សន្លឹកគន្លឹះស្តីពីសុវត្ថិភាពទិន្នន័យក្នុងការគ្រប់គ្រងទិន្នន័យប្រតិបត្តិការ
ខែមេសា ឆ្នាំ 2022

ការបកប្រែសន្លឹកព័ត៌មានដំនួយនេះត្រូវបានសម្របសម្រួលដោយ CartONG
ដោយអរគុណចំពោះការគាំទ្ររបស់ CLEAR Global និងក្រសួងអឺរ៉ុប និងក្រសួងការបរទេសបារាំង។

សេចក្តីផ្តើម
សុវត្ថិភាពទិន្នន័យគឺជាធាតុផ្សំសំខាន់នៃទំនួលខុសត្រូវទិន្នន័យ៖ ការគ្រប់គ្រងប្រកបដោយសុវត្ថិភាព ក្រមសីលធម៌ និងប្រសិទ្ធភាពនៃទិន្នន័យសម្រាប់ការឆ្លើយតបប្រតិបត្តិការ។
វារួមបញ្ចូលនូវសំណុំនៃវិធានការរួបរួម បច្ចេកវិទ្យា និងនីតិវិធីដែលការពារភាពសម្ងាត់ សុចរិតភាព និងភាពអាចរកបាននៃទិន្នន័យ និងបង្ការការបាត់បង់ដោយខុសច្បាប់ ឬដោយគ្មានការអនុញ្ញាត, ការបំផ្លិចបំផ្លាញ, ការផ្លាស់ប្តូរ, ការទិញ ឬការបើកបង្ហាញដោយចៃដន្យ ឬដោយចេតនា។

សន្លឹកពតគន្លឹះនេះផ្តល់នូវសំណុំនៃសកម្មភាពដែលបានណែនាំសម្រាប់សុវត្ថិភាពទិន្នន័យក្នុងការគ្រប់គ្រងទិន្នន័យប្រតិបត្តិការ។ សកម្មភាពគួរតែត្រូវបានអនុវត្តស្របតាមអាណត្តិ គោលនយោបាយ និងក្របខ័ណ្ឌច្បាប់ និងបទប្បញ្ញត្តិរបស់ស្ថាប័នពាក់ព័ន្ធ។

អនុវត្តការគ្រប់គ្រងពាក្យសម្ងាត់បានល្អ
- ការពារសុវត្ថិភាពឧបករណ៍ និងគណនីរបស់អ្នកជាមួយនឹងពាក្យសម្ងាត់រឹងមាំ ដែលបញ្ចូលលេខ អក្សរធំ និងអក្សរតូច និងនិមិត្តសញ្ញាដែលយ៉ាងហោចណាស់មាន 16+ តួ សម្រាប់មួយពាក្យសម្ងាត់។
- បើកដំណើរការភស្តុតាងបញ្ជាក់ពហុកត្តាសម្រាប់គណនីទាំងអស់។
- កុំប្រើពាក្យសម្ងាត់ដដែលឡើងវិញសម្រាប់គណនីច្រើន។
- កុំរក្សាទុកពាក្យសម្ងាត់របស់អ្នកជារូបវន្ត (ឧ. នៅលើកំណត់ចំណាំ) ឬជាឌីជីថល (ក្នុងឯកសារនៅលើឧបករណ៍របស់អ្នក)
ហើយកុំចែករំលែកពាក្យសម្ងាត់របស់អ្នកជាមួយអ្នកដទៃ។
- កុំបើកមុខងារ 'Remember Me' នៅក្នុងកម្មវិធី និងកម្មវិធីរុករក។
- ផ្លាស់ប្តូរពាក្យសម្ងាត់របស់អ្នកនៅលើគណនីអនឡាញរបស់អ្នកភ្លាមៗ ប្រសិនបើឧបករណ៍របស់អ្នកបានបាត់បង់ ឬត្រូវបានគេលួច។

ប្រើកម្មវិធីកំចាត់មេរោគ/ប្រឆាំងមេរោគ
- សូមប្រាកដថាអ្នកមានកម្មវិធីកំចាត់មេរោគ/ប្រឆាំងមេរោគសមស្របនៅលើឧបករណ៍របស់អ្នក។
- ប្រសិនបើអ្នកមានសំណួរអំពីឧបករណ៍សមស្រប ឬរបៀបកំណត់រចនាសម្ព័ន្ធឧបករណ៍ សូមពិនិត្យជាមួយអ្នកជំនាញផ្នែកព័ត៌មានវិទ្យានៅក្នុងការិយាល័យរបស់អ្នក។

ធ្វើបច្ចុប្បន្នភាពសូវែរ និងប្រព័ន្ធប្រតិបត្តិការ
- សូមពិនិត្យជាប្រចាំអំពីការធ្វើបច្ចុប្បន្នភាពលើឧបករណ៍ សូវែរ កម្មវិធី និងកម្មវិធីជំនួយស្វែងរកកតាមអ៊ីនធឺណិតរបស់អ្នក
និងបើកដំណើរការការធ្វើបច្ចុប្បន្នភាពដោយស្វ័យប្រវត្តិសម្រាប់ប្រព័ន្ធប្រតិបត្តិការរបស់អ្នក។
- សូមប្រើកម្មវិធីរុករកតាមអ៊ីនធឺណិតដូចជា Chrome ឬ Firefox ដែលទទួលបានការធ្វើបច្ចុប្បន្នភាពសុវត្ថិភាពដោយស្វ័យប្រវត្តិ។
- សូមបិទឧបករណ៍នៅចុងបញ្ចប់នៃការប្រើប្រាស់ ដើម្បីធ្វើបច្ចុប្បន្នភាព និងការពារប្រឆាំងនឹងការវាយប្រហារ។

ជៀសវាងតំណឆបោក និងសូមប្រុងប្រយ័ត្ននូវអ្វីដែលអ្នកចុច

- នៅពេលទទួលបានអ៊ីមែល ឬសារគួរឱ្យសង្ស័យ តែងតែពិនិត្យមើលអាសយដ្ឋាន/ព័ត៌មានទំនាក់ទំនងរបស់អ្នកផ្ញើ ហើយគ្រាន់តែចុចលើតំណភ្ជាប់ ឬឯកសារភ្ជាប់ នៅពេលអ្នកទុកចិត្តអ្នកផ្ញើ។
- កុំឆ្លើយតបនឹងអ៊ីមែលដែលគួរឱ្យសង្ស័យ ឬបញ្ជូនបន្តទៅមិត្តរួមការងាររបស់អ្នក។
- រាយការណ៍ពីសកម្មភាពគួរឱ្យសង្ស័យណាមួយទៅកាន់ក្រុមជំនួយផ្នែកព័ត៌មានវិទ្យារបស់អ្នក។

ប្រើឧបករណ៍ចល័តប្រកបដោយការទទួលខុសត្រូវ

- **ប្រសិនបើអាចទៅរួច សូមប្រើឧបករណ៍ដាច់ដោយឡែកសម្រាប់គោលបំណងការងារ។ សូមរក្សាឧបករណ៍ការងាររបស់អ្នកនៅកន្លែងដែលមានសុវត្ថិភាពគ្រប់ពេលវេលា និងជៀសវាងការយកវាទៅតាមខ្លួនដោយមិនចាំបាច់។**
- **ប្រើឧបករណ៍ផ្ទៃសារដែលត្រូវបានអនុម័តដោយស្ថាប័នរបស់អ្នក ដែលមានការផ្តល់នូវការអ៊ិនគ្រីបទាំងមូល។**
- **បិទការភ្ជាប់ប៊ូធូស នៅពេលដែលអាចធ្វើទៅបាន និងកាត់បន្ថយការភ្ជាប់ប៊ូធូស។**
- **ប្រើបណ្តាញឯកជននិម្មិត (VPN) ដែលត្រូវបានអនុម័តដោយស្ថាប័នរបស់អ្នក នៅពេលធ្វើការលើអ៊ីនធឺណិត។ តែងតែចាកចេញពីគណនីរបស់អ្នក ប្រសិនបើអ្នកកំពុងប្រើកុំព្យូទ័រ ឬឧបករណ៍សហគមន៍។**
- **បិទដំណើរការមុខងារដោះសោជីវមាត្រ - ជាពិសេសនៅពេលធ្វើដំណើរ។**

ការពារទិន្នន័យរសើប និងអនុវត្តការបង្រួមអប្បបរមាទិន្នន័យ

- **រក្សា[ការចុះបញ្ជីទ្រព្យសកម្មទិន្នន័យ](#)ដែលបង្ហាញពីកម្រិតនៃភាពរសើបសម្រាប់ប្រភេទទិន្នន័យនីមួយៗដែលគ្រប់គ្រងដោយការិយាល័យរបស់អ្នក។ ពិនិត្យកម្រិតភាពរសើបជាប្រចាំ នៅពេលដែលបរិបទមានការវិវត្ត។**
- **ប្រមូលតែចំនួនអប្បបរមានៃទិន្នន័យដែលត្រូវការដើម្បីសម្រេចបាននូវកម្មវត្ថុ និងគោលបំណងសម្រាប់សកម្មភាពគ្រប់គ្រងទិន្នន័យដែលបានផ្តល់ឱ្យ។**
- **រក្សាទុកតែទិន្នន័យរសើបចាំបាច់ដើម្បីបំពេញគោលបំណងការគ្រប់គ្រងទិន្នន័យ និងតាមការទាមទារដោយការណែនាំ ច្បាប់ និងបទប្បញ្ញត្តិដែលត្រូវអនុវត្ត។**
- **ផ្ទេរ និងរក្សាទុកទិន្នន័យដោយប្រើឧបករណ៍ និងបណ្តាញដែលត្រូវបានអនុម័តដោយស្ថាប័នរបស់អ្នក (នៅលើម៉ាស៊ីនមេ កុំព្យូទ័រ ឬកុំព្យូទ័រយួរដៃនៅក្នុងទីតាំងអង្គភាព។ ឬនៅលើម៉ាស៊ីនមេ និងប្រព័ន្ធដែលដំណើរការពីចម្ងាយតាមរយៈកម្មវិធីដូចជា OneDrive, SharePoint និង Teams)។**
- **ពាក្យសម្ងាត់ការពារឯកសារ (Word, Excel, PDF) ដែលមានផ្ទុកទិន្នន័យរសើប និងចែករំលែកពាក្យសម្ងាត់ឯកសារតាមរយៈបណ្តាញដាច់ដោយឡែក (ឧ. សរសេរពាក្យសម្ងាត់សម្រាប់ឯកសារដែលបានផ្ញើតាមអ៊ីមែល)។**
- **ដាក់ដែនកំណត់ និងតាមដានដោយយកចិត្តទុកដាក់នូវចំនួនបុគ្គលដែលមានសិទ្ធិចូលប្រើទិន្នន័យរសើប ។**
- កំណត់កាលវិភាគរក្សាទុក និងការបំផ្លាញសម្រាប់ទិន្នន័យទាំងអស់ដែលបានគ្រប់គ្រង និងប្រើប្រាស់ឧបករណ៍សមស្របសម្រាប់ការបំផ្លាញទិន្នន័យ។
- អ៊ិនគ្រីបសារអ៊ីមែលរបស់អ្នក។

<u>ធនធានសំខាន់ៗ</u>

- [មគ្គុទេសក៍ណែនាំអំពីប្រតិបត្តិការ IASC ស្តីពីទំនួលខុសត្រូវទិន្នន័យក្នុងសកម្មភាពមនុស្សធម៌](#)
- [មគ្គុទេសក៍ណែនាំអំពីការគ្រប់គ្រងឧប្បត្តិហេតុទិន្នន័យ](#)

- [សន្លឹកគន្លឹះស្តីពីការប្រើប្រាស់ប្រកបដោយការទទួលខុសត្រូវនៃឧបករណ៍សន្និសីទអនឡាញ]

សម្រាប់ព័ត៌មានបន្ថែមអំពីការគ្រប់គ្រងទិន្នន័យរសើបក្នុងប្រតិបត្តិការមនុស្សធម៌ សូមចូលទៅកាន់ទំព័រ ទំនួលខុសត្រូវទិន្នន័យ នៅលើគេហទំព័ររបស់មជ្ឈមណ្ឌល ឬទាក់ទងក្រុមការងាររបស់យើងតាមរយៈ centrehumdata@un.org ។