ត្រូវបញ្ជូនវិធានចំលងនៃឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ ឯកសារវិធានស្តីអំពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ដែលបានកែសម្រួលនិងវាយតំលៃរួច និងឯកសារមិនទាន់បំពេញព័ត៌មាន ទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល និងរក្សាទុកឯកសារទាំងនេះរយៈពេលប្រាំឆ្នាំ។

ការចែកចាយលទ្ធកម្ម និងការរក្សាទុកឯកសារដ៏ទៃទៀតត្រូវបានកំណត់ដោយស្តាប់ននីមួយៗ វាជាការសំខាន់ ដែលត្រូវមានការប្រុងប្រយ័ត្នខ្ពស់ក្នុងការទុកដាក់ឯកសារដែលមានផ្ទុកនូវព័ត៌មានសម្ងាត់ (ដូចជា IP address របស់ម៉ាស៊ីនកុំព្យូទ័រមេ (Server) និងព័ត៌មានផ្ទាល់ខ្លួនជាដើម)។

៤.៦. <u>ការគ្រប់គ្រងបញ្ជីព័ត៌មាន</u>

វាជាការចាំបាច់ដែលត្រូវគ្រប់គ្រងបញ្ជីព័ត៌មាន (Records) សំរាប់ការអនុវត្តន៍តាមវិធាននិងនីតិវិធីនានា។ ការគ្រប់គ្រងលើការអនុញ្ញាតការកែសម្រួលការចែកចាយលទ្ធកម្ម និងការរក្សាទុកឯកសារមិនទាន់បំពេញព័ត៌មាន អាចត្រូវបានកំណត់ នៅក្នុងឯកសារវិធានស្តីអំពីសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល។

ជាទូទៅ បញ្ជីព័ត៌មានត្រូវបានបញ្ជូនដោយមន្ត្រីដែលបានចាត់តាំង ត្រូវតម្កល់ និងបំរុងទុកដោយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន។ សូមរក្សាការចុះលំដាប់លេខរៀង លើកំណត់ត្រាព័ត៌មាននីមួយៗ ដោយប្រើប្រាស់លេខសំគាល់ដាច់ដោយឡែកពីគ្នា។ រយៈពេលកំណត់ សំរាប់ការរក្សាទុកបញ្ជីព័ត៌មានទាំងនេះគឺមួយឆ្នាំ និងប្រែប្រួលទៅតាមការកំណត់ដាក់ស្តែង។

បញ្ជីព័ត៌មានតែងតែផ្ទុកនូវព័ត៌មានសម្ងាត់ដូចជា IP Address របស់ម៉ាស៊ីនកុំព្យូទ័រមេ (Server) និងព័ត៌មានផ្ទាល់ខ្លួនជាដើម ដែលតម្រូវឲ្យមានការរក្សាទុកដោយយកចិត្តទុកដាក់

និងប្រុងប្រយ័ត្ន។

៥. ធំនួលខុសត្រូវក្នុងការងារគ្រប់គ្រង

៥.១. <u>កិច្ចប្រឹងប្រែងក្នុងការងារគ្រប់គ្រង</u>

តាមរយៈសេចក្តីប្រកាសស្តី អំពីគោលនយោបាយរបស់ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន របស់រាជរដ្ឋាភិបាល ថ្នាក់ដឹកនាំរាជរដ្ឋាភិបាលកម្ពុជាមាននាទីទទួលខុសត្រូវក្នុងការបង្កើតការ អនុវត្តន៍ ការតាមដាន និងការថែទាំប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដើម្បីរក្សាឲ្យបាននូវ និរន្តរភាពផ្នែករដ្ឋបាល នៃរាជរដ្ឋាភិបាលកម្ពុជា និងដើម្បីកាត់បន្ថយហានិភ័យនៃការខូចខាត តាមរយៈការបង្ការនូវឧប្បត្តិហេតុផ្សេងៗ និងតាមរយៈការកាត់បន្ថយ ផលប៉ះពាល់នៃឧប្បត្តិ ហេតុទាំងនេះដែលអាចនឹងកើតមានឡើង។ ថ្នាក់ដឹកនាំនៅតាមនាយកដ្ឋាននីមួយៗ មាននាទី ទទួលខុសត្រូវដោយផ្ទាល់ចំពោះការអនុវត្តប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងជាពិសេស ចំពោះការធ្វើឲ្យបុគ្គលិកក្រោមឱវាទទាំងអស់អនុវត្តតាម។

៥.២. <u>អង្គភាពការពារសន្តិសុខព័ត៌មានវិទ្យារបស់រាជរដ្ឋាភិបាល</u>

គ្រប់ស្ថាប័នទាំងអស់របស់រាជរដ្ឋាភិបាលកម្ពុជាត្រូវតែងតាំង នាយកផ្នែកព័ត៌មានរបស់ រាជរដ្ឋាភិបាល (GCIO) សំរាប់ស្ថាប័នរបស់ខ្លួន។ ប្រមុខរាជរដ្ឋាភិបាលកម្ពុជាត្រូវបង្កើត គណៈកម្មាធិការនាយកផ្នែកព័ត៌មានរបស់រាជរដ្ឋាភិបាល (គណៈកម្មាធិការ GCIO)។ ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល (ការិយាល័យ GIS) ត្រូវបាន បង្កើតឡើង ដោយមានតួនាទីជាលេខាធិការ របស់គណៈកម្មាធិការនាយកផ្នែកព័ត៌មានរបស់ រាជរដ្ឋាភិបាល (GCIO) ហើយអ.អ.ប.គ.ពទទួលខុសត្រូវក្នុងការបំពេញទួនាទីជាការិយាល័យ គ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាលនេះ។ *សូមបញ្ជាក់ថាការកំណត់នេះគឺជាសេចក្តី ព្រាងប៉ុណ្ណោះ។ ការឧបត្ថម្ភគាំទ្រសំរាប់ GCIO នឹងត្រូវបានចាត់ចែងនៅក្នុងគំរោងអភិវឌ្ឍន៍*

GCIO។

ថ្នាក់ដឹកនាំរបស់អង្គភាពរដ្ឋនីមួយៗ ត្រូវតែងតាំងនាយកផ្នែកសន្តិសុខព័ត៌មាន (CISO) ដែលទទួលបានសិទ្ធិបង្កើតនូវការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន។

៥.៣. <u>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

៥.៤. <u>ការពិនិត្យមើលអំពីការគ្រប់គ្រង</u>

GCIO ត្រូវបានតម្រូវឲ្យពិនិត្យឡើងវិញ រាល់ដំណើរការទាំងអស់នៃ GISMS របស់អង្គភាពរដ្ឋនានា ហើយការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ត្រូវបានអនុញ្ញាតឲ្យដាក់សំណើរ ទៅកាន់អង្គភាពរដ្ឋទាំងអស់ឲ្យរាយការណ៍អំពីស្ថានភាព GISMS របស់ពួកគេ។

ការិយាល័យរបស់ CISO និងការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន នៅតាមអង្គភាពរដ្ឋនីមួយៗ ត្រូវបានតម្រូវឲ្យធ្វើប្រតិបត្តិការដូចគ្នាក្នុងការងារពិនិត្យឡើងវិញរាល់ដំណើរការនៃ GISMS ដែលជាការបំពេញនូវតម្រូវការនានា របស់ការិយាល័យ GIS និងចំនុចទី ៤.៣ ស្តីអំពីការត្រួតពិនិត្យ (ធ្វើការតាមដាន និងពិនិត្យមើលឡើងវិញ)។

៦. ការគ្រប់គ្រង និងដំណោះស្រាយ

៦.១. <u>ប្រភេទនៃការគ្រប់គ្រង</u>

ការគ្រប់គ្រងត្រូវបានចែកជាបួនផ្នែករួមមាន ការកាត់បន្ថយហានិភ័យ ការផ្ទេរហានិភ័យ ការចៀសវាងហានិភ័យ និងការទទួលយកហានិភ័យ (ដោយចេតនានិងតាមតថភាពជាក់ស្តែង)។

ការកាត់បន្ថយហានិភ័យ គឺជាចំណាត់ការក្នុងការគ្រប់គ្រងដ៏សំខាន់មួយប្រឆាំងនឹងហានិភ័យដែលបានរកឃើញ។ ឧទាហរណ៍កុំព្យូទ័រមួយគ្រឿងដែលងាយទទួលរងនូវការវាយលុកដោយមេរោគ ត្រូវដំឡើងនិងប្រតិបត្តិការកម្មវិធីប្រឆាំងមេរោគ ដែលជាវិធានការមួយក្នុងការគ្រប់គ្រង។

ការផ្ទេរហានិភ័យ គឺជាវិធានការគ្រប់គ្រងមួយដែលអាចអនុវត្តបានតាមបែបផ្ទៀបាល។ ឧបមាថាកុំព្យូទ័រមួយគ្រឿងផ្ទុកនូវព័ត៌មានដ៏មានតំលៃ ហើយវាងាយទទួលរងនូវគ្រោះថ្នាក់អគ្គីភ័យ ដូច្នេះការចំលងទិន្នន័យបំរុងទុក (Data Backup) នៅទីកន្លែងដាច់ដោយឡែកមួយ គឺជាវិធានការគ្រប់គ្រងមួយ ដែលមានលក្ខណៈជាការកាត់បន្ថយហានិភ័យ។ ការទិញប័ណ្ណធានារ៉ាប់រងអគ្គីភ័យ និងការធានាការខូចខាតនៃទិន្នន័យដែលបាត់បង់ គឺជាការគ្រប់គ្រងតាមរយៈការផ្ទេរហានិភ័យ។

ការជៀសវាងហានិភ័យ គឺជាជម្រើសមួយទៀតក្នុងការបំបាត់នូវប្រភពនៃហានិភ័យ។ ជាក់ស្តែងការស្រាវជ្រាវពីមុនៗ បានប្រមែប្រមូលនូវព័ត៌មានសម្ងាត់ជាច្រើន ដែលមិនទាក់ទងនឹងការងារសំខាន់ៗ ហើយងាយនឹងធ្លាយចេញទៅខាងក្រៅ ដូច្នេះការលុបបំបាត់នូវព័ត៌មានទាំងនេះប្រកបដោយសន្តិសុខ គឺជាវិធានគ្រប់គ្រងមួយក្នុងការចៀសវាងនូវហានិភ័យ។

ការទទួលយកហានិភ័យដោយចេតនា និងតាមភាពជាក់ស្តែង គឺជាជម្រើសចុងក្រោយ។ ឧទាហរណ៍ជាទូទៅយើងត្រូវបង្កើតប្រព័ន្ធការពារសុវត្ថិភាពបណ្តាញកុំព្យូទ័រ (Firewall) ដើម្បីការពារសន្តិសុខបណ្តាញកុំព្យូទ័រខាងក្នុង (LAN) ក្នុងខណៈដែលម៉ាស៊ីនកុំព្យូទ័រមេគេហទំព័រ (Web Server) សំរាប់អ្នកប្រើប្រាស់ខាងក្រៅ ត្រូវបានបង្កើតឡើងដោយស្ថិតនៅក្រៅ ប្រព័ន្ធការពារសុវត្ថិភាពបណ្តាញកុំព្យូទ័រ (Firewall)។ វាជាករណីដែលអាចទទួលយកបាន ចំពោះម៉ាស៊ីនកុំព្យូទ័រមេ គេហទំព័រ (Web Server) លើបណ្តាញអ៊ីនធឺណិតដែលងាយទទួលរងការវាយលុកពីខាងក្រៅ ទោះបីវាត្រូវការនូវកិច្ចប្រឹងប្រែងមួយចំនួន សំរាប់ការជួសជុលឡើងវិញក្តីនៅពេលដែលមានការវាយលុកកើតឡើង។ ការទទួលយកហានិភ័យគួរត្រូវបានគ្រប់គ្រងដោយប្រុងប្រយ័ត្ន និងតែងតែទាមទារនូវការពិនិត្យឡើងវិញ និងការផ្តល់ការអនុញ្ញាតពីថ្នាក់ដឹកនាំកំពូល។

៦.២. <u>ការគ្រប់គ្រង និងដំណោះស្រាយតាមរយៈសំភារៈព័ត៌មាន</u>

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

ឧបសម្ព័ន្ធទី១៖ សេចក្តីណែនាំអំពីការពិនិត្យមើលហានិភ័យ

សេចក្តីណែនាំរបស់ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យ	
ឯកសារសំរាប់ពិនិត្យមើលហានិភ័យត្រូវបានប្រើប្រាស់នៅក្នុងដំណាក់កាលរៀបចំផែនការ GISMS ។ សូមធ្វើតាមសេចក្តីណែនាំខាងក្រោមជាដំណាក់ៗ៖	
ដំណាក់កាលទី ១	ធ្វើការកំណត់អត្តសញ្ញាណរបស់សំភារៈព័ត៌មាន។
ដំណាក់កាលទី ១.១	សូមពិនិត្យមើលសំភារៈព័ត៌មានទាំងនេះ ដែលបានចុះក្នុងជួរបន្ទាត់ C នៃបញ្ជីសំរាប់ពិនិត្យមើលហានិភ័យ។ សំភារៈព័ត៌មានវិទ្យាប្រាំមួយប្រភេទដែលត្រូវបានកំណត់ រួមមាន៖ ព័ត៌មានវិទ្យា បុគ្គលិក សេវាកម្ម ឬបរិក្ខារ ក្រដាសឯកសារ ឧបករណ៍ផ្នែករឹង ឬកម្មវិធីកុំព្យូទ័រ និងបណ្តាញម៉ាស៊ីនកុំព្យូទ័រមេ (Server) ។
ដំណាក់កាលទី ១.២	បែងចែកសំភារៈទាំងនេះដោយយោងទៅតាមរចនាសម្ព័ន្ធរបស់អង្គភាព ។
	លក្ខណៈរបស់សំភារៈពីរប្រភេទ គឺព័ត៌មាន និងបុគ្គលិកត្រូវបានកំណត់នៅថ្នាក់ ស្ថាប័ន យោងទៅតាមលក្ខ័ណទូទៅនៃអភិបាលកិច្ច ។

	លក្ខណៈរបស់សំភារៈដ៏ទៃទៀតដូចជា សេវាកម្ម ឬបរិក្ខារ ក្រដាសឯកសារ ឧបករណ៍ផ្នែករឹង ឬកម្មវិធីកុំព្យូទ័រ និងបណ្តាញកុំព្យូទ័រ ឬម៉ាស៊ីនកុំព្យូទ័រមេ (Server) ត្រូវបានកំណត់នៅថ្នាក់នាយកដ្ឋាននីមួយៗដែលជាស្ថាប័នអាចធ្វើការត្រួតពិនិត្យដោយខ្លួនឯងបាន។
ដំណាក់កាលទី ១.៣	ធ្វើការកែតម្រូវព័ត៌មាននៅក្នុងជួរបន្ទាត់ C និង D ដោយយោងទៅតាមការបែងចែក ដែលបានអនុវត្តនៅក្នុងដំណាក់ទី១.២។
	លោកអ្នកអាចចំលង (Copy) និងបញ្ចូល (Paste) ប្រភេទសំភារៈព័ត៌មាននីមួយៗទៅក្នុងជួរបន្ទាត់នៃនាយកដ្ឋានមួយៗដើម្បីងាយស្រួលក្នុងការត្រួតពិនិត្យ ដោយសារសំភារៈព័ត៌មាននីមួយៗ មានចំនុចត្រួតពិនិត្យលើសពីពីរ សំរាប់កំណត់នូវហានិភ័យនានាសូមធ្វើការចំលង (Copy) ដោយប្រុងប្រយ័ត្ន ដើម្បីឲ្យបានគ្រប់ចំនុចដែលមានចុះក្នុងជួរបន្ទាត់ទាំងអស់។
ដំណាក់កាលទី ២	ធ្វើការវាយតំលៃអំពីសំភារៈ។
ដំណាក់កាលទី ២.១	ធ្វើការវាយតំលៃអំពីការសម្ងាត់ផលប៉ះពាល់ និងលទ្ធភាព (ផ្តល់សេវាកម្ម ឬបរិក្ខារ) ដើម្បីបំពេញនូវលក្ខណៈនិច្ឆ័យ ដែលបានរៀបរាប់នៅក្នុងបញ្ជីតារាងវាយតំលៃ។
	លោកអ្នកអាចធ្វើការជ្រើសរើសផ្នែកណាមួយពីបញ្ជីជ្រើសរើសនៅក្នុងជួរបន្ទាត់ G H និង I។
	សូមប្រើប្រាស់ពិន្ទុដែលបានកំណត់ស្រាប់ ប្រសិនបើលោកអ្នកគិតថាវាមានការលំបាកក្នុងការវាយតំលៃ។
ដំណាក់កាលទី ២.២	បញ្ជីសំរាប់ពិនិត្យមើលហានិភ័យបង្ហាញដោយស្វ័យប្រវត្តិនៅក្នុងជួរបន្ទាត់ J នូវពិន្ទុសរុបទទួលបានពីការវាយតំលៃនៃសំភារៈនីមួយៗ។
	ធ្វើការពិនិត្យឡើងវិញនូវលទ្ធផលទទួលបាន និងធ្វើការពិនិត្យផ្ទៀងផ្ទាត់ជាមួយនឹងលក្ខណៈនិច្ឆ័យដែលបានចុះនៅក្នុងបញ្ជីតារាងវាយ

	តំលៃ។ ធ្វើការកែសម្រួលការវាយតំលៃអំពីការសម្ងាត់ ផលប៉ះពាល់ និងលទ្ធភាព ប្រសិនបើលោកអ្នកគិតថាកំរិតនៃពិន្ទុវាយតំលៃសរុបអំពីសំការៈព័ត៌មាននីមួយៗ ខុសពីការពិតជាក់ស្តែង។
ដំណាក់កាលទី ៣	ធ្វើការត្រួតពិនិត្យសំការៈ។
ដំណាក់កាលទី ៣.១	សូមមើលពាក្យក្នុងជួរបន្ទាត់ L និង M ហើយធ្វើការជ្រើសរើសពាក្យបានអនុវត្ត ឬមិនបានអនុវត្តនៅក្នុងជួរបន្ទាត់ N។
ដំណាក់កាលទី ៤	ធ្វើការវាយតំលៃអំពីហានិភ័យ។
ដំណាក់កាលទី ៤.១	ធ្វើការវាយតំលៃអំពីបញ្ហាគំរាមនិងភាពងាយទទួលរងផលប៉ះពាល់ដើម្បីបំពេញនូវលក្ខណានិច្ឆ័យ ដែលបានរៀបរាប់នៅក្នុងបញ្ជីតារាងវាយតំលៃ។
	លោកអ្នកអាចធ្វើការជ្រើសរើសផ្នែកណាមួយពីបញ្ជីជ្រើសរើសនៅក្នុងជួរបន្ទាត់ P និង R។
	សូមមើលសេចក្តីអធិប្បាយអំពីបញ្ហាគំរាមនីមួយៗនៅក្នុងជួរបន្ទាត់ Q សំរាប់ជាជំនួយក្នុងការសម្រេចលើការវាយតំលៃអំពីបញ្ហាគំរាម។
	សូមប្រើប្រាស់ពិន្ទុដែលបានកំណត់ជូនស្រាប់ ប្រសិនបើលោកអ្នកគិតថាវាមានការលំបាកក្នុងការវាយតំលៃ។
ដំណាក់កាលទី ៤.២	បញ្ជីសំរាប់ពិនិត្យមើលហានិភ័យបង្ហាញដោយស្វ័យប្រវត្តិនូវពិន្ទុវាយតំលៃសរុបនៅក្នុងជួរបន្ទាត់ T ។
	ធ្វើការពិនិត្យឡើងវិញនូវលទ្ធផលទទួលបាន និងធ្វើការពិនិត្យផ្ទៀងផ្ទាត់ជាមួយនឹងលក្ខណានិច្ឆ័យ ដែលបានចុះនៅក្នុងបញ្ជីតារាងវាយតំលៃ។ ធ្វើការកែសម្រួលការវាយតំលៃអំពីបញ្ហាគំរាមនិងភាពទទួលរងនូវផលប៉ះពាល់ 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 បាននូវលទ្ធភាពសំរាប់អនុវត្តបានទេ។
ដំណាក់កាលទី ៥.៤	ធ្វើការបញ្ចូលទិន្នន័យបន្ថែម (Update) ទៅក្នុងជួរបន្ទាត់ U ស្តីអំពីសេក្តីអធិប្បាយពីវិធានការគ្រប់គ្រង ជួរបន្ទាត់ V ស្តីអំពីឯកសារយោង និងធ្វើការបញ្ចូលទិន្នន័យបន្ថែម (Update) ទាក់ទងនឹងបញ្ញត្តិ និងនីតិវិធីដែលអាចប្រើប្រាស់ និងអនុវត្តបាននៅក្នុងអង្គភាព។
ដំណាក់កាលទី ៦	ធ្វើការវាយតំលៃអំពីហានិភ័យបន្ទាប់ពីបានចាត់វិធានការគ្រប់គ្រងបញ្ហាទាំងនេះ។
ដំណាក់កាលទី ៦.១	ធ្វើការវាយតំលៃអំពីបញ្ហាគំរាមនិងភាពងាយទទួលរងផលប៉ះពាល់ដើម្បីបំពេញនូវលក្ខណៈនិច្ចិយ ដែលបានរៀបរាប់នៅក្នុងបញ្ជីតារាង

	វាយតំលៃ។
	លោកអ្នកអាចធ្វើការជ្រើសរើសផ្នែកណាមួយពីបញ្ជីជ្រើសរើសនៅក្នុងជួរបន្ទាត់ W និង Y។
	ប្រើបាស់នូវពិន្ទុដែលបានកំណត់ជូនស្រាប់ ប្រសិនបើលោកអ្នកមិនបានផ្លាស់ប្តូរវិធានការក្នុងការគ្រប់គ្រងវិធាននិងនីតិវិធីនៅក្នុងឯកសារស្តីអំពីសន្តិសុខព័ត៌មាននោះទេ។
ដំណាក់កាលទី ៦.២	បញ្ជីសំរាប់ពិនិត្យមើលហានិភ័យបង្ហាញដោយស្វ័យប្រវត្តិនូវពិន្ទុវាយតំលៃសរុបនៅក្នុងជួរបន្ទាត់ AA។
	ធ្វើការពិនិត្យឡើងវិញនូវលទ្ធផលទទួលបាននិងធ្វើការពិនិត្យផ្ទៀងផ្ទាត់ជាមួយនឹងលក្ខណៈវិនិច្ឆ័យដែលបានចុះនៅក្នុងបញ្ជីតារាងវាយតំលៃ។ ធ្វើការកែសម្រួលការវាយតំលៃអំពីបញ្ហាគំរាម និងភាពងាយទទួលរងនូវផលប៉ះពាល់ប្រសិនបើលោកអ្នកគិតថាកំរិតនៃពិន្ទុវាយតំលៃសរុបអំពីហានិភ័យខុសពីការពិតជាក់ស្តែង។
ដំណាក់កាលទី ៦.៣	ត្រូវប្រាកដថាពិន្ទុសរុបនៃការវាយតំលៃអំពីហានិភ័យនីមួយៗដែលទទួលបានមានកំរិតទាប។ ធ្វើការសម្រេចចិត្តក្នុងការចាត់វិធានការបន្ថែមដើម្បីកាត់បន្ថយនូវហានិភ័យឬធ្វើការរៀបរាប់អំពីលក្ខ័ណដែលអាចទទួលយកនូវហានិភ័យដែលមិនទាន់ជួបប្រទះ។