ជំពូក ២

GISMS1.0 (ចេញផ្សាយនៅក្នុងខែធ្នូ ឆ្នាំ២០០៨)

ផ្នែក ទី១

គោលនយោបាយ នៃប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន

របស់ រាជរដ្ឋាភិបាល

គោលនយោបាយ នៃប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល

[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 និងជំបូន្មានផ្សេងៗ។
- ប្រធានគ្រប់គ្រងទាំងអស់មានភារកិច្ចទទួលខុសត្រូវ ដោយផ្ទាល់ចំពោះការអនុវត្តន៍គោលនយោបាយ និងធ្វើឲ្យបុគ្គលិកនៅក្នុងនាយកដ្ឋានរបស់ខ្លួនគោរពតាមគោលនយោបាយទាំងនេះ។
- ការគោរពតាមគោលនយោបាយ ស្តីអំពីសន្តិសុខព័ត៌មាននេះ គឺជាការកិច្ចចាំបាច់ដែលត្រូវអនុវត្ត។

អគ្គលេខាធិការដ្ឋាន អាជ្ញាធរជាតិឧទ្ធរណ៍កិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា

ផ្នែក ទី២

ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រង
សន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល

អាជ្ញាធរជាតិឧទ្ធលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា
គមនាគមន៍ ព័ត៌មានវិទ្យា

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

- កែសម្រួល និងរៀបរៀងដោយក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការ
សន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន

១.សេចក្តីផ្តើម

ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រដ្ឋាភិបាល (GISMS) ត្រូវបានកំណត់នូវលក្ខខណ្ឌដែលរាជរដ្ឋាភិបាលកម្ពុជាត្រូវបំពេញរួមមាន ការបង្កើត ការអនុវត្តន៍ ការត្រួតពិនិត្យ និងការចាត់វិធានការក្នុងនាមជា អង្គភាពទទួលបន្ទុកប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ស្ថិតក្នុងគោលនយោបាយស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GISMS) ដែលបានប្រកាសដោយនាយករដ្ឋមន្ត្រីដែលជាថ្នាក់ដឹកនាំរាជរដ្ឋាភិបាល។

២. ទិសាលភាព

ឯកសារណែនាំស្តីអំពី GISMS ត្រូវបានរៀបរៀងឡើង ដោយរួមបញ្ចូលនូវក្រសួងស្ថាប័ន 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 ឧត្តុនិយម

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 ដោយមានតួនាទីជាលេខាធិការ របស់គណៈកម្មាធិការនាយកផ្នែករបស់រាជរដ្ឋាភិបាល (GCIO) ហើយ អ.អ.ប.ត.ព ជាអង្គភាពដែលទទួលខុសត្រូវក្នុងការបំពេញតួនាទីរបស់ការិយាល័យ GIS នេះ។ ស្ថាប័ននេះទទួលខុសត្រូវក្នុងការបង្កើតគោលនយោបាយ បទដ្ឋាន និងសេចក្តីណែនាំរបស់ GISMS និងទទួលខុសត្រូវផែងដែរ ចំពោះការងារទាំងឡាយ ដែលពាក់ព័ន្ធនឹង GISMS នៅក្នុងរាជរដ្ឋាភិបាលកម្ពុជា។ *និយមន័យនេះ គឺជាសេចក្តីព្រាងប៉ុណ្ណោះ។*

ការឧបត្ថម្ភគាំទ្រសំរាប់ GCIO នឹងត្រូវបានចាត់ចែងនៅក្នុងគំរោងអភិវឌ្ឍន៍ GCIO។

- នាយកផ្នែកសន្តិសុខព័ត៌មាន (CISO)៖

មន្ត្រីម្នាក់នៃស្ថាប័ននីមួយៗ នឹងត្រូវតែងតាំងសំរាប់មុខងារនេះហើយទំនួលខុសត្រូវផ្សេងៗ ត្រូវបានកំណត់ដោយជាក់លាក់នៅក្នុង ឯកសារណែនាំស្តីអំពី GISMS និងឯកសារវិធានស្តីអំពីសន្តិសុខព័ត៌មាន។

- 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។ វាជាការប្រសើរបំផុតដែលសាមីស្ថាប័នត្រូវយកគំរូតាមឯកសារគំរូនេះ ក្នុងកំរិតមួយជាអប្បបរមា។

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។ ជំពូកនេះនឹងធ្វើការនិយាយអំពីជំណើរការការងាររបស់ 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 ស្ថាប័នមួយនេះត្រូវកំណត់នូវវិសាលភាពសំរាប់វដ្តនៃ PDCA ជាក់លាក់មួយ។ ជាទូទៅវាអាចប្រព្រឹត្តទៅបានចំពោះការកំណត់វិសាលភាពដោយយោងទៅលើសេវាកម្ម ឬបរិក្ខាររូបវន្តដូចជា ព្រំដី ឬអាគារជាដើម។ ការកំណត់វិសាលភាពនេះ ក៏អាចអនុវត្តទៅបានដោយយោងទៅលើបណ្តាញកុំព្យូទ័រប្រព័ន្ធព័ត៌មាន ដើម្បីកំណត់ឲ្យបាននូវការគ្រប់គ្រង និងដំណោះស្រាយប្រកបដោយប្រសិទ្ធិភាពទប់ទល់នឹងបញ្ហាគំរាមផ្សេងៗ។ សាមីស្ថាប័នក៏ត្រូវមានការប្រុងប្រយ័ត្នផងដែរ ចំពោះការកំណត់វិសាលភាព ដោយយោងទៅលើតារាងរចនាសម្ព័ន្ធដោយហេតុថា ការប្រព្រឹត្តបែបនេះ ពេលខ្លះនឹងធ្វើឲ្យការអនុវត្តជាក់ស្តែងមានការលំបាក។

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

<u>៤.១.៣. ការវាយតំលៃអំពីហានិភ័យ</u>

ដំណើរការនៃការវាយតំលៃអំពីហានិភ័យត្រូវបានចែកចេញជា ៥ ដំណាក់កាល រួមមាន៖

- ការកំណត់សំការៈព័ត៌មាន
- ការវាយតំលៃអំពីសំការៈព័ត៌មាន
- ការពិនិត្យមើលអំពីហានិភ័យដែលអាចនឹងកើតមាន
- ការវាយតំលៃអំពីហានិភ័យ
- ការកំណត់ហានិភ័យ ។

ដំណើរការលំអិតត្រូវបានកំណត់នៅក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ។ សូមមើលសេចក្តីណែនាំនៅក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ (ឧបសម្ព័ន្ធទី១៖ ឯកសារសំរាប់ ពិនិត្យមើលហានិភ័យ)។

<u>ដំណាក់កាលទី១៖ ការកំណត់សំការៈព័ត៌មាន</u>

ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ បានបញ្ចូលសំការៈព័ត៌មានចំនួន ៦ប្រភេទ ក្នុងនោះសំការៈព័ត៌មាន៤ប្រភេទរួមមាន សេវាកម្ម ឬបរិក្ខារកុំព្យូទ័រ ក្រដាសឯកសារ បណ្តាញកុំព្យូទ័រ និងម៉ាស៊ីនកុំព្យូទ័រមេ (Server) នឹងត្រូវ កំណត់ដោយនាយកដ្ឋាននីមួយៗ ដែលទទួលបន្ទុកពិនិត្យមើលដោយខ្លួនឯង។

<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 ឬមិនមានប្រតិបត្តិការហូតដល់២៤ ម៉ោង
A៣	៥.ខ្ពស់	៥		មិនដំណើរការ ឬមិនមានប្រតិបត្តិការហូតដល់៤ម៉ោង

លទ្ធផលចុងក្រោយនៃការវាយតំលៃ អំពីសំភារៈព័ត៌មានណាមួយឆ្លុះឲ្យឃើញតាមរយៈពិន្ទុសរុបទទួលបានពីចំនុចទាំងបី។ ប្រសិនបើលោកអ្នកគិតថា លទ្ធផលសរុបនៃការវាយតំលៃអំពីសំភារៈព័ត៌មានមានលក្ខណៈខុសពីការពិតជាក់ស្តែង សូមធ្វើការពិនិត្យ និងកែសម្រួលឡើងវិញ នូវចំនួនពិន្ទុ នៅក្នុងចំនុចវាយតំលៃទាំងបីនោះ។

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	សំភារៈព័ត៌មានមានផល់ប៉ះពាល់យ៉ាងខ្លាំងលើអកិបាលកិច្ច

<u>ដំណាក់កាលទី៣៖ ការពិនិត្យមើលអំពីសំភារៈព័ត៌មាន</u>

ក្នុងការពិនិត្យមើលអំពីសំភារៈព័ត៌មាន លោកអ្នកគ្រាន់តែជ្រើសរើសពាក្យបានអនុវត្ត ឬមិនបានអនុវត្ត សំរាប់ចំនុចត្រួតពិនិត្យនីមួយៗ។

(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