AEON

សៀវភៅណែនាំអំពីសន្តិសុខព័ត៌មាន

ក្រុមហ៊ុន

ឈ្មោះ

អាសយដ្ឋានទំនាក់ទំនងពាក់ព័ន្ធនឹងប្រព័ន្ធព័ត៌មាន

ឈ្មោះផ្នែក

លេខទំនាក់ទំនង - -

លេខទំនាក់ទំនង - -

គោលការណ៍មូលដ្ឋានស្តីពីសន្តិសុខព័ត៌មាន

អនុ ទទួលស្គាល់សារៈសំខាន់នៃសន្តិសុខព័ត៌មាន ហើយប្រតិបត្តិតាមទស្សនគ្រប់គ្រងរបស់ខ្លួនគឺ «ការស្វែងរកសន្តិភាពជាមួយអតិថិជនជាចំណុចចាប់ផ្តើមរបស់យើង ការគោរពមនុស្សជាតិ និងការចូលរួមចំណែកដល់សហគមន៍ក្នុងតំបន់»។ យើងនឹងការពារព័ត៌មានសំខាន់ៗពីការគំរាមកំហែងផ្សេងៗ និងរួមចំណែកដល់ការកសាងជីវិតដែលមានសុវត្ថិភាព និងវិបុលភាព។ លើសពីនេះ យើងចាត់ទុកព័ត៌មានផ្សេងៗរបស់អ៊ីអន ជាទ្រព្យសម្បត្តិដ៏សំខាន់សម្រាប់ការអភិវឌ្ឍសកម្មភាពអាជីវកម្ម និងបង្កើតតម្លៃបន្ថែម ហើយយើងនឹងគ្រប់គ្រងវាឱ្យបានត្រឹមត្រូវ និងមានសុវត្ថិភាព ដើម្បីកសាងទំនាក់ទំនងរឹងមាំ និងភាពជឿជាក់ពីអ្នកដែលមានទំនាក់ទំនងជាមួយអ៊ីអន រួមទាំងអតិថិជន សហគមន៍មូលដ្ឋាន ដៃគូអាជីវកម្ម និងភាគទុនិក។ ដើម្បីសម្រេចបាននូវគោលដៅទាំងនេះ យើងបានដាក់ចេញនូវគោលនយោបាយមូលដ្ឋានសន្តិសុខព័ត៌មាន ជាមគ្គុទ្ទេសក៍សម្រាប់បុគ្គលិកអ៊ីអនទាំងអស់ ដើម្បីរក្សាការយល់ដឹងអំពីសន្តិសុខព័ត៌មានក្នុងកម្រិតខ្ពស់ និងធ្វើសកម្មភាពស្របតាមនោះ។

បង្កើតនៅថ្ងៃទី១ ខែកញ្ញា ឆ្នាំ២០១៩ ក្រុមហ៊ុនអ៊ីអន

សកម្មភាពស្តីពីសន្តិសុខព័ត៌មាន

អ៊ីអន នឹងអនុវត្តសកម្មភាពដូចខាងក្រោម ដើម្បីប្រតិបត្តិគោលនយោបាយមូលដ្ឋានសន្តិសុខព័ត៌មានឱ្យបានជាក់លាក់។

①យើងនឹងបង្កើតប្រព័ន្ធដើម្បីរក្សា និងបន្តកែលម្អសន្តិសុខព័ត៌មាន។
②យើងនឹងបង្កើត និងអនុវត្តតាមបទប្បញ្ញត្តិ ដើម្បីធានាសន្តិសុខព័ត៌មាន។
③ដើម្បីការពារព័ត៌មាន យើងនឹងធ្វើការវាយតម្លៃហានិភ័យឱ្យបានត្រឹមត្រូវ និងអនុវត្តវិធានការសមហេតុផល និងសមស្រប។
④យើងនឹងផ្តល់ការអប់រំសមស្របអំពីសន្តិសុខព័ត៌មានដល់បុគ្គលិក និងភាគីពាក់ព័ន្ធផ្សេងទៀត ដើម្បីបង្កើនការយល់ដឹងរបស់ពួកគេ។
⑤យើងនឹងអនុវត្តតាមច្បាប់ បទប្បញ្ញត្តិ និងកិច្ចសន្យាទាំងអស់ជាមួយអតិថិជន ដៃគូអាជីវកម្ម និងបុគ្គលិក ព្រមទាំងប្រើប្រាស់ព័ត៌មានឱ្យបានត្រឹមត្រូវ។
⑥យើងនឹងបង្កើតប្រព័ន្ធមួយដើម្បីឆ្លើយតបយ៉ាងឆាប់រហ័ស និងមានប្រសិទ្ធភាពចំពោះឧប្បត្តិហេតុ ឬបញ្ហាសន្តិសុខព័ត៌មានណាមួយដែលអាចកើតឡើង។
⑦ទោះបីជាផ្តល់ការងារទៅខាងក្រៅក៏ដោយ យើងខិតខំរក្សាកម្រិតសន្តិសុខព័ត៌មានឱ្យបានស្មើ ឬខ្ពស់ជាងកម្រិតសន្តិសុខព័ត៌មានរបស់អ៊ីអន។
⑧យើងនឹងខិតខំកាត់បន្ថយផលប៉ះពាល់នៃគ្រោះមហន្តរាយ និងការវាយប្រហារតាមអ៊ីនធឺណិតតាមរយៈសកម្មភាពសន្តិសុខព័ត៌មាន និងធានាបាននូវនិរន្តរភាពនៃសកម្មភាពអាជីវកម្ម។
⑨យើងខ្ញុំនឹងអនុវត្តការត្រួតពិនិត្យ និងសវនកម្មជាប្រចាំ និងមិនទៀងទាត់លើសកម្មភាពខាងលើ ព្រមទាំងខិតខំកែលម្អជាបន្តបន្ទាប់។
⑩ការរំលោភបំពានណាមួយលើគោលការណ៍មូលដ្ឋាននេះ និងបទប្បញ្ញត្តិរបស់ក្រុមហ៊ុនទាក់ទងនឹងសន្តិសុខព័ត៌មាននឹងត្រូវទទួលពិន័យស្របតាមបទប្បញ្ញត្តិរបស់ក្រុមហ៊ុន។

វិន័យមូលដ្ឋានសុវត្ថិភាព

ចំណុចបំរាម

ប្រើប្រាស់ឧបករណ៍ផ្សេងទៀតក្រៅពីការផ្តល់ដោយក្រុមហ៊ុន

យកកុំព្យូទ័រ ។ល។ របស់ក្រុមហ៊ុនចេញដោយគ្មានការអនុញ្ញាត

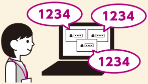
ឧទាហរណ៍៖ ប្រើ USB

ប្រើអង្គផ្ទុកទិន្នន័យខាងក្រៅដោយពុំបានស្នើសុំជាមុន

មើលគេហទំព័រផ្ទាល់ខ្លួនអំឡុងម៉ោងធ្វើការ

ប្រើប្រាស់កម្មវិធី ឬសេវាកម្មដោយគ្មានការអនុញ្ញាត

ចំណុចសំខាន់៖



ការប្រើប្រាស់ពាក្យសម្ងាត់ឡើងវិញ

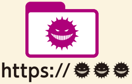
ចុច OK ដោយមិនបានមើលបញ្ជាក់

ពេលប្រើប្រាស់អ៊ីម៉ែល

ចំណុចប្រុងប្រយ័ត្នពេលទទួលអ៊ីម៉ែល

បញ្ជាក់មើលអាសយដ្ឋាននអ៊ីម៉ែលឱ្យបានត្រឹមត្រូវ

មិនឆ្លើយតប/បញ្ជូនតដោយគ្មានការប្រុងប្រយ័ត្ន



មិនបើកមើលឯកសារ ឬ Linkមិនច្បាស់ប្រភព

ចំណុចប្រុងប្រយ័ត្នពេលផ្ញើអ៊ីម៉ែល

បញ្ជាក់មើលខ្លឹមសារ និងអាសយដ្ឋានផ្ញើ

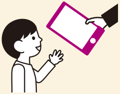
ដាក់ពាក្យសម្ងាត់សម្រាប់ឯកសារសំខាន់

ពេលធ្វើការពីចម្ងាយ (នៅខាងក្រៅក្រុមហ៊ុន)

ចំណុចបំរាម

ភ្ជាប់Wi-Fiសាធារណៈ

ការបង្ហាញជាសាធារណៈដោយអចេតនានូវឯកសារ/ព័ត៌មានដែលបានថតទុក



យកកុំព្យូទ័រ ។ល។ ដែលខ្ចីប្រើជាលក្ខណៈគ្រួសារ

ចំណុចប្រុងប្រយ័ត្ន

ពេលចេញពីកន្លែងអង្គុយត្រូវដាក់លេខសម្ងាត់

ពេលធ្វើដំណើរ មិនត្រូវឃ្លាតពីកុំព្យូទ័រ ។ល។ឡើយ

សំខាន់ ពេលឆ្លងមេរោគត្រូវធ្វើដូចម្តេច! លំហូរនៃដំណោះស្រាយ

ការឆ្លើយតបដំបូង

ដំបូង សូមផ្តាច់ចេញពីបណ្តាញឱ្យបានរហ័ស!

ដកខ្សែ LAN

ផ្តាច់ Wi-Fi

បិតការភ្ជាប់បណ្តាញពីស្មាតហ្វូន

ជម្រើសចុងក្រោយ OFF! គឺបិតម៉ាស៊ីន

រាយការណ៍ពីបញ្ហា

រាយការណ៍ទៅក្រុមហ៊ុនឱ្យបានរហ័ស

រាយការណ៍ ទាក់ទង ពិគ្រោះ

មិនត្រូវដោះស្រាយដោយខ្លួនឯងទេ!

បើមិនអាចទាក់ទងនរណាបាន កុំស្លន់ស្លោ រង់ចាំរហូតដល់ទាក់ទងបាន!

រក្សាទុកស្ថានភាពបច្ចុប្បន្ន

រក្សាទុកស្ថានភាពបច្ចុប្បន្នដើម្បីសិក្សា

កុំប៉ះពាល់កុំព្យូទ័រ *ជាគោលការណ៍គឺមិនត្រូវបិតភ្លើងទេ

ក្នុងករណីបែបនេះ សូមរាយការណ៍ជាបន្ទាន់

បើមានហេតុការណ៍ដូចខាងក្រោម
ត្រូវរាយការណ៍ភ្លាមទៅកាន់ផ្នែកទំនាក់ទំនងបន្ទាន់

កុំព្យូទ័រមានសកម្មភាពមិនប្រក្រតី

ដំណើរការឡើងវិញច្រើនដង

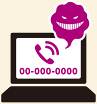
ឃើញមានសញ្ញាមិនស្គាល់

មិនអាចបិត Window

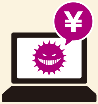
ឯកសារជាប់កូដសម្ងាត់មិនអាចបើកបាន

ទិន្នន័យដែលបានរក្សាទុកពុំឃើញ/ខូច

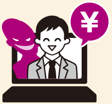
ទំនាក់ទំនងពីភាគីទីបីដែលមានគំនិតអាក្រក់



បង្ហាញលេខទូរស័ព្ទហើយជម្រុញឱ្យទាក់ទង



ទាមទារប្រាក់ជាថ្នូរនឹងការជួសជុល



ទាមទារប្រាក់ដោយធ្វើពុតជាដៃគូអាជីវកម្ម

លំហូរនៃការរាយការណ៍

ការរកឃើញបញ្ហា

គ្រប់អាជីវកម្ម/ក្រុមហ៊ុន/ហាង

ក្រុមហ៊ុនថែទាំ
និងប្រតិបត្តិការប្រព័ន្ធ

ផ្នែករដ្ឋបា
លគ្រប់ក្រុមហ៊ុន

ក្រុមហ៊ុនអ៊ីអន ស្មាត
តិចណូឡូជី ខូ អិលធីឌី

ផ្នែកប្រព័ន្ធរបស់ក្រុមហ៊ុននីមួយៗ
(រួមទាំងវិស័យហិរញ្ញវត្ថុ)

ការរាយការណ៍បញ្ហា (ស្វែងយល់ពីស្ថានភាព)

ក្រុមហ៊ុន អ៊ីអន ផែនការ ICT (ការិយាល័យសន្តិសុខ)
/ផ្នែករដ្ឋបាល

ទំនាក់ទំនង

ការបញ្ជាក់ពីផលប៉ះពាល់ (ការស្វែងយល់ពីផលប៉ះពាល់)

សមាជិកក្រុមគ្រប់គ្រងហានិភ័យ

បង្កើតទីស្នាក់ការកណ្ដា
លគ្រប់គ្រងលើស្ថានភាព

អ្នកគ្រប់គ្រងហាង/អ្នកគ្រប់គ្រង
ផ្នែកជាប្រធានគ្រប់គ្រងប្រព័ន្ធ

ទំនាក់ទំនង

ទំនាក់ទំនង

ប្រធានក្រុមហ៊ុន/អ្នកគ្រប់គ្រងប្រព័ន្ធ
ក្រុមហ៊ុនអ៊ីអន ផ្នែកពាក់ព័ន្ធ

ប្រធាន/អគ្គនាយកក្រុមហ៊ុន/អគ្គនាយករង/នាយកប្រតិបត្តិ

អនុវត្តវិធានការ

៣០នាទី

៣០នាទី