ផ្នែក ទី៣

ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន
របស់រាជរដ្ឋាភិបាល

អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា
គមនាគមន៍ ព័ត៌មានវិទ្យា

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

- កែសម្រួល និងរៀបរៀងដោយក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការ
សន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន

១. សេចក្តីផ្តើម

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

២. វិធានជាមូលដ្ឋានចីប្រតេចសំរាប់រក្សាសន្តិសុខព័ត៌មាន

[វិធានទី១] ជានិច្ចកាលត្រូវធ្វើការពិចារណាឲ្យបានជិតដល់ 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។

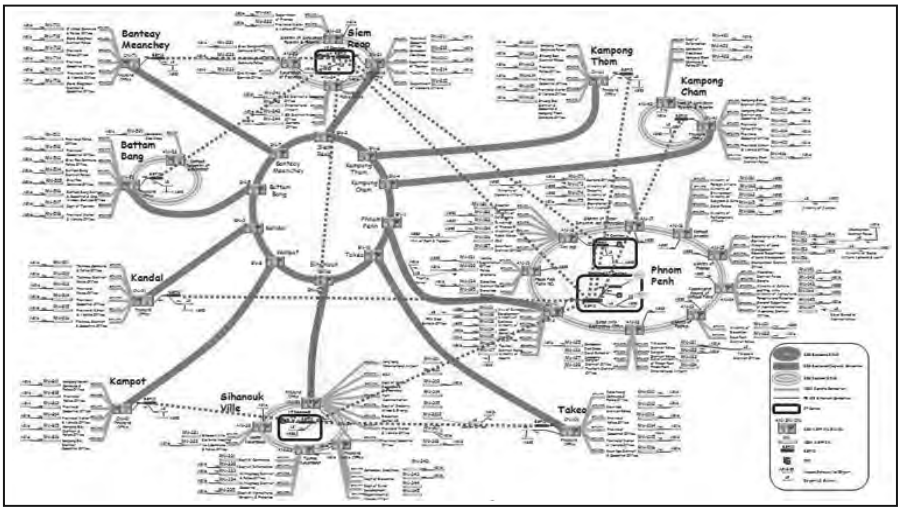
៣. វិសាលភាព

វិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ដែលមាននៅក្នុងឯកសារនេះ សំរាប់អនុវត្តនៅក្នុង អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍បច្ចេកវិទ្យា 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 ដោយធ្វើការតភ្ជាប់ជាលក្ខណៈបណ្តាញទៅតាមបណ្តា ខេត្ត-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)៖

វាជាប្រភេទកុំព្យូទ័រសំរាប់ប្រើប្រាស់ក្នុងការិយាល័យដូចជា កុំព្យូទ័រលើតុ កុំព្យូទ័រយួរដៃ ឬ កុំព្យូទ័រចល័ត។

ពាក្យដ៏ទៃទៀតត្រូវបានយោងទៅតាមពាក្យ និងនិយមន័យ 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៖

<u>នាយកផ្នែកសន្តិសុខព័ត៌មាន (CISO)</u>៖

មន្ត្រីមួយរូបនៅក្នុងក្រសួង ត្រូវបានចាត់តាំងឲ្យទទួលមុខដំណែងនេះ។ មន្ត្រីរូបនេះក៏ជាសមាជិកម្នាក់ នៃការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (GISO) ផងដែរ ដែលត្រូវបានកំណត់នៅក្នុងប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

<u>ប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន (IS Manager)</u>៖

មន្ត្រីមួយរូបនៅក្នុងនាយកដ្ឋាន ត្រូវបានចាត់តាំងឲ្យទទួលមុខដំណែងនេះ។ ការទទួលខុសត្រូវផ្សេងៗ ត្រូវបានកំណត់នៅក្នុងឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល និងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល។

<u>មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន (មន្ត្រីទទួលខុសត្រូវផ្នែក IS)</u>៖

មន្ត្រីមួយរូបនៅក្នុងនាយកដ្ឋានត្រូវបានចាត់តាំងឲ្យទទួលមុខដំណែងនេះ។ ការទទួលខុសត្រូវផ្សេងៗ ត្រូវបានកំណត់នៅក្នុងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

<u>មន្ត្រីធម្មតា</u>៖

សំដៅទៅលើនិយោជិតដ៏ទៃទៀតទាំងអស់ ដែលបិតនៅក្នុងក្របខ័ណ្ឌនៃអង្គភាព។

៥.២. <u>បញ្ជីសមាជិកការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន</u>

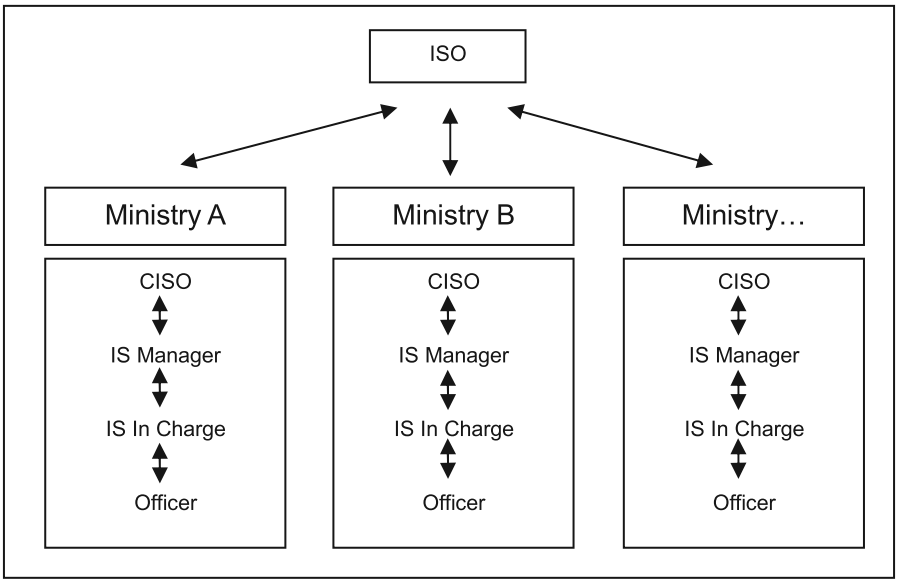
សមាសភាពមន្ត្រីការិយាល័យសុវត្ថិភាពព័ត៌មាន និងត្រូវតែងតាំងដោយអគ្គលេខាធិការ នៃអគ្គលេខាធិការដ្ឋាន អាជ្ញាធរជាតិ អ.អ.ប.ត.ព។

៥.៣. <u>បណ្តាញទំនាក់ទំនងសំរាប់គ្រាអាសន្ន</u>

បែបបទនៃការរាយការណ៍ ជាទូទៅត្រូវបានអនុវត្តតាមឋានានុក្រម គឺពីមន្ត្រីធម្មតា ទៅមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន ពីមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន ទៅប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងពីប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន ទៅការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន

ឬនាយកផ្នែកសន្តិសុខព័ត៌មាន។ ផ្ទុយទៅវិញ បែបបទនៃការផ្តល់ការណែនាំ គឺអនុវត្តពីការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ឬនាយកផ្នែកសន្តិសុខព័ត៌មាន ទៅប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន ពីប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន 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 សំរាប់តែក្នុងប្រតិបត្តិការការងាររបស់រាជរដ្ឋាភិបាលប៉ុណ្ណោះ។

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 និតិវិធី លើនិយោជិត</u> (នឹងត្រូវកំណត់នាពេលអនាគត**)**

(ក) ន័យធាន

(ផ្នែកនេះ នឹងធ្វើការកំណត់នូវតម្រូវការសន្តិសុខ ទាក់ទងនឹងការជ្រើសរើសនិយោជិត ដូចជាការពិនិត្យមើលអំពីគុណសម្បត្តិរបស់បេក្ខជន កំឡុងពេលជ្រើសរើសបុគ្គលិកថ្មី ការពិពណ៌នាអំពីការងារទាក់ទងនឹងបញ្ហាសន្តិសុខព័ត៌មាន និងតម្រូវការផ្សេងៗ នៅពេលបញ្ចប់ការជួលឲ្យបំរើការងារ)។

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

៦.៣.១. <u>អគារ និងបន្ទប់ការិយាល័យ</u>

(ក) វិធាន

(ក១) ត្រូវកំណត់នូវបុគ្គល ដែលមានសិទ្ធិចេញចូលអគារ ឬបន្ទប់។

(ក២) ត្រូវអនុវត្តនូវប្រព័ន្ធសម្ងាត់សមរម្យមួយ សំរាប់ការចេញចូលអគារ ឬបន្ទប់។

(ក៣) ត្រូវបែងចែកឲ្យដាច់រវាងការិយាល័យធ្វើការ និងទីកន្លែងដ៏ទៃទៀត ដែលសំរាប់ប្រើប្រាស់រួម។

(ក៤) ត្រូវចាត់បុគ្គលិកដែលមានការយល់ដឹងការងារផ្ទៃក្នុង ឲ្យអមភ្ញៀវដែលមកពីខាងក្រៅ។

ចំនុចព្យួរធុកបណ្តោះអាសន្ន

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៣.២. <u>ទូតម្កល់ឯកសារ និងតុធ្វើការ</u>

(ក) វិធាន

(ក១) ត្រូវរក្សាទុកសំភារៈព័ត៌មាន ដោយសម្ងាត់ក្នុងទូតម្កល់ឯកសារ ដែលបានចាក់សោត្រឹមត្រូវ។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៣.៣. <u>ម៉ាស៊ីនទូរសារ និងម៉ាស៊ីនបោះពុម្ព</u>

(ក) វិធាន

(ក១) ត្រូវបោះចោលដោយប្រុងប្រយ័ត្ន នូវឯកសារដែលបានបោះពុម្ព និងបញ្ជូនតាមទូរសារនានា។

(ក២) ត្រូវរក្សាទុកបញ្ជីព័ត៌មានស្តីអំពីការបញ្ជូនទូរសារ(ទៅ ឬមក)។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៤. <u>សន្តិសុខព័ត៌មានរូបវន្ត</u>

៦.៤.១. <u>ក្រដាសឯកសារ</u>

(ក) ខិឆាន

(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) ខិឆាន

(ក១) ជានិច្ចកាល ត្រូវធ្វើការកំណត់អំពីព័ត៌មានសម្ងាត់ ដោយប្រុងប្រយ័ត្ននៅក្នុងឧបករណ៍ផ្ទុកឯកសារនីមួយៗ។

(ក២) ត្រូវរក្សាទុកឧបករណ៍ផ្ទុកឯកសារសម្ងាត់ទាំងនេះ នៅកន្លែងសន្តិសុខមួយ ដើម្បីជៀស