វាងនូវការលួចប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត។

(ក៣)បំផ្លាញចោលនូវឧបករណ៍ផ្ទុកឯកសារ ដែលលែងប្រើប្រាស់(DVD/CD/FD/Tape)។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៥. <u>វិធាន និង នីតិវិធី សន្តិសុខកុំព្យូទ័រ</u>

៦.៥.១. <u>កុំព្យូទ័ររលើតុ</u>

(ក) វិធាន

ទិដ្ឋភាពទូទៅ

(ក១) ការការពារសន្តិសុខជារូបវន្តនៃកុំព្យូទ័ររបស់លោកអ្នក គឺជាការទទួលខុសត្រូវផ្ទាល់ខ្លួនរបស់លោកអ្នក។ ដូចនេះសូមមានការប្រុងប្រយ័ត្នខ្ពស់ក្នុងការថែរក្សាកុំព្យូទ័ររបស់លោកអ្នក។ ម្យ៉ាងវិញទៀត លោកអ្នកក៏ត្រូវមានសុភនិច្ឆ័យនិងប្រុងប្រៀបជានិច្ច ដើម្បីទប់ទល់នឹងហានិភ័យនានាផងដែរ។

(ក២) រាល់កុំព្យូទ័រនីមួយៗត្រូវស្ថិតក្រោមការទទួលខុសត្រូវរបស់មន្ត្រីម្នាក់ៗជាក់លាក់ ទោះបីជាកុំព្យូទ័រទាំងនេះត្រូវបានប្រើប្រាស់ដោយមន្ត្រីច្រើនគ្នាក៏ដោយ។

(ក៣) លោកអ្នកត្រូវទទួលខុសត្រូវដោយផ្ទាល់ ចំពោះការប្រើប្រាស់កុំព្យូទ័រ លើបណ្តាញតាមរយៈអត្តសញ្ញាណ (User ID) ផ្ទាល់ខ្លួន។ ដូច្នេះ សូមថែរក្សាលេខ ឬពាក្យសម្ងាត់ (Password) របស់លោកអ្នកដោយប្រុងប្រយ័ត្ន និងសម្ងាត់បំផុត។ លេខ ឬពាក្យសម្ងាត់ (Password) នេះត្រូវតែមានលក្ខណៈស្មុគស្មាញ ដែលមិនងាយនឹងលួចប្រើប្រាស់បាន ហើយវាត្រូវតែផ្លាស់ប្តូរជាទៀងទាត់។ លោកអ្នកមិនត្រូវចែករំលែកការប្រើប្រាស់ លេខ ឬ

ពាក្យសម្ងាត់នេះជាមួយអ្នកដ៏ទៃឡើយ ទោះបីជាសមាជិកគ្រួសារ មិត្តភក្តិ ឬអ្នកបច្ចេកទេសដែលធ្វើការជាមួយលោកអ្នកក៏ដោយ។

(ក៤) ត្រូវជៀសវាងទុកនិងបើកកុំព្យូទ័រចោលដោយមិនបានប្រើប្រាស់។ ជានិច្ចកាល មុនពេលលោកអ្នកចាកចេញពីកុំព្យូទ័រ ត្រូវបិទ ឬឡក់ឌីស (Logoff) ឬដាក់លេខ ឬពាក្យសម្ងាត់ នៅលើស្ក្រីនសេវើ (Screensaver) នៃកុំព្យូទ័ររបស់លោកអ្នក។

បង្ការការឆ្លងមេរោគ

(ក៥) ការឆ្លងមេរោគក្នុងកុំព្យូទ័រ គឺជាបញ្ហាដ៏ចំបងមួយ សំរាប់ អ.អ.ប.គ.ព ក្នុងការដោះស្រាយ ដោយសារកុំព្យូទ័រនានា ងាយនឹងទទួលរងការឆ្លងមេរោគ ប្រសិនបើកម្មវិធីប្រឆាំងមេរោគរបស់កុំព្យូទ័រទាំងនោះ មិនត្រូវបានធ្វើអោយទាន់សម័យ (Update Definition) យ៉ាងតិចចំនួនមួយដងក្នុងមួយសប្តាហ៍។ វិធីសាស្ត្រដែលងាយស្រួលបំផុតសំរាប់អនុវត្តការងារនេះ គឺត្រូវបើកអោយកម្មវិធីកំចាត់មេរោគដំណើរការនូវមុខងារធ្វើអោយទាន់សម័យដោយស្វ័យប្រវត្តិ ដោយតភ្ជាប់កុំព្យូទ័ររបស់លោកអ្នកទៅនឹង បណ្តាញអ៊ីនធឺណិត។ ប្រសិនបើលោកអ្នកមិនអាចធ្វើបែបនេះបាន ដោយសារប្រការណាមួយ សូមទំនាក់ទំនងទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដើម្បីទទួលបាននូវសេចក្តីណែនាំពីនីតិវិធីក្នុងការដំឡើងកម្មវិធីកំចាត់មេរោគកុំព្យូទ័រ។

(ក៦) ជានិច្ចកាល ត្រូវរុករក (Scan) មេរោគ នូវរាល់ឯកសារទាំងឡាយដែលបានទាញយក (Download) មកទុកក្នុងកុំព្យូទ័ររបស់លោកអ្នកពីប្រភពផ្សេងៗ ដូចជា (CD/DVD /USB/Hard Disk/Memory Stick) ឯកសារបញ្ជូនតាមបណ្តាញកុំព្យូទ័រ ឯកសារជូនភ្ជាប់ក្នុងសារអេឡិចត្រូនិច (E-mail Attachments) ឬឯកសារពីបណ្តាញអ៊ីនធឺណិត)។ ដើម្បីអោយងាយស្រួល ត្រូវបើកអោយកម្មវិធីកំចាត់មេរោគដំណើរការនូវមុខងារចាប់

មេរោគដោយស្វ័យប្រវត្តិ និងចាំបាច់កំណត់កាលវិភាគសំរាប់ការរុករកមេរោគ ដោយត្រូវអនុវត្តយ៉ាងតិចមួយដងជារៀងរាល់សប្តាហ៍។

(ក៧) ត្រូវរាយការណ៍ជាបន្ទាន់ ទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន អំពីហេតុការណ៍ទាក់ទងទៅនិងសន្តិសុខព័ត៌មាន ដូចជាហេតុការនៃការឆ្លងមេរោគចូលក្នុងប្រព័ន្ធកុំព្យូទ័រដើម្បីកាត់បន្ថយនូវការខាតបង់នានា។

(ក៨) ត្រូវឆ្លើយតបជាបន្ទាន់ ទៅនឹងសារព្រមានអំពីលទ្ធភាពឆ្លងមេរោគនានា ក្នុងកុំព្យូទ័ររបស់លោកអ្នក។ ប្រសិនបើមានការសង្ស័យអំពីមេរោគណាមួយ ឧទាហរណ៍ឯកសារដែលមានលក្ខណៈមិនប្រក្រតី សូមទាក់ទងទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន មិនត្រូវបញ្ជូនបន្ត (Forward) នូវឯកសារណាមួយ ឬបញ្ចូល (Upload) ទិន្នន័យទៅលើបណ្តាញកុំព្យូទ័រទេ ប្រសិនបើសង្ស័យថាកុំព្យូទ័ររបស់លោកអ្នកបានឆ្លងមេរោគ។

(ក៩) ត្រូវមានការប្រុងប្រយ័ត្នជាពិសេសក្នុងការរុករកមេរោគ នៅក្នុងប្រព័ន្ធកុំព្យូទ័ររបស់លោកអ្នក មុនពេលផ្ញើចេញនូវឯកសារណាមួយ។ ឯកសារទាំងនេះរួមមាន ឯកសារជូនភ្ជាប់ក្នុងសារអេឡិចត្រូនិច (E-mail Attachments) និងឯកសារដែលបានពីCD/DVD។

(ក១០) រាល់កុំព្យូទ័រលើតុទាំងអស់ ត្រូវតភ្ជាប់ទៅកាន់ឧបករណ៍រក្សាចរន្តអគ្គីសនី (UPS) ដើម្បីចៀសវាងការបាត់បង់ទិន្នន័យ។

ការសម្អាតទិន្នន័យ

(ក១១) ត្រូវលុបសម្អាតទិន្នន័យរូបវន្ត (Physical Formatting) ក្នុងឧបករណ៍ផ្ទុកទិន្នន័យនៃកុំព្យូទ័រដោយមិនបន្សល់ទុកនូវទិន្នន័យ ឬព័ត៌មានដែលអាចទាញយកមកវិញបាន។

(ខ) នីតិវិធី (សំរាប់មន្ត្រីគ្រប់រូប)

បង្ការការឆ្លងមេរោគ

(ខ១) ដើម្បីអនុវត្តតាមនីតិវិធីខាងក្រោមនេះបាន លោកអ្នកត្រូវប្រាកដថា រាល់កម្មវិធីកំចាត់មេរោគ នៅក្នុងកំព្យូទ័រទាំងអស់ត្រូវធ្វើអោយទាន់សម័យតាមចំនួនដងដាក់លាក់។

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	ណែនាំឲ្យមានការផ្តល់ជូននូវបញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.២	អនុវត្តការរុករកមេរោគ	អ្នកប្រើប្រាស់	មិនមាន
ខ១.៣	ធ្វើការបោះពុម្ព និងដាក់ជូននូវបញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ	អ្នកប្រើប្រាស់	បញ្ជីព័ត៌មានស្តីអំពីការរុករកមេរោគ (Scan) របស់កម្មវិធីប្រឆាំងមេរោគ
ខ១.៤	តម្កល់ទុកបញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ និងរក្សាទុកសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.៥	ពិនិត្យតាមដានមន្ត្រីដែលមិនបានរុករកមេរោគ និងដាក់ជូននូវបញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

ចំណាត់ការក្នុងការចាប់មេរោគ

(ខ២) នីតិវិធីខាងក្រោម ត្រូវបានបង្កើតឡើងដើម្បីចាត់វិធានការណ៍ ចាប់មេរោគផ្សេងៗ។

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ២.១	អនុវត្តនូវសកម្មភាពការពារសន្តិសុខព័ត៌មាន ដូចជាសកម្មភាពចាប់មេរោគជាដើម	អ្នកប្រើប្រាស់	មិនមាន
ខ២.២	ត្រូវផ្តាច់ប្រព័ន្ធកុំព្យូទ័រ ជាបន្ទាន់ពីបណ្តាញកុំព្យូទ័រ	អ្នកប្រើប្រាស់	មិនមាន
ខ២.៣	ជូនដំណឹងទៅការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានជាបន្ទាន់ នៅពេលដែលចាប់បានមេរោគ	អ្នកប្រើប្រាស់	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន
ខ២.៤	ធ្វើការវិភាគអំពីផលវិបាកនៃហេតុការណ៍នីមួយៗ និងចាត់វិធានការសមរម្យដើម្បីដោះស្រាយ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.៥	ប្រសិនបើមានការចាំបាច់ ត្រូវបញ្ឈប់ប្រព័ន្ធដំណើរការបណ្តាញកុំព្យូទ័រ (Network Application)	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.៦	ប្រសិនបើមានការចាំបាច់ ត្រូវអនុវត្តជាបន្ទាន់នូវវិធីសាស្ត្របង្ការការឆ្លងមេរោគ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.៧	សរសេរចូលក្នុងរបាយការណ៍អំពីការវិភាគ និងវិធានការនីមួយៗ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន(ដែលបានបញ្ចូលព័ត៌មានថ្មី)

១២.៨	តម្កល់ទុករបាយការណ៍ទាំងនេះ និងរក្សាទុកសំរាប់ រយៈពេល កំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវ ផ្នែកសន្តិសុខ ព័ត៌មាន	មិនមាន

៦.៥.២. <u>កុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័ត</u>

(ក) វិធាន

ទិដ្ឋភាពទូទៅ

វិធានមួយចំនួនខាងក្រោម ត្រូវបានប្រើប្រាស់សំរាប់តែកុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តប៉ុណ្ណោះ។ បញ្ហាទាក់ទងនឹងកុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តនេះ ក៏ត្រូវតែអនុវត្តតាមវិធាននិងនីតិវិធី ដែលបាន កំណត់នៅក្នុងចំនុចទី **៦.៥.១. កុំព្យូទ័រលើតុ** ផងដែរ។

(ក១) គ្រប់ពេលបើអាចធ្វើទៅបាន ត្រូវរក្សាទុកកុំព្យូទ័រយួរដៃរបស់លោកអ្នកនៅជាប់នឹងខ្លួន ជានិច្ច ប្រៀបដូចនឹងកាបូបដាក់ហោប៉ៅ កាបូបយួរដៃ ឬទូរស័ព្ទចល័តរបស់លោកអ្នក។ ជាពិសេស ត្រូវរក្សាទុកវាដោយប្រុងប្រយ័ត្នបំផុតនៅទីសាធារណៈ ដូចជា អាហារដ្ឋានជាដើម (សូមបញ្ជាក់ថា វាប្រើរយៈពេលដ៏ខ្លីបំផុត សំរាប់អ្នកដែលមានបំណងលួចទិន្នន័យ នៅក្នុងកុំព្យូទ័រយួរដៃ ដែលម្ចាស់របស់វាមិនបានប្រុងប្រយ័ត្ន)។

(ក២) ប្រសិនបើលោកអ្នកមានការចាំបាច់ ត្រូវទុកកុំព្យូទ័រចោលបណ្តោះអាសន្ននៅក្នុង ការិយាល័យ បន្ទប់ប្រជុំ ឬបន្ទប់សណ្ឋាគារ សូមប្រើប្រាស់ខ្សែសន្តិសុខរបស់កុំព្យូទ័រយួរដៃ ឬឧបករណ៍ស្រដៀងគ្នានេះ ដើម្បីចងភ្ជាប់កុំព្យូទ័រទៅនឹងតុ ឬគ្រឿងសង្ហារឹមដែលធ្ងន់ៗ ទោះបីក្នុងរយៈពេលមួយខ្លីក៏ដោយ។ ការការពារបែបនេះមិនសូវជាមានសន្តិសុខ ប៉ុន្តែវា អាចបង្ការនូវការបាត់បង់កុំព្យូទ័រដោយចៃដន្យ។

(ក៣) នៅពេលដែលលោកអ្នកលែងត្រូវការប្រើប្រាស់កុំព្យូទ័រ សូមរក្សាទុកកុំព្យូទ័រក្នុងទីកន្លែងដែលមានសុវត្ថិភាពខ្ពស់ ដែលអាចប្រព្រឹត្តទៅបាននៅ គេហដ្ឋាន ការិយាល័យ ឬ សណ្ឋាគារ។ មិនត្រូវទុកចោលកុំព្យូទ័រយួរដៃរបស់លោកអ្នកនៅក្នុងយានយន្ត ដែលបុគ្គលដ៏ទៃអាចមើលឃើញដោយងាយឡើយ។ ប៉ុន្តែប្រសិនបើមានការចាំបាច់បំផុតដែលត្រូវធ្វើបែបនេះ សូមចាក់សោវាទុកនៅក្នុងផ្នែកខាងក្រោយនៃរថយន្ត ឬប្រអប់ដាក់សម្ភារៈក្បែរអ្នកបើកបរ វាមានសន្តិសុខច្រើនជាងប្រសិនបើលោកអ្នកយកវាទៅតាមខ្លួន។

(ក៤) យកទៅតាមខ្លួននូវកុំព្យូទ័រយួរដៃរបស់លោកអ្នក ដែលបានទុកដាក់យ៉ាងត្រឹមត្រូវនៅក្នុងកាបូបដែលមានទ្រនាប់អាចការពារការប៉ះទង្គិចដោយចៃហេតុ ឬកាបូបកុំព្យូទ័រដែលមានលក្ខណៈមាំទាំ ដើម្បីចៀសវាងនូវការខូចខាតដល់កុំព្យូទ័រ។ មិនត្រូវទំលាក់ ឬធ្វើអោយប៉ះទង្គិចកុំព្យូទ័ររបស់លោកអ្នកជាមួយនឹងវត្ថុរឹងឡើយ។ ការវេចខ្ចប់កុំព្យូទ័រយួរដៃរបស់លោកអ្នកជាមួយនឹងបន្ទះផ្លាស្ទិក (ដែលបង្កើតដោយថង់ខ្យល់តូចៗជាច្រើនសំរាប់ជាទ្រនាប់) អាចការពារការប៉ះទង្គិចបាន។ កាបូបដាក់កុំព្យូទ័រដែលមានរូបរាងសាមញ្ញទំនងជាមានភាពទាក់ទាញចោរលួច តិចជាងកាបូបដែលមានភាពលេចធ្លោ។

(ក៥) កុំព្យូទ័រយួរដៃរបស់រដ្ឋ ត្រូវបានប្រគល់ជូននិយោជិត ដែលមានសិទ្ធិត្រឹមត្រូវ សំរាប់ប្រើប្រាស់ក្នុងលក្ខណៈផ្លូវការ។ មិនត្រូវឲ្យកុំព្យូទ័រយួរដៃរបស់លោកអ្នកទៅអ្នកដ៏ទៃ ដូចជាក្រុមគ្រួសារ ឬមិត្តភក្តិ ឬប្រើប្រាស់ឡើយ។

(ក៦) ត្រូវកត់ត្រាទុកនូវព័ត៌មានទាក់ទងនឹងម៉ាក ម៉ូដែល លេខស៊េរី (Serial Number) និងស្លាកសម្គាល់ម្ចាស់កម្មសិទ្ធិ (ឧទាហរណ៍ អ.អ.ប.គ.ព) នៃកុំព្យូទ័រយួរដៃរបស់ លោកអ្នក ប៉ុន្តែមិនត្រូវរក្សាទុកព័ត៌មាននេះក្នុង ឬជាប់នឹងកុំព្យូទ័ររបស់លោកអ្នកឡើយ។ ប្រសិនបើវាបាត់បង់ ឬត្រូវបានលួច ត្រូវប្តឹងទៅមន្ត្រីនគរបាលជាបន្ទាន់ ហើយត្រូវជូនដំណឹងទៅ

ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានវិទ្យាភ្លាមៗ តាមលទ្ធភាពដែលអាចធ្វើបាន (សូមអនុវត្តបែបនេះ បន្ទាប់ពី១ ឬ២ម៉ោងក្រោយមក មិនមែន១ ឬ២ថ្ងៃក្រោយមកទេ)។

ការគ្រប់គ្រងការប្រើប្រាស់កុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តដោយពុំមាន ការអនុញ្ញាត

(ក៧) វាជាការប្រសើរបំផុត ដែលរាល់កុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តទាំងអស់ ប្រើប្រាស់នូវកម្មវិធីសំរាប់ផ្លាស់ប្តូរទំរង់ដើមរបស់ព័ត៌មាន (Encryption) ដែលមានការទទួលស្គាល់ត្រឹមត្រូវ។ ក្នុងករណីនេះត្រូវជ្រើសប្រើប្រាស់នូវឃ្លា ឬលេខ ឬពាក្យសម្ងាត់ដែលវែង និងមិនងាយលួចប្រើប្រាស់បាន ហើយត្រូវរក្សាទុកវាឲ្យមានសន្តិសុខ។ ត្រូវទំនាក់ទំនងទៅកាន់ ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ដើម្បីទទួលបានព័ត៌មានបន្ថែមអំពី ការផ្លាស់ប្តូរ ទំរង់ដើមរបស់ព័ត៌មាន (Encryption) របស់កុំព្យូទ័រយួរដៃ។ ប្រសិនបើកុំព្យូទ័រយួរដៃ ឬ កុំព្យូទ័រចល័តណាមួយបានបាត់ ឬត្រូវបានលួច ការផ្លាស់ប្តូរទំរង់ដើមរបស់ព័ត៌មាន (Encryption) ផ្តល់ការការពារយ៉ាងមានប្រសិទ្ធិភាពជាទីបំផុត ទប់ទល់ទៅនឹងការលួចចូលក្នុងកុំព្យូទ័រដើម្បីប្រើប្រាស់ទិន្នន័យ។

(ក៨) មិនត្រូវរក្សាទុកព័ត៌មានសម្ងាត់នៅក្នុងកុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តរបស់លោកអ្នកជំនួសការផ្លាស់ប្តូរទំរង់ដើមរបស់ព័ត៌មាន (Encryption) ដូចបានរៀបរាប់នៅក្នុងប្រយោគខាងលើឡើយ។

(ខ) នីតិវិធី (សំរាប់មន្ត្រីគ្រប់រូប)

វិធានការគ្រប់គ្រងសម្ភារៈដែលបានបាត់បង់ ឬត្រូវបានលួច

(ខ១) ប្រសិនបើកុំព្យូទ័រយួរដៃ ឬកុំព្យូទ័រចល័តណាមួយបានបាត់ ឬត្រូវបានលួច សូមធ្វើតាមបែបបទដូចខាងក្រោម ៖

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	ពិនិត្យមើលហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន ដូចជា ការបាត់បង់ ឬការលួចទ្រព្យសម្បត្តិ	អ្នកប្រើប្រាស់	មិនមាន
ខ១.២	ដាក់បណ្តឹងទៅមន្ត្រីនគរបាល	អ្នកប្រើប្រាស់	មិនមាន
ខ១.៣	ក្នុងរយៈពេលមួយម៉ោងបន្ទាប់ពីកើតហេតុ ត្រូវផ្តល់ព័ត៌មានទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	អ្នកប្រើប្រាស់	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន
ខ១.៤	ធ្វើការវិភាគអំពីផលវិបាកនៃហេតុការណ៍នេះ និងចាត់វិធានការសមរម្យដើម្បីដោះស្រាយភ្លាម។ កត់ត្រាអំពីហេតុការណ៍ចូលក្នុងរបាយការណ៍។	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន(ដែលបានបញ្ចូលព័ត៌មានថ្មី)
ខ១.៥	តម្កល់ទុករបាយការណ៍ទាំងនេះ និងរក្សាទុកសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

៦.៥.៣. <u>ឧបករណ៍ផ្ទុកទិន្នន័យ (ហាត ឌីស (Hard Disk) ឬមេមម៉ូរី ស្ទិក (Memory Stick) ឬ មេមម៉ូរី ខាដ (Memory Card))</u>

(ក) និយាយ

ទិដ្ឋភាពទូទៅ

(ក១) ត្រូវចងខ្សែក្លាប់ឧបករណ៍ទាំងនេះ ដើម្បីងាយស្រួលដាក់ជាប់នឹងខ្លួនរបស់លោកអ្នក។ ឧបករណ៍ផ្ទុកទិន្នន័យទំនើបៗបច្ចុប្បន្នមានទ្រង់ទ្រាយតូច ងាយជ្រុះ និងបាត់បង់ជាទី