បំផុត។

បច្ចារការឆ្លងមេរោគ

(ក២) នៅពេលដោតឧបករណ៍ផ្ទុកទិន្នន័យទៅកុំព្យូទ័ររបស់លោកអ្នក មិនត្រូវអនុវត្តការបើកឯកសារដោយស្វ័យប្រវត្តិឡើយ។

(ក៣) ជានិច្ចកាល ត្រូវរុករក (Scan) មេរោគ ក្នុងឧបករណ៍ផ្ទុកទិន្នន័យ នៅពេលដោតវាទៅកុំព្យូទ័ររបស់លោកអ្នក។

ការលុបសម្អាតទិន្នន័យ

(ក៤) ត្រូវលុបសម្អាត ឬបំផ្លាញចោលនូវទិន្នន័យរូបវន្តក្នុងឧបករណ៍ផ្ទុកទិន្នន័យនៃកុំព្យូទ័រដោយមិនបន្សល់ទុកនូវទិន្នន័យ ឬព័ត៌មាន ដែលអាចលួចប្រើប្រាស់បានឡើយ។

(ខ) នីតិវិធី(សំរាប់មន្ត្រីគ្រប់រូប)

វិធានការគ្រប់គ្រងសម្ភារៈដែលបានបាត់បង់ ឬត្រូវបានលួច

(ខ១) ប្រសិនបើឧបករណ៍ផ្ទុកទិន្នន័យបានបាត់បង់ ឬត្រូវបានលួច សូមប្រតិបត្តិតាមនីតិវិធីដែលបានរៀបរាប់នៅក្នុង**វិធានការគ្រប់គ្រងសម្ភារៈដែលបានបាត់បង់ ឬត្រូវបានលួចក្រោមវិធាន និងនីតិវិធីទាក់ទងនឹងកុំព្យូទ័រយួរដៃ** ឬកុំព្យូទ័រចល័ត។

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 និងដោយទទួលបានការអនុញ្ញាត ពីប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មាន។

(ក២) ត្រូវរៀបចំរូបសណ្ឋាន (Configure) កម្មវិធីកុំព្យូទ័រ ដោយយោងទៅតាមការណែនាំ របស់មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន។

(ក៣) ត្រូវបញ្ចូលកម្មវិធីផេតស៍ (Patches) ភ្លាមៗ បន្ទាប់ពីទទួលបានការណែនាំពីមន្ត្រី ទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន។

កម្មវិធី កុំព្យូទ័រ ដែលមិនមានកម្មសិទ្ធិបញ្ញា

(ក៤) ត្រូវមានការប្រុងប្រយ័ត្នចំពោះការទទួលបានសិទ្ធិប្រើប្រាស់កម្មវិធីកុំព្យូទ័រ។ កម្មវិធីភាគ ច្រើនអាចត្រូវបានដំឡើង និងប្រើប្រាស់បានក្នុងករណីដែលលោកអ្នកបានបង់ថ្លៃ កម្មសិទ្ធិ បញ្ញារួចរាល់ លើកលែងតែជា «កម្មវិធីដែលមិនគិតថ្លៃ» ឬ «កម្មវិធីសំរាប់ប្រើប្រាស់ជា សាធារណៈ» ។ ត្រូវលុបចោល ឬសុំសិទ្ធិប្រើប្រាស់ កម្មវិធីដែលមិនគិតថ្លៃ មានតម្លៃថោក ឬកម្មវិធីសំរាប់ប្រើប្រាស់សាកល្បង នៅពេលដែលផុតកំណត់រយៈ ប្រើប្រាស់សាកល្បង។ កម្មវិធីមួយចំនួនត្រូវបានកំណត់ការប្រើប្រាស់ដោយមិនគិតថ្លៃ សំរាប់បុគ្គលឯកជន ប៉ុន្តែ តម្រូវឲ្យបង់ថ្លៃសំរាប់ទទួល បានសិទ្ធិប្រើប្រាស់ក្នុងការងារជំនួញ។ បុគ្គលនិងស្ថាប័នមួយ ចំនួនអាចត្រូវបានប្តឹងពីបទរំលោភច្បាប់កម្មសិទ្ធបញ្ញា ទាក់ទងនឹងការប្រើប្រាស់កម្មវិធី

កុំព្យូទ័រ។ 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 និងឧបករណ៍បង្កើតពាក្យ ឬលេខសម្ងាត់ ត្រូវបានហាមឃាត់ជាចំហមិនឲ្យប្រើប្រាស់ ជាមួយសម្ភារៈនានារបស់ស្ថាប័ន 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)។

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	ត្រូវបញ្ចូលនិងកំណត់ព័ត៌មានថ្មីៗរបស់កម្មវិធី កុំព្យូទ័រ ដែលមានបទដ្ឋានត្រឹមត្រូវ និងបញ្ចូលនូវព័ត៌ថ្មីៗចុងក្រោយរបស់ផេតស៍ (Patches) ជាប្រចាំ។ (បញ្ជីនេះអាចសរសេរ «ជានិច្চকাল ត្រូវធ្វើការបញ្ចូលទិន្នន័យថ្មីៗ (Update) របស់ Windows ភ្លាមៗ លើកលែងតែមានបំរាមជាចំហ»)	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	(បញ្ជីរាយព័ត៌មានថ្មីៗរបស់កម្មវិធី 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	ដាក់ជូននូវរបាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មានប្រសិនបើបានរកឃើញ	អ្នកប្រើប្រាស់	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹង

	នូវចំនុចដែលមិនសមស្រប		សន្តិសុខព័ត៌មាន
ខ២.៤	តម្កល់ទុករបាយការណ៍ទាំងនេះ និងរក្សាទុកសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

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

(ក) និយាន

(ក១) បច្ចុប្បន្ន ឯកសារជូនភ្ជាប់ក្នុងសារអេឡិចត្រូនិច (E-mail Attachments) គឺជាប្រភពដ៏ចំបងបំផុតនៃការចម្លងមេរោគកុំព្យូទ័រ។ ត្រូវចៀសវាងបើករាល់ឯកសារជូនភ្ជាប់ក្នុងសារអេឡិចត្រូនិច (E-mail Attachments) លើកលែងតែលោកអ្នកបានដឹង ច្បាស់លាស់អំពីប្រភពព័ត៌មាននៃអ្នកដែលផ្ញើឯកសារនេះ។

(ក២) មិនត្រូវប្រើប្រាស់សារអេឡិចត្រូនិចៈ

(ក២.១) ដើម្បីផ្ញើចេញនូវព័ត៌មានដែលសម្ងាត់ ឬរសើប ជាពិសេសនៅលើបណ្តាញអ៊ីនធឺណិត (Internet) លើកលែងតែវាត្រូវបានផ្លាស់ប្តូរទំរង់ជើម (Encrypted) ដោយប្រព័ន្ធសំរាប់ផ្លាស់ប្តូរទំរង់ជើម ដែលទទួលស្គាល់ត្រឹមត្រូវថាអាចធានាបាននូវសន្តិសុខព័ត៌មាន។

(ក២.២) សំរាប់ការងារឯកជន ឬការងារសប្បុរសធម៌ ដែលមិនទាក់ទងនឹងការងារស្របច្បាប់របស់អង្គភាព។

(ក២.៣) នៅក្នុងលក្ខខណ្ឌដែលបំពេញនូវកិច្ចការទាក់ទងនឹងការចេញនូវសេចក្តីថ្លែងការណ៍

ជាសាធារណៈ និងជាផ្លូវការតំណាងឲ្យអង្គភាព លើកលែងតែលោកអ្នកមានតួនាទីជាអ្នកនាំពាក្យ ដែលទទួលបានការតែងតាំងជាចំហដោយថ្នាក់ដឹកនាំ ដើម្បីចេញសេចក្តីរាយការណ៍បែបនេះ។

(ក២.៤) ដើម្បីធ្វើសារដោយប្រើប្រាស់ អត្តសញ្ញាណ និងលេខសម្ងាត់ (Account) របស់នរណាម្នាក់ ឬធ្វើក្នុងលក្ខណៈតំណាងឲ្យនរណាម្នាក់ រួមទាំងការប្រើប្រាស់អាស័យដ្ឋានក្លែងក្លាយ ដែលសរសេរក្នុង «កន្លែងបំពេញអាសយដ្ឋានធ្វើចេញ»។ ប្រសិនបើមានការអនុញ្ញាតពីអ្នកគ្រប់គ្រង លេខាធិការម្នាក់អាចធ្វើសារអេឡិចត្រូនិច (E-mail) ជំនួសបាន ប៉ុន្តែគួរតែមានហត្ថលេខារបស់លេខាធិការនោះចុះក្នុងសារអេឡិចត្រូនិច។

(ក២.៥) ដើម្បីធ្វើនូវអ្វីមួយដែលមានលក្ខណៈរំខាន 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) ត្រូវមានសុកនិច្ច័យក្នុងវិជ្ជាជីវៈ នៅពេលប្រើប្រាស់សារអេឡិចត្រូនិច ដូចជាត្រូវគោរព

តាមច្បាប់សុជីវធម៌ ដែលត្រូវបានទទួលស្គាល់ជាទូទៅទាក់ទងនឹងសារអេឡិចត្រូនិច។

(ក៤) ត្រូវពិនិត្យមើលសារអេឡិចត្រូនិចឡើងវិញ ដោយប្រុងប្រយ័ត្នមុនពេលផ្ញើចេញ ជាពិសេសចំពោះសារផ្លូវការ សំរាប់ទំនាក់ទំនងជាមួយបុគ្គលខាងក្រៅ។

(ក៥) បើមិនចាំបាច់ មិនត្រូវបញ្ចេញព័ត៌មានដែលមានលក្ខណៈរសើប តាមរយៈសារដែលផ្ញើចេញពីការិយាល័យឡើយ។

(ក៦) មន្ត្រីរាជការទាំងឡាយមិនត្រូវស្ទាក់លួច បញ្ជូនត កែប្រែ លុប រក្សាទុក ឬបង្ហាញចេញនូវព័ត៌មាននៅក្នុងសារអេឡិចត្រូនិចឡើយ លើកលែងទទួលបានការអនុញ្ញាត ត្រឹមត្រូវពីថ្នាក់ដឹកនាំ ឬវាជាប្រការចាំបាច់សំរាប់ការងារគ្រប់គ្រងប្រព័ន្ធបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន។

(ក៧) ក្នុងករណីដែលមានកិច្ចការមិនសូវសំខាន់កើតឡើងម្តងម្កាល និងមិនប៉ះពាល់ដល់ការងាររបស់អង្គភាព ការប្រើប្រាស់ផ្ទាល់ខ្លួនដោយមានកំណត់នូវប្រព័ន្ធសារអេឡិចត្រូនិចរបស់អង្គភាពអាចត្រូវបានអនុញ្ញាត តាមរយៈការយល់ព្រមពីថ្នាក់ដឹកនាំរបស់ខ្លួន។ លោកអ្នកមិនត្រូវគិតថា នឹងទទួលបាននូវភាពសម្ងាត់ក្នុងការប្រើប្រាស់សារអេឡិចត្រូនិចឡើយ ដោយហេតុថារាល់សារទាំងអស់ដែលឆ្លងកាត់ប្រព័ន្ធ និងបណ្តាញកុំព្យូទ័ររបស់រដ្ឋ នឹងត្រូវបានរុករកមេរោគ (Scan) ដោយស្វ័យប្រវត្តិ នឹងអាចត្រូវបានរក្សាទុកដាច់ដោយឡែក នឹងត្រូវបានពិនិត្យឡើងវិញដោយនិយោជិតដែលបានចាត់តាំង។

(ក៨) ត្រូវផ្ញើ និងរក្សាទុកសារអេឡិចត្រូនិចរបស់លោកអ្នកក្នុងទំហំ និងចំនួនមួយសមរម្យ។ ជានិច្চকাল ត្រូវសម្អាតប្រអប់សារ (Mailbox) របស់លោកអ្នក លុបចោលសារអេឡិចត្រូនិចចាស់ៗដែលលែងត្រូវការ និងតម្កល់ទុកសារនានាដោយត្រូវរក្សាទុកឲ្យបានត្រឹមត្រូវ

នៅក្នុងកន្លែងផ្ទុកឯកសារ (Folders) របស់សារអេឡិចត្រូនិច។

ពន្យារការអនុវត្តន៍

(ខ) នីតិវិធី (សំរាប់មន្ត្រីគ្រប់រូប)

វិធានការចូវៅសំរាប់ដោះស្រាយបញ្ហាទាក់ទងនឹងសន្តិសុខព័ត៌មាន

(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