មី)
ខ១.៥	តម្កល់ទុករបាយការណ៍ទាំងនេះ និងរក្សាទុកសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

៦.៥.៣. <u>ឧបករណ៍ផ្ទុកទិន្នន័យ (ហាត ឌីស (Hard Disk) ឬមេមម៉ូរី ស្ទិត (Memory Stick) ឬ មេមម៉ូរី ខាដ (Memory Card))</u>

(ក) និយាន

និយ្យតាពន្ធនៅ

(ក១) ត្រូវចងខ្សែភ្ជាប់ឧបករណ៍ទាំងនេះ ដើម្បីងាយស្រួលដាក់ជាប់នឹងខ្លួនរបស់លោកអ្នក។ ឧបករណ៍ផ្ទុកទិន្នន័យទំនើបៗបច្ចុប្បន្នមានទ្រង់ទ្រាយតូច ងាយជ្រុះ និងបាត់បង់ជាទីបំផុត។

បង្ការការឆ្លងមេរោគ

(ក២) នៅពេលដោតឧបករណ៍ផ្ទុកទិន្នន័យទៅកុំព្យូទ័ររបស់លោកអ្នក មិនត្រូវអនុវត្តការបើកឯកសារដោយស្វ័យប្រវត្តិឡើយ។

(ក៣) ជានិច្চកាល ត្រូវរុករកមេរោគ (Scan) ក្នុង ឧបករណ៍ផ្ទុកទិន្នន័យ នៅពេលដោតវាទៅកុំព្យូទ័ររបស់លោកអ្នក។

ការលុបសម្អាតទិន្នន័យ

(ក៤) ត្រូវលុបសម្អាត ឬបំផ្លាញចោលនូវទិន្នន័យរូបវន្តក្នុងឧបករណ៍ផ្ទុកទិន្នន័យនៃកុំព្យូទ័រ ដោយមិនបន្សល់ទុកនូវទិន្នន័យ ឬព័ត៌មាន ដែលអាចលួចប្រើប្រាស់បានឡើយ។

(ខ) នីតិវិធី(សំរាប់មន្ត្រីគ្រប់រូប)

វិធានការគ្រប់គ្រងសម្ភារៈដែលបានបាត់បង់ ឬត្រូវបានលួច

(ខ១) ប្រសិនបើឧបករណ៍ផ្ទុកទិន្នន័យបានបាត់បង់ ឬត្រូវបានលួច សូមប្រតិបត្តិតាមនីតិវិធីដែលបានរៀបរាប់នៅក្នុង**វិធានការគ្រប់គ្រងសម្ភារៈដែលបានបាត់បង់ ឬត្រូវបានលួចក្រោមវិធាន និងនីតិវិធីទាក់ទងនឹងកុំព្យូទ័រយួរដៃ** ឬ**កុំព្យូទ័រចល័ត**។

៦.៥.៤. <u>សម្ភារៈផ្ទាល់ខ្លួន</u>

(ក) វិធាន

(ក១) ត្រូវសុំការអនុញ្ញាតពីប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដើម្បីអាចនាំយកសម្ភារៈទាក់ទងនឹងកុំព្យូទ័រផ្ទាល់ខ្លួនចេញ ឬចូលក្នុងការិយាល័យ។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៥.៥. <u>កម្មវិធី (ប្រព័ន្ធកុំព្យូទ័រ)</u>

(ក) វិធាន

ទិដ្ឋភាពទូទៅ

(ក១) ត្រូវដំឡើងកម្មវិធីក្នុងប្រព័ន្ធកុំព្យូទ័រដោយបើកចំហ និងដោយទទួលបានការអនុញ្ញាតពីប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន។

(ក២) ត្រូវរៀបចំរូបសណ្ឋាន (Configure) កម្មវិធីកុំព្យូទ័រ ដោយយោងទៅតាមការណែនាំរបស់មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន។

(ក៣) ត្រូវបញ្ចូលកម្មវិធីផេតស៍ (Patches) ភ្លាមៗបន្ទាប់ពីទទួលបានការណែនាំពីមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន។

កម្មវិធី កុំព្យូទ័រ ដែលមិនមានកម្មសិទ្ធិបញ្ញា

(ក៤) ត្រូវមានការប្រុងប្រយ័ត្នចំពោះការទទួលបានសិទ្ធិប្រើប្រាស់កម្មវិធីកុំព្យូទ័រ។ កម្មវិធីភាគច្រើនអាចត្រូវបានដំឡើងនិងប្រើប្រាស់បានក្នុងករណីដែលលោកអ្នកបានបង់ថ្លៃ កម្មសិទ្ធិបញ្ញារួចរាល់ លើកលែងតែជា «កម្មវិធីដែលមិនគិតថ្លៃ» ឬ «កម្មវិធីសំរាប់ប្រើប្រាស់ជាសាធារណៈ» ។ ត្រូវលុបចោល ឬសុំសិទ្ធិប្រើប្រាស់ កម្មវិធីដែលមិនគិតថ្លៃ មានតម្លៃថោក ឬកម្មវិធីសំរាប់ប្រើប្រាស់សាកល្បង នៅពេលដែលផុតកំណត់រយៈ ប្រើប្រាស់សាកល្បង។ កម្មវិធីមួយចំនួនត្រូវបានកំណត់ការប្រើប្រាស់ដោយមិនគិតថ្លៃ សំរាប់បុគ្គលឯកជន ប៉ុន្តែតម្រូវឲ្យបង់ថ្លៃសំរាប់ទទួល បានសិទ្ធិប្រើប្រាស់ក្នុងការងារជំនួញ។ បុគ្គលនិងស្ថាប័នមួយចំនួនអាចត្រូវបានប្តឹងពីបទរំលោភច្បាប់កម្មសិទ្ធបញ្ញា ទាក់ទងនឹងការប្រើប្រាស់កម្មវិធីកុំព្យូទ័រ។ ដូច្នេះមិនត្រូវធ្វើឲ្យខ្លួនឯងនិងស្ថាប័នអាប់ឱនកិត្តិយសដោយសារការប្រព្រឹត្តខុសទៅនឹងច្បាប់បែបនេះឡើយ។

កម្មវិធី កុំព្យូទ័រ ដែលមិនមានការអនុញ្ញាត

(ក៥) មិនត្រូវទាញយក (Download) និង ដំឡើងកម្មវិធីកុំព្យូទ័រប្រើប្រាស់ ដោយមិនមានការអនុញ្ញាតឡើយ។ កម្មវិធីទាំងនេះអាចបង្កភាពគ្រោះថ្នាក់ធ្ងន់ធ្ងរដល់កុំព្យូទ័រផ្ទាល់ខ្លួន ឬបណ្តាញកុំព្យូទ័រ របស់ស្ថាប័នក៏ដូចជាប៉ះពាល់ទៅដល់ប្រតិបត្តិការការងារនៃប្រព័ន្ធកុំព្យូទ័រ របស់លោកអ្នកផងដែរ។ កម្មវិធីកុំព្យូទ័រដែលអនុញ្ញាតឲ្យកុំព្យូទ័ររបស់លោកអ្នកអាច «ត្រូវបានគ្រប់គ្រងពីចំងាយ» (ឧទាហរណ៍ កម្មវិធី PCAnyWhere) ហើយ «ឧបករណ៍

(Tool) សំរាប់ចូលក្នុងប្រព័ន្ធកុំព្យូទ័រដោយពុំមានការអនុញ្ញាត (Hacking)»។
ឧទាហរណ៍៖ ឧបករណ៍ Network Sniffers និងឧបករណ៍ បង្កើតពាក្យ ឬលេខសម្ងាត់ ត្រូវបានហាមឃាត់ជាចំហមិនឲ្យប្រើប្រាស់ ជាមួយសម្ភារៈនានារបស់ ស្ថាប័ន លើកលែងតែទទួលបានការអនុញ្ញាតជាមុនពីថ្នាក់ដឹកនាំក្នុងគោលដៅបំរើការងារស្របច្បាប់។
ឧទាហរណ៍៖ ក្រុមការងារបណ្តាញកុំព្យូទ័រប្រើប្រាស់កម្មវិធីទាំងនេះ ដើម្បីប្រតិបត្តិការបណ្តាញកុំព្យូទ័រ។

ការចំលងទិន្នន័យទុកសំរាប់បង្ការគ្រោះអាសន្ន (Backup)

(ក៦) លោកអ្នកត្រូវចំលងទិន្នន័យទុក (Backup) ពីកុំព្យូទ័រផ្ទាល់ខ្លួនសំរាប់បង្ការគ្រោះអាសន្ន។ វិធីដ៏ងាយស្រួលបំផុត ដើម្បីអនុវត្តកិច្ចការនេះ គឺលោកអ្នកគ្រាន់តែបើកចូលទៅក្នុងកុំព្យូទ័រលោកអ្នក និងផ្ទេរទិន្នន័យដែលបានចំលង ទៅដាក់ក្នុងកុំព្យូទ័រណាមួយដាក់លាក់នៅលើបណ្តាញកុំព្យូទ័រ ជាប្រចាំយ៉ាងតិចមួយដងក្នុងមួយសប្តាហ៍ហើយវាជាការប្រសើរបំផុត ប្រសិនបើអាចអនុវត្តបានជារៀងរាល់ថ្ងៃ។ ប្រសិនបើលោកអ្នកមិនមានបណ្តាញកុំព្យូទ័រទេ លោកអ្នកត្រូវទទួលខុសត្រូវចំលងទិន្នន័យទុក (Backup) ជាប្រចាំដាក់ក្នុងឧបករណ៍ផ្ទុកទិន្នន័យ CD/ DVD/ USB hard disks/ Memory Card/ Memory Stick ។ល។ ការចំលងទិន្នន័យទុក (Backup) ដោយមិនប្រើប្រាស់ បណ្តាញកុំព្យូទ័រ លោកអ្នកត្រូវផ្លាស់ប្តូរទំរង់ទិន្នន័យ (Data Encryption) និង ធ្វើឲ្យទិន្នន័យទាំងនេះមានសន្តិសុខជារូបវន្ត។ ត្រូវចងចាំថាប្រសិនបើកុំព្យូទ័ររបស់អ្នកត្រូវបានលួច បាត់បង់ ខូចខាត ឬលែងដំណើរការ លោកអ្នកមិនអាចយកបានមកវិញនូវទិន្នន័យណាមួយពីកុំព្យូទ័របានទេ។ ការចំលងទិន្នន័យទុក (Backup) ដោយមិនប្រើប្រាស់បណ្តាញកុំព្យូទ័រនេះ នឹងជួយបង្ការនូវស្ថានភាពដែលនាំឲ្យលោកអ្នកខកបំណង និងចំណាយពេលវេលាបន្ថែម ក្នុងការបំពេញការងារ។

(ខ) នីតិវិធី(សំរាប់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន)

សេចក្តីណែនាំសំរាប់ Patch Application

(ខ១) នីតិវិធីខាងក្រោមត្រូវបានកំណត់សំរាប់ណែនាំអំពីរបៀបបញ្ចូលផេតស៍ (Patches)។

ដំណាក់	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	ត្រូវបញ្ចូលនិងកំណត់ព័ត៌មានថ្មីៗ របស់កម្មវិធី កុំព្យូទ័រ ដែលមានបទដ្ឋានត្រឹមត្រូវ និងបញ្ចូលនូវព័ត៌ថ្មីៗចុងក្រោយរបស់ផេតស៍ (Patches) ជាប្រចាំ។ (បញ្ជីនេះអាចសរសេរ «ជានិច្ចកាល ត្រូវធ្វើការបញ្ចូលទិន្នន័យថ្មីៗ (Update) របស់ Windows ភ្លាមៗ លើកលែងតែមានបំរាមជាចំហ»)	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	(បញ្ជីរាយព័ត៌មានថ្មីៗ របស់កម្មវិធី កុំព្យូទ័រ ដែលមានបទដ្ឋានត្រឹមត្រូវ និងព័ត៌ថ្មីៗចុងក្រោយរបស់ផេតស៍ (Patches))
ខ១.២	ធ្វើការចែកចាយបញ្ជីទាំងនេះទៅមន្ត្រីនានា និងជំរុញឲ្យមានការអនុវត្តន៍ភ្លាមៗ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.៣	ត្រូវបញ្ចូលផេតស៍ (Patches) ភ្លាមៗ បន្ទាប់ពីទទួលបានការណែនាំពីមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	អ្នកប្រើប្រាស់	មិនមាន

ការពិនិត្យមើលអំពីការកំណត់ព័ត៌មានរបស់កម្មវិធី កុំព្យូទ័រ

(ខ២) នីតិវិធីខាងក្រោមត្រូវបានបង្កើតឡើង ដើម្បីធ្វើសវនកម្មទាក់ទងនឹងការកំណត់ព័តិមាន របស់កម្មវិធី កុំព្យូទ័រ ផ្នែកខាងក្នុង៖

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ២.១	ដាក់ចេញនូវផែនការ និងរៀបចំការពិនិត្យមើលអំពីការកំណត់ព័ត៌មានរបស់កម្មវិធី កុំព្យូទ័រដូចជាព័ត៌មានពាក់ព័ន្ធកាលបរិច្ឆេទនិងសម្ភារៈកុំព្យូទ័រសំរាប់ប្រើប្រាស់គំរូជាដើម។	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.២	ពិនិត្យមើលអំពីការកំណត់ព័ត៌មានរបស់កម្មវិធីម្តងមួយៗ។ នៅពេលដែលរកឃើញចំនុចណាមួយដែលមិនសមស្រប ត្រូវណែនាំឲ្យម្ចាស់កុំព្យូទ័រកែតម្រូវឲ្យបានត្រឹមត្រូវ។	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.៣	ដាក់ជូននូវរបាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មានប្រសិនបើបានរកឃើញនូវចំនុចដែលមិនសមស្រប	អ្នកប្រើប្រាស់	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន
ខ២.៤	តម្កល់ទុករបាយការណ៍ទាំងនេះ និងរក្សាទុកសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

៦.៥.៦. <u>សារអេឡិចត្រូនិច (E-mail)</u>

(ក) និយាន

(ក១) បច្ចុប្បន្ន ឯកសារជូនភ្ជាប់ក្នុងសារអេឡិចត្រូនិច (E-mail Attachments) គឺជាប្រភព

ដ៏ចំបងបំផុតនៃការចម្លងមេរោគកុំព្យូទ័រ។ ត្រូវចៀសវាងបើករាល់ឯកសារជូនភ្ជាប់ក្នុងសារអេឡិចត្រូនិច (E-mail Attachments) លើកលែងតែលោកអ្នកបានដឹង ច្បាស់លាស់អំពីប្រភពព័ត៌មាននៃអ្នកដែលផ្ញើឯកសារនេះ។

(ក២) មិនត្រូវប្រើប្រាស់សារអេឡិចត្រូនិច៖

(ក២.១) ដើម្បីផ្ញើចេញនូវព័ត៌មានដែលសម្ងាត់ ឬរសើប ជាពិសេសនៅលើបណ្តាញអ៊ីនធឺណិត (Internet) លើកលែងតែវាត្រូវបានផ្លាស់ប្តូរទំរង់ដើម (Encrypted) ដោយប្រព័ន្ធសំរាប់ផ្លាស់ប្តូរទំរង់ដើម ដែលទទួលស្គាល់ត្រឹមត្រូវថាអាចធានាបាននូវសន្តិសុខព័ត៌មាន។

(ក២.២) សំរាប់ការងារឯកជន ឬការងារសប្បុរសធម៌ ដែលមិនទាក់ទងនឹងការងារស្របច្បាប់របស់អង្គភាព។

(ក២.៣) នៅក្នុងលក្ខខណ្ឌដែលបំពេញនូវកិច្ចការទាក់ទងនឹងការចេញនូវសេចក្តីថ្លែងការណ៍ជាសាធារណៈ និងជាផ្លូវការតំណាងឲ្យអង្គភាព លើកលែងតែលោកអ្នកមានតួនាទីជាអ្នកនាំពាក្យ ដែលទទួលបានការតែងតាំងជាចំហដោយថ្នាក់ដឹកនាំ ដើម្បីចេញសេចក្តីរាយការណ៍បែបនេះ។

(ក២.៤) ដើម្បីផ្ញើសារដោយប្រើប្រាស់ អត្តសញ្ញាណ និងលេខសម្ងាត់ (Account) របស់នរណាម្នាក់ ឬផ្ញើក្នុងលក្ខណៈតំណាងឲ្យនរណាម្នាក់ រួមទាំងការប្រើប្រាស់អាស័យដ្ឋានក្លែងក្លាយ ដែលសរសេរក្នុង «កន្លែងបំពេញអាសយដ្ឋានផ្ញើចេញ»។ ប្រសិនបើមានការអនុញ្ញាតពីអ្នកគ្រប់គ្រង លេខាធិការម្នាក់អាចផ្ញើសារអេឡិចត្រូនិច (E-mail) ជំនួសបាន

ប៉ុន្តែគួរតែមានហត្ថលេខារបស់លេខាធិការនោះចុះក្នុងសារអេឡិចត្រូនិច។

(ក២.៥) ដើម្បីផ្ញើនូវអ្វីមួយដែលមានលក្ខណៈរំខាន ប្រមាថមើលងាយ គ្មានសីលធម៌ខុសច្បាប់ ឬមិនសមរម្យ រួមទាំងសេចក្តីអធិប្បាយដែលមានលក្ខណៈរើសអើងទាក់ទង នឹងសាសនា ភេទ ពណ៌សម្បុរ ពិការភាព ភេទសម្ព័ន្ធ អាសគ្រាម ភេរវកម្ម ការប្រតិបត្តិ និងជំនឿផ្នែកសាសនា ជំនឿផ្នែកនយោបាយ ប្រភពដើមនៃសញ្ជាតិ និង គេហទំព័រសំរាប់ចូលទៅក្នុងគេហទំព័រដ៏ទៃ (Hyperlinks) ឬឯកសារយោងដ៏ទៃទៀត សំរាប់ចូលទៅកាន់គេហទំព័រដែលមិនសមរម្យ ឬប្រមាថមើលងាយដោយចំហ រួមជាមួយនឹងអ្វីដែលស្រដៀងគ្នានេះ ដូចជារឿងកំប្លែង សំបុត្រធ្វើបន្ត (Chain Letters) ការព្រមានអំពីមេរោគ ការបោកបញ្ឆោត ការស្នើសុំការបរិច្ចាគមេរោគ ឬកម្មវិធីកុំព្យូទ័រដ៏ទៃទៀត ដែលមានលក្ខណៈលេងសើច។

(ក២.៦) ក្នុងគោលបំណងអ្វីមួយដែលខុសច្បាប់ គ្មានសីលធម៌ និងមិនមានការអនុញ្ញាត។

(ក៣) ត្រូវមានសុកនិច្ឆ័យក្នុងវិជ្ជាជីវៈ នៅពេលប្រើប្រាស់សារអេឡិចត្រូនិច ដូចជាត្រូវគោរពតាមច្បាប់សុជីវធម៌ ដែលត្រូវបានទទួលស្គាល់ជាទូទៅទាក់ទងនឹងសារអេឡិចត្រូនិច។

(ក៤) ត្រូវពិនិត្យមើលសារអេឡិចត្រូនិចឡើងវិញ ដោយប្រុងប្រយ័ត្នមុនពេលផ្ញើចេញ ជាពិសេសចំពោះសារផ្លូវការ សំរាប់ទំនាក់ទំនងជាមួយបុគ្គលខាងក្រៅ។

(ក៥) បើមិនចាំបាច់ មិនត្រូវបញ្ចេញព័ត៌មានដែលមានលក្ខណៈរសើប តាមរយៈសារដែលផ្ញើចេញពីការិយាល័យឡើយ។

(ក៦) មន្ត្រីរាជការទាំងឡាយមិនត្រូវស្នាក់លួច បញ្ជូនត កែប្រែ លុប រក្សាទុក ឬបង្ហាញចេញ

នូវព័ត៌មាននៅក្នុងសារអេឡិចត្រូនិចឡើយ លើកលែងទទួលបានការអនុញ្ញាត ត្រឹមត្រូវពីថ្នាក់ដឹកនាំ ឬវាជាប្រការចាំបាច់សំរាប់ការងារគ្រប់គ្រងប្រព័ន្ធបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន។

(ក៧) ក្នុងករណីដែលមានកិច្ចការមិនសូវសំខាន់កើតឡើងម្តងម្កាល និងមិនប៉ះពាល់ដល់ការងាររបស់អង្គភាព ការប្រើប្រាស់ផ្ទាល់ខ្លួនដោយមានកំណត់នូវប្រព័ន្ធសារអេឡិចត្រូនិចរបស់អង្គភាពអាចត្រូវបានអនុញ្ញាត តាមរយៈការយល់ព្រមពីថ្នាក់ដឹកនាំរបស់ខ្លួន។ លោកអ្នកមិនត្រូវគិតថា នឹងទទួលបាននូវភាពសម្ងាត់ក្នុងការប្រើប្រាស់សារអេឡិចត្រូនិចឡើយដោយហេតុថារាល់សារទាំងអស់ដែលឆ្លងកាត់ប្រព័ន្ធ និងបណ្តាញកុំព្យូទ័ររបស់រដ្ឋ នឹងត្រូវបានរុករកមេរោគ (Scan) ដោយស្វ័យប្រវត្តិ នឹងអាចត្រូវបានរក្សាទុកជាច់ដោយឡែក នឹងត្រូវបានពិនិត្យឡើងវិញដោយនិយោជិតដែលបានចាត់តាំង។

(ក៨) ត្រូវធ្វើ និងរក្សាទុកសារអេឡិចត្រូនិចរបស់លោកអ្នកក្នុងទំហំ និងចំនួនមួយសមរម្យ។ ជានិច្ចកាល ត្រូវសម្អាតប្រអប់សារ (Mailbox) របស់លោកអ្នក លុបចោលសារអេឡិចត្រូនិចចាស់ៗដែលលែងត្រូវការ និងតម្កល់ទុកសារនានាដោយត្រូវរក្សាទុកឲ្យបានត្រឹមត្រូវនៅក្នុងកន្លែងផ្ទុកឯកសារ (Folders) របស់សារអេឡិចត្រូនិច។

ពន្យារការអនុវត្តន៍

(ខ) នីតិវិធី(សំរាប់មន្ត្រីគ្រប់រូប)

វិធានការទូទៅសំរាប់ដោះស្រាយបញ្ហាទាក់ទងនឹងសន្តិសុខព័ត៌មាន

(ខ១) នីតិវិធីខាងក្រោមត្រូវបានបង្កើតឡើង ដើម្បីធ្វើសេចក្តីរាយការណ៍ភ្លាមៗ អំពីបញ្ហាទាក់ទងនឹងសន្តិសុខព័ត៌មាន៖

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	ពិនិត្យមើលហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន ដូចជាការផ្ញើសារអេឡិចត្រូនិចដែលមិនសម្បូរឬមិនល្អ	អ្នកប្រើប្រាស់	មិនមាន
ខ១.២	ត្រូវជូនដំណឹងទៅការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានមិនលើសពីមួយម៉ោង បន្ទាប់ពីមានបញ្ហាណាមួយកើតឡើង	អ្នកប្រើប្រាស់	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន
ខ១.៣	ធ្វើការវិភាគអំពីផលប៉ះពាល់នៃបញ្ហាដែលកើតឡើង និងចាត់វិធានសមរម្យណាមួយដើម្បីដោះស្រាយ។ ធ្វើការកត់ត្រាចូលក្នុងរបាយការណ៍។	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន (ដែលបានបញ្ចូលព័ត៌មានថ្មី)
ខ១.៤	តម្កល់ទុករបាយការណ៍ទាំងនេះនិងរក្សាទុកសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

៦.៥.៧. <u>ការស្វែងរកព័ត៌មានលើបណ្តាញអ៊ីនធឺណិត</u>

(ក) ខិចាន

ទិដ្ឋភាពទូទៅ

(ក១) មិនត្រូវទាញយក (Download) ឯកសារដែលអាចដំណើរការបាន (Executable File) ក្នុងប្រព័ន្ធប្រតិបត្តិការកុំព្យូទ័រ ដោយគ្មានការអនុញ្ញាតពីប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មានឡើយ។

(ក២) អាចទាញយក (Download) តែឯកសារណា ដែលមានវិញ្ញាបនប័ត្រ ឬអាជ្ញាប័ណ្ណ ប៉ុណ្ណោះ។

(ក៣) មិនត្រូវចុចភ្ជាប់បន្ត (Link) ទៅកាន់គេហទំព័រ ឬសារអេឡិចត្រូនិចណាមួយផ្សេងទៀត ដែលមិនបានស្គាល់ច្បាស់លាស់ឡើយ។

(ក៤) វាជាការប្រសើរបំផុត ដែលអាចជៀសវាងការរក្សាទុកឃុគឃី (Cookies) ដែលអាចធ្វើឲ្យមានការលេចធ្លាយនូវព័ត៌មានទាក់ទងនឹងអត្តសញ្ញាណអ្នកប្រើប្រាស់ (User ID) និងលេខ ឬពាក្យសម្ងាត់ (Password)។

(ក៥) កំណត់នៅក្នុងកម្មវិធីមើលគេហទំព័រ (Web Browser) ដែលទាក់ទងទៅនឹងចំនុចដែលបានរៀបរាប់ខាងលើ។

បញ្ហាមិនសមរម្យ

(ក៦) ការិយាល័យសន្តិសុខព័ត៌មាននៃ អ.អ.ប.គ.ព ក៏ដូចជាការិយាល័យសន្តិសុខព័ត៌មានតាមបណ្តាស្ថាប័ន មិនអនុញ្ញាតអោយមានប្រើប្រាស់ឯកសារ រូបភាព រូបភាពវីដេអូ ឬសារអេឡិចត្រូនិចមិនសមរម្យ ដែលបង្ហាញពីភាពអាសគ្រាម ការប្រកាន់ពូជសាសន៍ ការបង្ខូចកេរ្តិ៍ឈ្មោះ ឬការរំខាននានា ដែលអាចបង្កឲ្យមានការអាក់អន់ចិត្ត ឬភាពអាម៉ាស់ឡើយ។ មិនត្រូវរក្សាទុក ចំលង ប្រើប្រាស់ ឬចរាចរនូវអ្វីដែលបានរៀបរាប់ខាងលើ និងជៀសវាងចូលទៅប្រើប្រាស់ គេហទំព័រណាមួយដែលគួរឲ្យសង្ស័យ។ ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវត្រួតពិនិត្យបណ្តាញកុំព្យូទ័រ និងប្រព័ន្ធផ្សេងៗជាប្រចាំដើម្បីការពារកុំឲ្យមានការប្រើប្រាស់ ឬចរាចរនូវអ្វីដែលបានរៀបរាប់ខាងលើ និងធ្វើការតាមដានរាល់ការប្រើប្រាស់ អ៊ីនធឺណិត បើរកឃើញនៅកំហុសណាមួយ ការិយាល័យនេះនឹងរាយការណ៍ដោយ

ផ្ទាល់អំពីសកម្មភាពរបស់អ្នកដែលបានប្រព្រឹត្តខុសធ្ងន់ធ្ងរ ឬច្រំដែរ ទៅកាន់នាយកផ្នែកសន្តិសុខព័ត៌មាន មុននឹងមានការចាត់វិធានការដាក់វិន័យកើតឡើង។

- ប្រសិនបើលោកអ្នកទទួលបាននូវឯកសារណាមួយ មិនសមរម្យតាមរយៈសារអេឡិចត្រូនិច ឬតាមមធ្យោបាយផ្សេងៗ ត្រូវលុបចោលរបស់ឯកសារទាំងនោះជាបន្ទាន់។
- ប្រសិនបើលោកអ្នកបានចូលទៅកាន់គេហទំព័រណាមួយ មិនសមរម្យដោយចៃដន្យ ត្រូវចុចលើប៊ូតុង ត្រលប់ក្រោយ (Back) ឬបិទផ្ទាំងកម្មវិធីវីនដូ (Window) តែម្តង។
- ប្រសិនបើលោកអ្នកទទួលបានស្ពែម (Spam) ជាប្រចាំ ត្រូវរាយការណ៍ទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានដើម្បីត្រួតពិនិត្យ និងផ្តល់នីតិវិធីដោះស្រាយ។

(ខ) នីតិវិធី(សំរាប់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន)

កំណត់មុខងារត្រួតពិនិត្យលើ កម្មវិធីមើលគេហទំព័រ (Web Browser)

(ខ១) នីតិវិធីខាងក្រោមនេះត្រូវបានបង្កើតឡើង ដើម្បីត្រួតពិនិត្យការកំណត់ក្នុងកម្មវិធីបើកមើលគេហទំព័រ (Web Browser)

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	ដាក់ចេញនូវផែនការ និងរៀបចំការត្រួតពិនិត្យលើមុខងារក្នុងកម្មវិធីមើលគេហទំព័រដូចជា កាលបរិច្ឆេទ និងកុំព្យូទ័រដែលត្រូវប្រើជាគំរូ។ហើយធ្វើការណែនាំ មុនពេលធ្វើការត្រួតពិនិត្យ។	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.២	ដាក់ចេញនូវផែនការ និងរៀបចំការត្រួតពិនិត្យលើមុខងារក្នុង	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខ	មិនមាន

	កម្មវិធីមើលគេហទំព័រម្តងមួយៗ។ នៅពេលដែលរកឃើញនូវចំនុចដែលមិនសមស្រប ត្រូវណែនាំម្ចាស់កុំព្យូទ័រឲ្យធ្វើការកែតម្រូវ។	ព័ត៌មាន	
ខ១.៣	ដាក់ជូននូវរបាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មានប្រសិនបើបានរកឃើញនូវចំនុចដែលមិនសមរម្យ	អ្នកប្រើប្រាស់	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន
ខ១.៤	តម្កល់ទុករបាយការណ៍ទាំងនេះ និងរក្សាទុកសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

៦.៦. <u>សន្តិសុខបណ្តាញ កុំព្យូទ័រ និង ម៉ាស៊ីនកុំព្យូទ័រមេ (Server) ដែលនឹងត្រូវកំណត់ដោយពេញលេញនាពេលអនាគត</u>

៦.៦.១. <u>បណ្តាញកុំព្យូទ័រខាងក្នុង (LAN) និងប្រព័ន្ធអ៊ីនធឺណិត</u>

(ក) ទិដ្ឋាន

ពន្យារការអនុវត្តន៍

ផ្នែកនេះនឹងអនុវត្តនៅលើ ប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យា នៃរាជរដ្ឋាភិបាលកម្ពុជា នៃអាជ្ញាធរជាតិ អ.អ.ប.ត.ព។ ឯកសារណែនាំស្តីអំពីការគ្រប់គ្រងប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យា និងបណ្តាញជាតិ និងត្រូវបង្កើតឡើង។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៦.២. ម៉ាស៊ីនកុំព្យូទ័រមេ (Server)

(ក) និយាន

ពន្យារការអនុវត្តន៍

ផ្នែកនេះនឹងអនុវត្តនៅលើប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យានៃរាជរដ្ឋាភិបាលកម្ពុជា នៃអាជ្ញាធរជាតិ អ.អ.ប.គ.ព។ ឯកសារណែនាំស្តីអំពីការគ្រប់គ្រងប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យា និងបណ្តាញជាតិ និងត្រូវបង្កើតឡើង។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៧. សន្តិសុខកម្មវិធីប្រើប្រាស់ (Application) នឹងត្រូវបានកំណត់នាពេលអនាគត់

(ក) និយាន

(ផ្នែកនេះធ្វើការកំណត់អំពីតម្រូវការសន្តិសុខព័ត៌មាន និងអំពីបញ្ហានានានៃគំរោងបង្កើតកម្មវិធីប្រើប្រាស់)

៧. ការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មាន

៧.១. ដំណើរការនៃការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មាន

មន្ត្រីគ្រប់រូបត្រូវទទួលការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មាន យ៉ាងតិចម្តងជារៀងរាល់ឆ្នាំ។ នីតិវិធីខាងក្រោមកំណត់នូវការរៀបចំផែនការ និងការអនុវត្តន៍ការងារបណ្តុះបណ្តាល ផ្នែកសន្តិសុខព័ត៌មាន។

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	រៀបចំផែនការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មានសំរាប់ទាំងមន្ត្រីដែលមានបទពិសោធន៍ និងមន្ត្រីដែលទើបជ្រើសរើសថ្មី	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន

ខ១.២	អនុវត្តការបណ្តុះបណ្តាល	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.៣	កត់ត្រាព័ត៌មានទាក់ទងនឹងមន្ត្រីដែលបានចូលរួមក្នុងវគ្គបណ្តុះបណ្តាល និងរក្សាទុកកំណត់ត្រានេះសំរាប់រយៈកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	កំណត់ត្រាអំពីការបណ្តុះបណ្តាល

៧.២. <u>ការផ្លាស់លិខិតកិច្ចសន្យា</u>

មន្ត្រីទាំងអស់ត្រូវការផ្លាស់លិខិតកិច្ចសន្យាយ៉ាងតិចម្តង ដើម្បីការពារសន្តិសុខព័ត៌មាន។ វាជាការប្រសើរមួយ ដែលលោកអ្នកបានចុះហត្ថលេខា រាល់ពេលចូលរួមវគ្គបណ្តុះបណ្តាល។ នីតិវិធីខាងក្រោមធ្វើការកំណត់អំពីបែបបទនៃការផ្លាស់លិខិតកិច្ចសន្យា។

ដំណាក់កាល	**សេចក្តីអធិប្បាយ**	**អ្នកអនុវត្ត**	**បញ្ជីព័ត៌មាន**
ខ២.១	ចែកចាយលិខិតសន្យាដែលមិនទាន់បំពេញព័ត៌មាន	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.២	អានអត្ថន័យក្នុងលិខិតទាំងមូល ចុះហត្ថលេខាក្នុងលិខិត និងដាក់បញ្ជូនលិខិត	អ្នកប្រើប្រាស់	លិខិតសន្យា
ខ២.៣	តម្កល់ ឬរក្សាទុកលិខិតទាំងនេះសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

៨. ការខាយតំលៃ

បញ្ហាមួយចំនួនខាងក្រោម នឹងត្រូវបានវាយតំលៃពីមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន និងរាយការណ៍ទៅ ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានយ៉ាងតិចម្តងក្នុងមួយឆ្នាំ។ របាយការណ៍

នេះនឹងជំរុញការលើកកម្ពស់ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន យោងតាមសេចក្តីលំអិតនៃទិសដៅនីមួយៗ។

ល.រ	បញ្ហាដែលត្រូវដោះស្រាយ	និយមន័យ	អនុញ្ញាតដោយ
១	កំរិតនៃការបញ្ចប់ការបណ្តុះបណ្តាល	% នៃមន្ត្រីដែលបានបញ្ចប់វគ្គបណ្តុះបណ្តាល ក្នុងចំណោមមន្ត្រីស្ថាប័នដែលបានចូលរួម	ប្រធានស្ថាប័ននិងផ្នែកពាក់ព័ន្ធ
២	ហេតុការណ៍នៃសន្តិសុខព័ត៌មានស្របពេលនិងការបញ្ចប់ដំណើរការតាមប្រភេទហេតុការណ៍នីមួយៗ	រូបមន្តនៃការបូកបញ្ចូល (ពេលវេលាសំរាប់បញ្ចប់ដំណើរការដោះស្រាយបញ្ហា ដកចំនួនពេលវេលាដែលកើតហេតុការណ៍) ហើយចែកនឹងចំនួនហេតុការណ៍ដែលបានបែងចែកតាមប្រភេទគុណនិងចំនួន(ប្រភេទហេតុការណ៍នីមួយៗត្រូវបានកំណត់នៅក្នុងរបាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មានដែលមិនទាន់បំពេញព័ត៌មាន)	នាយកផ្នែកសន្តិសុខព័ត៌មាន
៣	កំរិតនៃប្រតិបត្តិការរុករក (Scan) មេរោគ	% នៃមន្ត្រីក្នុងចំណោមមន្ត្រី អ.អ.ប.គ.ព ទាំងអស់ដែលបានបំពេញការងាររុករក (Scan) មេរោគ ក្នុងកំឡុងពេលអនុវត្តនីតិវិធីការពារការឆ្លងមេរោគ	នាយកផ្នែកសន្តិសុខព័ត៌មាន
៤	កំរិតនៃការឆ្លង លិខិតកិច្ចសន្យា	% នៃមន្ត្រីដែលបានឆ្លងលិខិតកិច្ចសន្យា ក្នុងចំណោមមន្ត្រី អ.អ.ប.គ.ព ទាំងអស់	នាយកផ្នែកសន្តិសុខព័ត៌មាន
	-ផ្នែកចុងក្រោយនៃបញ្ជី-		

៩. ទោសប្បញ្ញត្តិ (នឹងត្រូវបានកំណត់នាពេលអនាគត)

(ក) និយាន

(ផ្នែកនេះធ្វើការកំណត់អំពីទោសប្បញ្ញត្តិ ទាក់ទងនឹងការបំពានច្បាប់សន្តិសុខព័ត៌មាន។ វាតម្រូវឲ្យមានការរៀបចំរបៀបរៀបរយ ធនធានមនុស្សផ្ទៃក្នុង សំរាប់មន្ត្រីរាជការទាំងអស់។)

១០. បញ្ជីកំណត់ត្រាព័ត៌មាន

ល.រ	ឈ្មោះបញ្ជី	ឯកសារយោង	ធ្វើសេចក្តីព្រាងដោយ	អនុញ្ញាតដោយ
១	បញ្ជីព័ត៌មានស្តីអំពីការបណ្តុះបណ្តាល	ជំពូកទី ៧.១៖ ដំណើរការនៃការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មាន	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	ប្រធានស្តាប័ន និងផ្នែកពាក់ព័ន្ធ
២	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន	(១) នីតិវិធីនៃចំណាត់ការក្នុងការចាប់មេរោគនៅក្នុងជំពូកទី៦.៥.១៖ កុំព្យូទ័រលើតុ (២) នីតិវិធីនៃវិធានការគ្រប់គ្រង សម្ភារៈដែលបានបាត់បង់ឬត្រូវបានលួចនៅក្នុងជំពូកទី ៦.៥.២៖ កុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័ត (៣) នីតិវិធីនៃការពិនិត្យមើលអំពីការកំណត់ព័ត៌មានរបស់កម្មវិធី	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	ប្រធានស្តាប័ន និងផ្នែកពាក់ព័ន្ធ

		(កុំព្យូទ័រ) នៅក្នុងជំពូកទី ៦.៥.៥៖ កម្មវិធី (ប្រព័ន្ធកុំព្យូទ័រ) (៤) នីតិវិធីនៃវិធានការទូទៅសំរាប់ដោះស្រាយបញ្ហាទាក់ទងនឹងសន្តិសុខព័ត៌មាននៅក្នុងជំពូកទី ៦.៥.៦៖សារអេឡិចត្រូនិច (E-mail) (៥) នីតិវិធីនៃការពិនិត្យមើលអំពីការកំណត់ព័ត៌មានរបស់មុខងារសំរាប់ស្វែងរកព័ត៌មានលើបណ្តាញអ៊ីនធឺណិត (web browser) នៅក្នុងជំពូកទី៦.៥.៦៖ ការស្វែងរកព័ត៌មានលើបណ្តាញអ៊ីនធឺណិត		
៣	បញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ	នីតិវិធីនៃចំណាត់ការក្នុងការចាប់មេរោគនៅក្នុងជំពូកទី៦.៥.១៖ កុំព្យូទ័រលើតុ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	ប្រធានស្ថាប័ន និងផ្នែកពាក់ព័ន្ធ
៤	លិខិតសន្យា	ជំពូកទី ៧.២៖ ការដាក់ជូនលិខិតសន្យា	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	ប្រធានស្ថាប័ន និងផ្នែកពាក់ព័ន្ធ
	-ផ្នែកចុងក្រោយនៃបញ្ជី			

ផ្នែក ទី៤

សេចក្តីសន្យា
ស្តីពី
ការរក្សាសន្តិសុខជ័ឥមាន របស់ រាជរដ្ឋាភិបាល

សេចក្តីសន្យា
ស្តីពីការរក្សាសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល

«គំរូ»

ក្នុងនាមជាមន្ត្រីរាជការមួយរូប នៃរាជរដ្ឋាភិបាលកម្ពុជា ខ្ញុំបាទ/នាងខ្ញុំសូមធ្វើការសន្យា ដូចខាងក្រោម ដើម្បីរក្សាសុវត្ថិភាពព័ត៌មាន របស់រាជរដ្ឋាភិបាល៖

- ជានិច្ចកាល ខ្ញុំបាទ/នាងខ្ញុំគោរពតាមគោលនយោបាយរបស់ប្រព័ន្ធគ្រប់គ្រងព័ត៌មាន របស់ រាជរដ្ឋាភិបាល និងគោរពតាមបទប្បញ្ញត្តិ និងនីតិវិធីដែលបានចែងនៅក្នុងសៀវភៅវិធាន ស្តីអំពីសន្តិសុខ ព័ត៌មានរបស់រដ្ឋាភិបាល គ្រប់គ្រងដោយក្រសួងមន្ទីរដែល ខ្ញុំបាទ/នាងខ្ញុំ កំពុងបំរើ ការងារ។
- ខ្ញុំបាទ/នាងខ្ញុំសូមទទួលខុសត្រូវចំពោះសកម្មភាពខាងក្រោម៖
  - ជានិច្ចកាលត្រូវសម្រេចថា តើខ្ញុំបាទ/នាងខ្ញុំអាចទទួលយករៀបចំ ឬ រក្សាទុកនូវព័ត៌មានសម្ងាត់នានាបានដែរឬទេ។ ខ្ញុំបាទ/នាងខ្ញុំ ត្រូវចៀសវាងនូវហានិភ័យមួយចំនួនដែល ប៉ះពាល់ដល់ព័ត៌មានទាំងនេះ ដូចជាការធ្វើឲ្យលេចធ្លាយការលួចបន្លំ និងលទ្ធភាពដែល មិនអាចប្រើប្រាស់បាន។
  - ខ្ញុំបាទ/នាងខ្ញុំត្រូវចាក់សោច្រកចេញចូល ទូឯកសារ និងថតគុនៅការិយាល័យធ្វើការ មុនពេលចាកចេញ។
  - ខ្ញុំបាទ/នាងខ្ញុំត្រូវបើកឲ្យដំណើរការនូវមុខងារចាប់មេរោគដោយស្វ័យប្រវត្តិ របស់កម្មវិធី កំចាត់មេរោគ។ ខ្ញុំបាទ/នាងខ្ញុំត្រូវ ធ្វើអោយកម្មវិធីកំចាត់មេរោគទាន់សម័យ (Update Definition) យ៉ាងតិចចំនួនមួយដងក្នុងមួយសប្តាហ៍។ ខ្ញុំបាទ/នាងខ្ញុំត្រូវរុករកមេរោគ (Scan) ក្នុងឧបករណ៍ផ្ទុកទិន្នន័យក្នុងកុំព្យូទ័ររបស់ខ្ញុំបាទ/នាងខ្ញុំជារៀងរាល់សប្តាហ៍ រួមជាមួយនឹងឧបករណ៍ផ្ទុកទិន្នន័យដ៏ទៃទៀត ដែលភ្ជាប់ពីខាងក្រៅកុំព្យូទ័រ (ឧទាហរណ៍ អេហ្វឌី មេមម៉ូរី ខាត/ស្តិគ (Memory Card/Stick) និងអេជឌីឌី) រាល់ពេលដែលភ្ជាប់ ទៅកាន់កុំព្យូទ័ររបស់ខ្ញុំបាទ/នាងខ្ញុំ។
- ខ្ញុំបាទ/នាងខ្ញុំបានយល់ច្បាស់អំពីហានិភ័យ ទាក់ទងនឹងសុវត្ថិភាពរបស់ព័ត៌មាន ហើយការបំពានច្បាប់សុវត្ថិភាពព័ត៌មាន អាចនាំឲ្យខ្ញុំបាទ/នាងខ្ញុំទទួលនូវទោសប្បញ្ញត្តិណាមួយជាធរមាន។

ហត្ថលេខា _____

(មុខងារៈ)

កាលបរិច្ឆេទ _____

ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ទីស្តីការគណៈរដ្ឋមន្ត្រី
លេខ: ១៩.សសរ

សេចក្តីសម្រេច
ស្តីពី
ការបង្កើតក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការសន្តិសុខ បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន

ឧបនាយករដ្ឋមន្ត្រី រដ្ឋមន្ត្រីទទួលបន្ទុកទីស្តីការគណៈរដ្ឋមន្ត្រី

- បានឃើញរដ្ឋធម្មនុញ្ញនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកត/០៩០៨/១០៥៥ ចុះថ្ងៃទី ២៥ ខែ កញ្ញា ឆ្នាំ ២០០៨ ស្តីពីការតែងតាំងរាជរដ្ឋាភិបាលនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រមលេខ ០២/នស/៩៤ ចុះថ្ងៃទី ២០ ខែកក្កដា ឆ្នាំ១៩៩៤ ដែលប្រកាសឱ្យប្រើច្បាប់ ស្តីអំពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃគណៈរដ្ឋមន្ត្រី
- បានឃើញព្រះរាជក្រមលេខ នស/រកម/០១៩៦/០៩ ចុះថ្ងៃទី ២៤ ខែ មករា ឆ្នាំ១៩៩៦ ដែលប្រកាសឲ្យប្រើច្បាប់ស្តីពីការបង្កើតទីស្តីការគណៈរដ្ឋមន្ត្រី
- បានឃើញព្រះរាជក្រឹត លេខ នស/រកត/០៨០០/១៥២ ចុះថ្ងៃទី ២៣ ខែ សីហា ឆ្នាំ ២០០០ ស្តីពីការបង្កើតអាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា
- យោងតាមការចាំបាច់

សម្រេច

ប្រការ ១៖ ត្រូវបានបង្កើត ក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន ជាភាសាអង់គ្លេសហៅថា ICT Security Management Technical Team (iSMTT) ដែលមានសមាសភាពដូចខាងក្រោម៖

១. ឯកឧត្តម **ជា ហានិក**	អគ្គលេខាធិការរង	ជាប្រធាន
២. លោក **ឥណ្ឌា ខែមម៉ា**	ប្រធានក្រុមការងារបណ្តាញ	ជាអនុប្រធាន
៣. លោក **ហាស កុសល**	ប្រធានក្រុមការងារប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យា	ជាអនុប្រធាន
៤. លោក **ឈួន ម៉ន់**	ប្រធានក្រុមការងារប្រព័ន្ធសច្ចានុម័តអេឡិចត្រូនិច	ជាសមាជិក
៥. លោក **លឹម កែវថារ៉ា**	មន្ត្រី	ជាសមាជិក
៦. កញ្ញា **សេង ម៉ូរី**	មន្ត្រី	ជាសមាជិក
៧. លោក **ម៉ាប់ ច័ន្ទតារក្ស**	មន្ត្រី	ជាសមាជិក
៨. លោក **អ៊ូច សុតា**	មន្ត្រី	ជាសមាជិក
៩. លោក **ម៉ម ពិសិដ្ឋ**	មន្ត្រី	ជាសមាជិក
១០. លោក **ថន មករា**	មន្ត្រី	ជាសមាជិក
១១. លោក **ហោច ម៉ារ៉ា**	មន្ត្រី	ជាសមាជិក
១២. លោក **តាន់ សុភ័ក្ត្រ**	មន្ត្រី	ជាសមាជិក
១៣. លោក **តាន់ សេរីសុជ**	មន្ត្រី	ជាសមាជិក
១៤. លោក **អ៊ុក ខេមរា**	មន្ត្រី	ជាសមាជិក
១៥. លោក **សុខ សុលីដា**	មន្ត្រី	ជាសមាជិក
១៦. លោក **ធឹម សំអាត**	មន្ត្រី	ជាសមាជិក
១៧. លោក **សូ សេរីរដ្ឋ**	មន្ត្រី	ជាសមាជិក
១៨. លោក **ឈុន សុវណ្ណដារ៉ា**	មន្ត្រី	ជាសមាជិក
១៩. សមាជិកក្រុមការងារបណ្តាញ		ជាសមាជិក
២០. សមាជិកក្រុមការងារអភិវឌ្ឍន៍ធនធានមនុស្ស		ជាសមាជិក
២១. ក្រុមការងារជាតិកម្ពុជាទប់ទល់នឹងបញ្ហាបន្ទាន់នៃកុំព្យូទ័រ (CamCERT)		ជាសមាជិក

ប្រការ ២៖ ក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការសន្តិសុខ បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន មានភារៈកិច្ច ដូចខាងក្រោម៖

- ជំរុញឲ្យអនុវត្តនូវប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រដ្ឋាភិបាល (Government Information Security Management System - GISMS) ក្នុងអគ្គលេខាធិការដ្ឋានអាជ្ញាធរជាតិ

ទទួលបន្ទុក កិច្ចការអភិវឌ្ឍន៍ បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា (អ.អ.ប.គ.ព / NiDA) មុននឹងឈានដល់ការដាក់ ឲ្យដំណើរការនៅតាមបណ្តាក្រសួង-ស្ថាប័ននានា

- សិក្សា កំ ណត់និយាម (Standard) ស្តីពី បរិក្ខារអេឡិចត្រូនិច ឧបករណ៍បច្ចេកទេសសម្ភារៈកុំព្យូទ័រ (Hardware) កំរងកម្មវិធីកុំព្យូទ័រ (Software) និងបរិក្ខារព័ត៌មានវិទ្យា ដ៏ទៃទៀតដែលត្រូវប្រើប្រាស់នៅ ក្នុង អ.អ.ប.គ.ព ក៏ដូចជាតាមបណ្តាក្រសួង-ស្ថាប័នពាក់ព័ន្ធនានា
- សិក្សាស្រាវជ្រាវប្រមូលទិន្នន័យ នៃការផ្តល់សេវាអ៊ីនធឺណិត និងបច្ចេកវិទ្យា ព័ត៌មានវិទ្យា ដើម្បីកំណត់និយាម (Standard) សន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន
- សិក្សារៀបចំបង្កើតទីតាំងសុវត្ថិភាពសម្រាប់រក្សាទុកទិន្នន័យព័ត៌មានអេឡិចត្រូនិច គេហទំព័រ សារអេឡិចត្រូនិច និងគ្រប់គ្រងការចុះឈ្មោះជាកម្មសិទ្ធនៃគេហទំព័រក្នុងទម្រង់ .gov.kh ដើម្បីជានាប្រសិទ្ធភាព និរន្តភាព និងសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន របស់រាជរដ្ឋាភិបាល
- រៀបចំការបណ្តុះបណ្តាលលើជំនាញការពារសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន ដោយជំរុញការប្រើប្រាស់ភាសាជាតិ ក្នុង វិស័យបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន
- ធ្វើកិច្ចសហប្រតិបត្តិការជាមួយដៃគូអភិវឌ្ឍន៍នានា ដើម្បីពង្រឹងវិស័យសន្តិសុខ បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន
- រៀបចំ ចងក្រងសៀវភៅឯកសារ ស្តីពីនិយាមបច្ចេកទេស និងការណែនាំអំពីវិធីសាស្ត្រ នៃការគ្រប់គ្រងឯកសារអេឡិចត្រូនិច ដោយប្រសិទ្ធភាព
- សិក្សា រៀបចំគោលនយោបាយ និងធ្វើផែនការ ស្តីពីកិច្ចការអភិវឌ្ឍវិស័យសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន
- ធ្វើសហប្រតិបត្តិការជាមួយក្រសួង-ស្ថាប័នពាក់ព័ន្ធ ដើម្បីបង្កើតក្របខ័ណ្ឌច្បាប់ និងបទដ្ឋានគតិយុត្តិ ស្តីពីសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន
- រៀបចំគោលនយោបាយ ផែនការយុទ្ធសាស្ត្រ ស្តីពីការគ្រប់គ្រង ការរក្សាទុក និងការកសាងមជ្ឈមណ្ឌលស្រោចស្រង់ទិន្នន័យព័ត៌មានអេឡិចត្រូនិច (Back-Up) របស់រដ្ឋាភិបាល
- រៀបចំប្រព័ន្ធការពារសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន នៃហេដ្ឋារចនាសម្ព័ន្ធ ព័ត៌មានជាតិ (National Information Infrastructure - NII) ដើម្បីជានាបាននូវសន្តិសុខទិន្នន័យប្រកបដោយប្រសិទ្ធភាព គុណភាពសេវា និងនិរន្តភាព
- សិក្សា ពិនិត្យអំពីគុណភាព និងកំរិតសន្តិសុខ លើក្រុមហ៊ុនផ្តល់សេវាកម្មអ៊ីនធឺណិត (ISP) អ្នកបែងចែកសេវាអ៊ីនធឺណិត និងសេវាបច្ចេកវិទ្យា ព័ត៌មានវិទ្យា
- ចេញវិញ្ញាប័នប្រើតទទួលស្គាល់កំរិតនិយាមសន្តិសុខប្រព័ន្ធគ្រប់គ្រង ឲ្យក្រុមហ៊ុនផ្តល់សេវា អ៊ីនធឺណិត សេវាបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន ដើម្បីជានាប្រសិទ្ធភាព នៃប្រព័ន្ធដំណើរការ

បច្ចេកវិទ្យា ព័ត៌មានវិទ្យា និងទប់ស្កាត់វិធ្វេទកម្មលើវិស័យបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន ដែលអាចកើតមានឡើងជាយថាហេតុ

- សម្របសម្រួលជាមួយក្រសួង-ស្ថាប័នពាក់ព័ន្ធ និងដៃគូអភិវឌ្ឍន៍នានា ដើម្បីបង្កើតមជ្ឈមណ្ឌលគ្រប់គ្រង និងចេញវិញ្ញាប័នប័ត្រហេដ្ឋារចនាសម្ព័ន្ធគន្លឹះសាធារណៈដែលជាភាសាបច្ចេកទេសហៅថា Certificate Authority (CA)
- សម្របសម្រួលជាមួយក្រសួង-ស្ថាប័នពាក់ព័ន្ធ ដើម្បីបង្កើតមូលដ្ឋានទិន្នន័យព័ត៌មាន អេឡិចត្រូនិច ទាក់ទិននឹងការគ្រប់គ្រងកូដអាស័យដ្ឋានអ៊ីនធឺណិត (IP Address) ទាំងអស់ ដើម្បីឆ្លើយតបទៅនឹងការគំរាមគំហែងវិស័យសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មានរបស់រាជរដ្ឋាភិបាលប្រកបដោយប្រសិទ្ធភាព
- ពិនិត្យ តាមដានអំពីប្រសិទ្ធភាពនៃការប្រើប្រាស់បរិក្ខារអេឡិចត្រូនិច ឧបករណ៍បច្ចេកទេស សម្ភារៈកុំព្យូទ័រ (Hardware) កំរងកម្មវិធីកុំព្យូទ័រ (Software) និងបរិក្ខារព័ត៌មានវិទ្យា ដោយផ្អែកទៅលើមូលដ្ឋាននិយាមដែលបានចែង និងផ្អែករលើគោលនយោបាយសន្តិសុខ នៃការប្រើប្រាស់ប្រព័ន្ធ ព័ត៌មានវិទ្យា (Standard Operation Procedures)
- ត្រួតពិនិត្យ និងកំណត់និយាមសុវត្ថិភាព មុននឹងអនុញ្ញាតឲ្យស្ថាប័នណាមួយតភ្ជាប់ជាមួយ នឹងហេដ្ឋារចនាសម្ព័ន្ធ នៃបណ្តាញតភ្ជាប់ទំនាក់ទំនង របស់ អ.អ.ប.ត.ព
- សហការយ៉ាងជិតស្និទ្ធិជាមួយក្រសួង-ស្ថាប័នពាក់ព័ន្ធ ដើម្បីសិក្សាអំពីលទ្ធភាពនៃការលើកកម្ពស់តួនាទីចាំបាច់របស់ក្រុមការងារបច្ចេកទេសនេះ ដើម្បីឈានទៅរកការបង្កើតទៅជា គណៈកម្មាធិការជាតិគ្រប់គ្រងកិច្ចការសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន
- ធ្វើកិច្ចសហប្រតិបត្តិការជាមួយក្រសួង-ស្ថាប័នពាក់ព័ន្ធ ដើម្បីឈានដល់ការបង្កើតឲ្យមានមុខងារ នៃ ប្រធានមន្ត្រីបច្ចេកទេសព័ត៌មានវិទ្យា (Chief Information Officer - CIO) និងមុខងារ នៃមន្ត្រីបច្ចេកទេសព័ត៌មានវិទ្យា (Information Officer - IO) នៅតាមបណ្តាក្រសួង-ស្ថាប័ននានា
- រៀបចំរបាយការណ៍ស្តីពីសកម្មភាពការងាររបស់ខ្លួន ជូនអគ្គលេខាធិការ នៃ អ.អ.ប.ត.ព ជាប្រចាំ។

ប្រការ ៣៖ ប្រធានក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន ស្ថិតក្រោមការដឹកនាំគ្រប់គ្រង របស់អគ្គលេខាធិការ អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា (អ.អ.ប.ត.ព)។ ក្រុមការងារបច្ចេកទេសនេះមានជំនាញការបច្ចេកទេសជាតិ និងអន្តរជាតិមួយចំនួនជាជំនួយការគាមការចាំបាច់។

ប្រការ ៤៖ ប្រធានក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន មានការៈកិច្ច លើកសំណើជូនអគ្គលេខាធិការ នៃ អ.អ.ប.ត.ព ដើម្បីពិនិត្យ និងសម្រេច លើការចាត់តាំងការបន្ថែមមន្ត្រី ការផ្លាស់ប្តូរមន្ត្រី និងការបង្កើតផ្នែកផ្សេងៗក្នុងក្រុមការងារបច្ចេកទេសតាមការចាំបាច់។

ប្រការ ៥៖ ក្រុមការងារជាតិកម្ពុជាទប់ទល់នឹងបញ្ហាបន្ទាន់នៃកុំព្យូទ័រ ហៅជាភាសាអង់គ្លេសថា National Cambodia Computer Emergency Response Team (CamCERT) ដែលបានបង្កើតឡើងតាមសេចក្តីសម្រេចលេខ ១១៩ សសរ ចុះថ្ងៃទី ១៣ ខែធ្នូ ឆ្នាំ២០០៧ ស្ថិតក្រោមការគ្រប់គ្រងរបស់ក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន ។

ប្រការ ៦៖ អគ្គលេខាធិការ អគ្គលេខាធិការរង ប្រធានក្រុមការងារទាំងអស់ អស់លោក លោកស្រីដូចមានចែងក្នុងប្រការ១ ខាងលើក្រមទាំងមន្ត្រីរាជការពាក់ព័ន្ធទាំងអស់នៃ អ.អ.ប.ត.ព ត្រូវចូលរួមសហការអនុវត្តនូវសេចក្តីសម្រេចនេះឲ្យមានប្រសិទ្ធភាពខ្ពស់ចាប់ពីថ្ងៃចុះហត្ថលេខានេះតទៅ។

រាជធានីភ្នំពេញ ថ្ងៃទី ៩ ខែ ០៦ ឆ្នាំ២០០៩

នាយករដ្ឋមន្ត្រី

សុខ អាន

ចំលងជូន៖
- ឧត្តមក្រឡាបញ្ជីរដ្ឋមន្ត្រីនាយករដ្ឋមន្ត្រី
- ឧត្តមក្រឡាបញ្ជីឯកឧត្តមឧបនាយករដ្ឋមន្ត្រី រដ្ឋមន្ត្រីទទួលបន្ទុកទីស្តីការគណៈរដ្ឋមន្ត្រី
- ក្រសួងមហាផ្ទៃ
- ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍
- ក្រសួងព័ត៌មាន
- ក្រសួងយុត្តិធម៌
- ទូរគមនាគមន៍កម្ពុជា
- ក្រប់ក្រុមហ៊ុនផ្តល់សេវាកម្មអ៊ីនធឺណិត (ISP)
- សាមីខ្លួន "ដើម្បីអនុវត្ត"
- ឯកសារ-កាលប្បវត្តិ