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

លទ្ធផលសរុបនៃការវាយតំលៃអំពីហានិភ័យ ត្រូវបានកំណត់ដោយយោងទៅតាមការគណនាខាងក្រោម៖

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 ដែលត្រូវបានវាយតំលៃថា មានហានិភ័យ «ខ្ពស់» គួរត្រូវបានគ្រប់គ្រងដោយម៉ត់ចត់។ ជាទូទៅស្តាប់ទាំងឡាយត្រូវអនុវត្តតាមវិធាននិងនីតិវិធីនានា ដើម្បីកាត់បន្ថយហានិភ័យទាំងនេះ។ ការប្រព្រឹត្តបែបនេះនាំឲ្យយើងអាចបង្កើតបាន នូវឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន សំរាប់រាជរដ្ឋាភិបាល។ បន្ទាប់ពីបានកំណត់ការគ្រប់គ្រង និងដោះស្រាយរាល់បញ្ហាទាក់ទងនឹងហានិភ័យរួចមក សូមធ្វើការវាយតំលៃអំពីហានិភ័យទាំងនេះម្តងទៀត ដើម្បីឲ្យប្រាកដថា រាល់ចំនុចត្រួតពិនិត្យទាំងអស់ ត្រូវបានវាយតំលៃក្នុងកំរិតមួយ «ទាប» (ឧទាហរណ៍៖ ធ្វើការកំណត់វិធាន និងនីតិវិធីនៅក្នុងឯកសារវិធានស្តីពី GIS)។

៤.១.៤. <u>ការបង្កើតឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល</u>

ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ត្រូវបានចងក្រងដោយស្តាប់ននីមួយៗ។ យោងតាមលទ្ធផលនៃការវាយតំលៃអំពីហានិភ័យដំណោះស្រាយដ៏ចម្បងនោះ គឺការកំណត់វិធាននិងនីតិវិធី ដើម្បីកាត់បន្ថយហានិភ័យដែលកើតឡើង។ ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលត្រូវបានចែកចេញជាប្រាំផ្នែកគឺ៖

១)វិសាលភាព ជាផ្នែកដែលត្រូវបានកំណត់នៅក្នុងចំនុចទី ៤.១.២ ស្តីអំពីការកំណត់វិសាលភាពនៃ GISMS

២) ការរៀបចំសន្តិសុខព័ត៌មាន

៣) វិធាន និងនីតិវិធី

៤) ការបណ្តុះបណ្តាលស្តីអំពីសន្តិសុខព័ត៌មាន

៥) ការប៉ាន់ប្រមាណអំពីកំរិតនៃការត្រួតពិនិត្យ និងការអនុវត្តន៍។

ស្ថាប័ននីមួយៗត្រូវបានតម្រូវឲ្យប្រើប្រាស់ ឯកសារវិធានគំរូអំពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ផ្តល់ជូនដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មារបស់រាជរដ្ឋាភិបាល ដែលតួនាទីរបស់ការិយាល័យនេះ នឹងត្រូវបានរៀបរាប់នៅក្នុងជំពូកទី៥ ស្តីអំពីទំនួលខុសត្រូវក្នុងការគ្រប់គ្រង។ ដំណាក់កាលចំនួនបីខាងក្រោមពន្យល់អំពីគន្លឹះក្នុងការចងក្រងឯកសារវិធានស្តីអំពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

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

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

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

នៅក្នុងវិសាលភាពនៃស្ថាប័ននីមួយៗ វិធាននិងនីតិវិធីនានា អាស្រ័យទៅលើសំភារៈព័ត៌មានជាក់ស្តែងនិងការសម្ងាត់របស់ពួកគេ។ វាមិនមានកាចាំបាច់

ក្នុងការកំណត់វិធាននិងនីតិវិធីទាំងនេះទេ លើកលែងតែមានសំការៈព័ត៌មានជាក់លាក់ ដែលបានរួមបញ្ចូលនៅក្នុងវិសាលភាពនេះ។

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

វិធាននិងនីតិវិធីទាំងនេះ គួរត្រូវបានកំណត់ថា «មានសន្តិសុខជាងមុន» ប្រសិនបើព័ត៌មានដែលបានប្រើប្រាស់នៅក្នុងស្ថាប័នមួយ កាន់តែមានលក្ខណៈសម្ងាត់ ដោយយោងទៅតាមលទ្ធផលនៃការវាយតំលៃអំពីហានិភ័យ។ ប្រសិនបើឯកសារវិធានគំរូពុំមានសំការៈព័ត៌មាន ដែលបានបញ្ចូលទៅក្នុងវិសាលភាពនោះទេ សូមសរសេរថា វិធាននិងនីតិវិធីទាំងនេះ «នឹងត្រូវបានកំណត់»។ ក្នុងករណីនេះវាជាប្រការសំខាន់មួយ ដែលត្រូវពិភាក្សាជាមួយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល មុននឹងចាប់ផ្តើមកំណត់វិធាននិងនីតិវិធីនានា ដើម្បីធ្វើការសម្រេចអំពីអ្នក ដែលនឹងត្រូវបង្កើតបទដ្ឋាននៃសំការៈព័ត៌មានថ្មីរបស់រាជរដ្ឋាភិបាលកម្ពុជា ដែលត្រូវបញ្ចូលទៅក្នុងវិសាលភាព។

៤.១.៥. <u>ការស្នើសុំការអនុម័ត</u>

ការផ្តល់ការអនុម័តត្រូវបានចែកចេញជាពីរដំណាក់កាល៖

- ការអនុម័តដោយថ្នាក់ដឹកនាំកំពូលនៃស្ថាប័ន
- ការអនុម័តដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

នៅពេលដែលដំណាក់កាលទាំងពីរដូចបានរៀបរាប់ពីចំនុច ៤.១.១ ដល់ចំនុច ៤.១.៤ ត្រូវបានបញ្ចប់ និងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ដែលក្នុងនោះស្តីអំពី ការតែងតាំងអ្នកគ្រប់គ្រង CISO និង IS ត្រូវបានចងក្រងរួចរាល់ ជំណើរការរៀបចំផែនការ និងឯកសារទាំងនេះគួរត្រូវបាន

ពិនិត្យឡើងវិញ និងទទួលបានការអនុម័តពីការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលជាមុនសិន ដើម្បីឲ្យប្រាកដថាពួកវាត្រូវបានបង្កើតឡើងដោយស្របទៅតាមគោលការណ៍របស់ GISMS។

ឆ្លងតាមការវាយតំលៃដោយស្វ័យប្រវត្តិ នៅក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ មានករណីលើកលែងមួយ ដែលអនុញ្ញាតឲ្យមានការទទួលយកហានិភ័យ ដែលមិនធ្លាប់ជួបប្រទះ ទោះបីជាវាស្ថិតនៅក្នុងកំរិតមួយដែលហួសពីការដែលអាចទទួលយកបាន នេះជាហេតុផលចាំបាច់ច្បាស់លាស់ និងដ៏ត្រឹមត្រូវមួយក្នុងការសម្រេចចិត្ត ដើម្បីទទួលបាននូវការអនុម័តពីការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

ការទទួលបានការអនុម័តពីថ្នាក់ដឹកនាំកំពូលនៃស្ថាប័ន គឺជាការចាំបាច់បំផុតសំរាប់ការអនុវត្តន៍ការងារនៅក្នុងស្ថាប័នឲ្យបានពេញលេញ និងប្រកបដោយប្រសិទ្ធិភាព។

៤.២. <u>ការអនុវត្តន៍ និងប្រតិបត្តិការ</u>

នៅពេលអនុវត្ត GISMS នៅក្នុងស្ថាប័នមួយ ត្រូវបង្កើតការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដោយនាយកផ្នែកនេះត្រូវធ្វើការចាត់តាំងសមាជិកមួយចំនួនសំរាប់ការិយាល័គ្រប់គ្រងសន្តិសុខព័ត៌មាននោះ ដើម្បីរៀបចំ និងផ្តល់ការបណ្តុះបណ្តាល។

ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន គឺជាប្រព័ន្ធ «គ្រប់គ្រង» មួយ ហេតុដូចនេះមន្ត្រីដែលមានឋានៈខ្ពស់ជាងគួរត្រូវបានបណ្តុះបណ្តាលមុនគេ ដើម្បីឲ្យពួកគាត់មានចំណេះដឹង ទាក់ទងនិងប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងអាចដឹកនាំមន្ត្រីក្រោមឪវាទក្នុងការអនុវត្តន៍ប្រព័ន្ធនេះ។

៤.៣. <u>ការតាមដាន និងពិនិត្យមើលឡើងវិញ</u>

ដើម្បីឲ្យការប្រើប្រាស់ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានចាក់គ្រឹះទៅក្នុងអង្គភាពរដ្ឋ យើងត្រូវធ្វើដំណើរនៅលើផ្លូវដ៏វែងឆ្ងាយមួយជាចាំបាច់ ក្នុងការខិតខំប្រឹងប្រែងនិងកែលំអជាបន្ត

បន្ទាប់។ ដើម្បីយល់អំពីគោលដៅ និងពិភាក្សាអំពីការកែលំអនានា វាត្រូវការនូវឧបករណ៍សំរាប់វាស់កំរិតការងារទាំងនេះ ដែលនឹងត្រូវបានកំណត់នៅក្នុងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

- ការធ្វើសវនកម្មផ្ទៃក្នុង ដើម្បីអង្កេតអំពីប្រសិទ្ធិភាពនៃប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានដែលបានអនុវត្ត ក៏ត្រូវបានស្នើឡើងដើម្បីស្វែងរកបញ្ហានានាសំរាប់ការកំណត់កំរិតនៃហានិភ័យ ក្នុងដំណើរការរៀបចំផែនការ និង/ឬ សំរាប់ពិនិត្យឡើងវិញនូវកំរិតហានិភ័យដែលអាចទទួលយកបាន។
- លទ្ធផលថ្មីៗនៃការវាយតំលៃអំពីហានិភ័យ គួរត្រូវបានបញ្ចូលទៅក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ។
- ចំនួនដងនៃការត្រួតពិនិត្យ និងសកម្មភាពអនុវត្តន៍គួរត្រូវបានកំណត់នៅក្នុងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។
- សកម្មភាពទាំងនេះគួរតែត្រូវបានអនុវត្តយ៉ាងហោចណាស់លើសពីមួយដងក្នុងមួយឆ្នាំ។

៤.៤. <u>ធ្វើការថែទាំ និងលើកកំពស់</u>

លទ្ធផលនៃការវាស់កំរិត និងការធ្វើសវនកម្មផ្ទៃក្នុងការងារ នាំឲ្យយើងអាចធ្វើការសម្រេចចិត្តអំពីសកម្មភាពនានា ដើម្បីលើកកំពស់ប្រសិទ្ធិភាពនៃប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងជៀសវាងពីហានិភ័យនានា។ សកម្មភាពទាំងនេះមិនត្រឹមតែជួយបង្កើនប្រសិទ្ធភាពនៃវិធាននិងនិតិវិធីនានាប៉ុណ្ណោះទេ ពួកវាថែមទាំងជួយផ្តល់ដំណោះស្រាយក្នុងការដំឡើងកម្មវិធី និងឧបករណ៍ផ្នែករឹងកុំព្យូទ័រ សំរាប់ការពារបណ្តាញកុំព្យូទ័រ ឬប្រព័ន្ធផងដែរ។ សកម្មភាពទាំងនេះ ក៏អាចរួមបញ្ចូលនូវការលុបបំបាត់វិធាននិងនីតិវិធីមួយចំនួន ដើម្បីតម្រូវទៅនឹងបំលាស់ប្តូរតួនាទី និងប្រតិបត្តិការការងារនៃស្ថាប័ននីមួយៗ។

៤.៥. ការគ្រប់គ្រងឯកសារ

ផ្នែកនេះនឹងធ្វើការកំណត់ឮអំពី រចនាសម្ព័ន្ធ ការអនុញ្ញាត ការកែសម្រួល ការចែកចាយ លទ្ធកម្ម និងការរក្សាទុកឯកសារ។

៤.៥.១. រចនាសម្ព័ន្ធឯកសារ និងការអនុញ្ញាត

ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល មានឯកសារសំខាន់ៗចំនួន បួនប្រភេទគឺ៖

១) គោលនយោបាយស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល

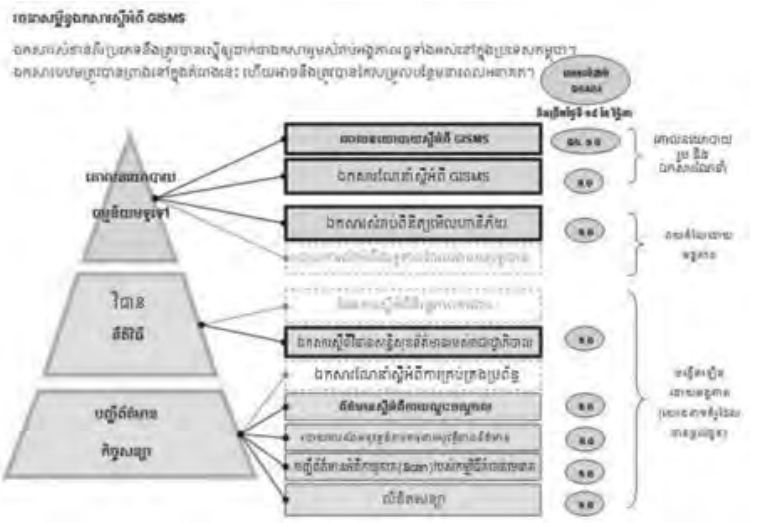
២) ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល

ឯកសារទាំងនេះត្រូវបានធ្វើសេចក្តីព្រាង ដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ពិនិត្យឡើងវិញដោយគណៈកម្មាធិការនាយកផ្នែកព័ត៌មានរបស់រាជរដ្ឋាភិបាល (ជាឈ្មោះបណ្តោះអាសន្នរហូតទាល់តែមានឈ្មោះជាផ្លូវការមួយត្រូវបានបង្កើតឡើងសំរាប់ជំនួស) និងផ្តល់ការអនុញ្ញាតដោយប្រធាន GCIO (ជាឈ្មោះបណ្តោះអាសន្ន)។ គោលនយោបាយស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល គួរត្រូវបានប្រកាសដោយប្រមុខនៃរាជរដ្ឋាភិបាលកម្ពុជា។ *ឯកសារបឋមលេខ ១.០ ត្រូវបានចងក្រងជាលើកទីមួយ ដោយ អ.អ.ប.គ.ព ក្រោមការឧបត្ថម្ភគាំទ្រដោយ JICA។*

៣) ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ

ចំនុចត្រួតពិនិត្យ ត្រូវបានព្រាងដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន

របស់រាជរដ្ឋាភិបាលពិនិត្យឡើងវិញ និងផ្តល់ការអនុញ្ញាតដោយគណៈកម្មាធិការ GCIO (ជាឈ្មោះបណ្តោះអាសន្នរហូតទាល់តែមានឈ្មោះជាផ្លូវការមួយត្រូវបានបង្កើតឡើងជំនួស)។ ឯកសារមិនទាន់បំពេញព័ត៌មានក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ ផ្តល់នូវចំលើយជ្រើសរើសជាស្រេចសំរាប់ការវាយតំលៃអំពីហានិភ័យ ហើយឯកសារដែលបានបំពេញរួចទាំងនេះ នឹងត្រូវបានវាយតំលៃ និងកែតម្រូវដោយសាមីស្តាប័ន។ សូមបំពេញឈ្មោះស្តាប័ននៅក្នុងឯកសារទាំងនេះបន្ទាប់ពីបានវាយតំលៃរួច។



៤) ឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល

ឯកសារនេះត្រូវបានចងក្រងដោយស្តាប័ននីមួយៗ។ ឯកសារវិធានគំរូមួយស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ត្រូវបានធ្វើសេចក្តីព្រាងដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ដោយយោងទៅតាមចំលើយជ្រើសរើសសំរាប់វាយតំលៃ អំពីហានិភ័យពីឯកសារមិនទាន់បំពេញ

ព័ត៌មាន ក្នុងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ។ ការចងក្រងឯកសារនេះគួរត្រូវបានទទួលការអនុញ្ញាតដោយថ្នាក់ដឹកនាំស្ថាប័ន។ សូមបញ្ចូលឈ្មោះស្ថាប័ននីមួយៗទៅក្នុងឯកសារនេះ។ ឯកសារបន្ថែមដ៏ទៃទៀតត្រូវបានបង្កើត និងប្រើប្រាស់ដោយស្ថាប័ននីមួយៗ។

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

<u>ការកែសម្រួល</u>

គោលនយោបាយស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល គួរត្រូវបានប្រកាសដោយប្រមុខនៃរាជរដ្ឋាភិបាលកម្ពុជា។ ដូច្នេះបែបបទនៃការកែសម្រួលត្រូវកំណត់ដោយវិធានដ៏ទៃទៀត ដែលបង្កើតឡើងដោយរាជរដ្ឋាភិបាលកម្ពុជា។ (បញ្ហានេះគួរត្រូវកំណត់ក្នុងក្រិតមួយជាក់លាក់នាពេលអនាគត) ឯកសារណែនាំស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល និងឯកសារសំរាប់ពិនិត្យមើលហានិភ័យត្រូវបានកែសម្រួលជារៀងរាល់ឆ្នាំ ដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល យោងទៅតាមមតិយោបល់ ឬសំណើរសុំពីស្ថាប័ននានាដែលនឹងកំពុងអនុវត្តប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន។ ឯកសារព្រាងទាំងនេះត្រូវបានផ្តល់ការអនុញ្ញាតដោយយោងតាមបែបបទដូចគ្នា ដូចបានកំណត់នៅក្នុងចំនុចទី ៤.៥.១ ស្តីអំពីរចនាសម្ព័ន្ធឯកសារ និងការផ្តល់ការអនុញ្ញាត។

ការកែសម្រួលឯកសារដ៏ទៃទៀត ទាក់ទងនឹងប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ត្រូវបានកំណត់ដោយស្ថាប័ននីមួយៗ ដោយយោងទៅតាមវដ្តដូចបានរៀបរាប់នៅក្នុងចំនុចទី ៤.៣ ស្តីអំពីការត្រួតពិនិត្យ និងចំនុចទី ៤.៤ (សកម្មភាពអនុវត្តន៍)។

ឯកសារណែនាំ ស្តីអំពីប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល

ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ និងឯកសារវិធានស្តីពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ត្រូវមានប្រវត្តិនៃការកែសម្រួល ដើម្បីឲ្យដឹងប្រាកដថា មួយណាដែលអ្នកអានយកជាឯកសារយោង។

<u>ការចែកចាយ លទ្ធកម្ម និងការរក្សាទុក</u>

កំរិតនៃភាពសម្ងាត់របស់ឯកសារទាក់ទងនឹងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលមានការ ប្រែប្រួល ទៅតាមឯកសារនីមួយៗ ដូចបានកំណត់ខាងក្រោម៖

១. គោលនយោបាយ និងឯកសារណែនាំស្តីអំពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ត្រូវបានចាត់ទុកជាឯកសារ «សាធារណៈ» ដែលមានន័យថា ឯកសារទាំងនេះអាចនឹងត្រូវបានបោះពុម្ពផ្សាយ ហើយប្រជាពលរដ្ឋកម្ពុជាទាំងអស់អាចរកអានបានដោយសេរី។

២. ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ ដែលមិនទាន់បានវាយតំលៃ មានកត់ត្រានូវហានិភ័យដែលមិនទាន់បានកំណត់ក្នុងស្តាប់ននីមួយៗ ហើយវាត្រូវបានចាត់ទុកជាឯកសារ «សាធារណៈ» ។ ឯកសារដែលបានវាយតំលៃរួចមានកត់ត្រានូវហានិភ័យដែលបានកំណត់ជាក់លាក់ (ដូចជាបញ្ហាគំរាម និងភាពងាយទទួលរងនូវផលប៉ះពាល់)។ ដូចនេះ វាត្រូវបានចាត់ទុកជាឯកសារ «ផ្ទៃក្នុង» ដែលតម្រូវឲ្យមានការប្រុងប្រយ័ត្នក្នុងការចែកចាយ លទ្ធកម្ម និងការរក្សាទុក និងសំរាប់ប្រើប្រាស់តែក្នុងប្រតិបត្តិការការងាររបស់រាជរដ្ឋាភិបាលប៉ុណ្ណោះ ។

៣. ឯកសារវិធានស្តីពី GIS រួមមាននូវវិធាននិងនីតិវិធីការងារផ្ទៃក្នុង ហើយវាត្រូវបានចាត់ទុកជាឯកសារ «ផ្ទៃក្នុង» ។