ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

អាជ្ញាធរសេវាហិរញ្ញវត្ថុមិនមែនធនាគារ
អង្គភាពសវនកម្មផ្ទៃក្នុង
លេខ:...០.២.៤.....អ.ស.ធ.ស.ណ.ស

សេចក្តីណែនាំ
ស្តីពី
សន្តិសុខព័ត៌មាន
របស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃអាជ្ញាធរសេវាហិរញ្ញវត្ថុមិនមែនធនាគារ

សេចក្តីណែនាំនេះ មានគោលបំណងដើម្បីធានាបាននូវសន្តិសុខព័ត៌មានរបស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃអាជ្ញាធរសេវាហិរញ្ញវត្ថុមិនមែនធនាគារ (**អ.ស.ហ.**) ប្រកបដោយប្រសិទ្ធភាព ស្ថិរភាព សុវត្ថិភាព និងគណនេយ្យភាព។

សេចក្តីណែនាំនេះ មានគោលដៅកំណត់នូវនីតិវិធីគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.**។

សេចក្តីណែនាំនេះ មានវិសាលភាពអនុវត្តចំពោះគ្រប់នាយកដ្ឋាន/ អង្គភាព និងក្រុមការងារនៃអង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** ។ អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** សូមដាក់ចេញនូវសេចក្តីណែនាំដូចខាងក្រោម÷

ក. ដើម្បីធានាសុវត្ថិភាពសន្តិសុខព័ត៌មាន មន្ត្រីត្រូវ÷

១. ប្រើប្រាស់ពាក្យសម្ងាត់ (Password) ចាប់ពី ៨ខ្ទង់ឡើងទៅគ្រប់គណនីនៃការប្រើប្រាស់ប្រព័ន្ធព័ត៌មានវិទ្យា ដោយក្នុងនោះរួមមាន អក្សរធំ អក្សរតូច លេខ និងនិមិត្តសញ្ញា។ ឧទាហរណ៍÷ Ad&Ministrator11

២. ប្រើប្រាស់ពាក្យសម្ងាត់ខុសៗគ្នាសម្រាប់គណនីផ្សេងគ្នា ដូចជា÷

គណនីប្រើប្រាស់ម៉ាស៊ីនកុំព្យូទ័ររបស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** គណនីអ៊ីម៉ែលរបស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** គណនី Facebook គណនី Gmail...។ល។

៣. ផ្លាស់ប្តូរពាក្យសម្ងាត់អ៊ីម៉ែលអង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** របស់អ្នកយ៉ាងហោចណាស់រៀងរាល់មួយត្រីមាសម្តង ឬផ្លាស់ប្តូរ ពាក្យសម្ងាត់ភ្លាមៗប្រសិនបើអ្នកសង្ស័យថាគណនីនោះត្រូវបានគេលួច

៤. ដាក់ពាក្យសម្ងាត់នៅលើឯកសារសំខាន់ដែលមាននៅក្នុងម៉ាស៊ីនកុំព្យូទ័រ ម៉ាស៊ីនកុំព្យូទ័រយួរដៃ ដែលជាកម្មសិទ្ធអង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** និងឧបករណ៍ចល័តផ្សេងៗ ដើម្បីជៀសវាងការបែកធ្លាយឯកសារសំខាន់ទាំងនោះ ដែលធ្វើឱ្យប៉ះពាល់ដល់ផលប្រយោជន៍របស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.**

៥. ប្រុងប្រយ័ត្នការក្លែងបន្លំ ឬឆបោកតាមរយៈសារអេឡិចត្រូចនិច ឬតាមរូបភាពផ្សេងៗ ដើម្បីការពារការបាត់បង់ទិន្នន័យ ការឆ្លងមេរោគ និងការលួចយកទិន្នន័យ

៦. លុបទិន្នន័យសម្ងាត់នៅក្នុងម៉ាស៊ីនកុំព្យូទ័ររបស់អ្នកឱ្យបានត្រឹមត្រូវចេញពីធុងសម្រាម (Recycle Bin) នៅពេលដែលអ្នកលែងត្រូវការ

៧. ចាក់សោរ (Lock) ម៉ាស៊ីនកំព្យូទ័ររបស់អ្នកនៅពេលដែលមិនបានប្រើប្រាស់ ដើម្បីការពារទិន្នន័យពីការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត

៨. រាយការណ៍គ្រប់សកម្មភាពសង្ស័យទាំងអស់ និងឧប្បត្តិហេតុតាមប្រព័ន្ធ Internet មកកាន់ការិយាល័យគ្រប់គ្រងព័ត៌មានវិទ្យា ដើម្បីទប់ស្កាត់ឱ្យបានទាន់ពេលវេលា និង

៩. រាយការណ៍ភ្លាមៗទៅកាន់ការិយាល័យគ្រប់គ្រងព័ត៌មានវិទ្យា នៅពេលដែលអ្នកបាត់បង់ម៉ាស៊ីនកុំព្យូទ័រយួរដៃដែលជាកម្មសិទ្ធិរបស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** ដើម្បីទប់ស្កាត់ការលួចយកព័ត៌មានរបស់អ្នកឱ្យបានទាន់ពេលវេលា។

ខ. ដើម្បីធានាសុវត្ថិភាពសន្តិសុខព័ត៌មាន មន្ត្រីមិនត្រូវ÷

១. ចែករំលែក ឬសរសេរពាក្យសម្ងាត់របស់អ្នកទៅឱ្យអ្នកដទៃ

២. ប្រើប្រាស់ព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នកដូចជាឈ្មោះ ថ្ងៃខែឆ្នាំកំណើត និងលេខទូរសព្ទធ្វើជាពាក្យសម្ងាត់

៣. ប្រកាសព័ត៌មានសម្ងាត់របស់ស្ថាបនទៅបុគ្គលផ្សេងទៀត ឬផ្សព្វផ្សាយនៅលើគេហទំព័រសាធារណៈ ប្រព័ន្ធបណ្តាញសង្គម ឬតាមរូបភាពផ្សេងៗដោយគ្មានការអនុញ្ញាតពីថ្នាក់ដឹកនាំរបស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.**

៤. ជ្រើសរើសយកពាក្យថាចងចាំ (Remember Me) នៅលើគេហទំព័រណាមួយនៅពេលដែលអ្នកចូលទៅប្រើប្រាស់គណនីរបស់អ្នកនៅលើម៉ាស៊ីនកុំព្យូទ័ររបស់អ្នកដទៃ ជាពិសេសនៅលើម៉ាស៊ីនកុំព្យូទ័រសាធារណៈ

៥. រក្សាទុកឯកសារសម្ងាត់របស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** នៅលើម៉ាស៊ីនកុំព្យូទ័រ ឬ Cloud ផ្សេងក្រៅពីម៉ាស៊ីនកុំព្យូទ័រ ឬ Cloud របស់អង្គភាព។ ឧទាហរណ៍: Google Drive, Dropbox, One Drive... និង

៦. បើកឯកសារដែលគ្មានប្រភពច្បាស់លាស់នៅក្នុងម៉ាស៊ីនកុំព្យូទ័ររបស់អ្នក ដើម្បីជៀសវាងការឆ្លងមេរោគចូលម៉ាស៊ីនកុំព្យូទ័រ ដែលបណ្តាលឱ្យបាត់បង់ឯកសារជាយថាហេតុ។

គ. វិធានការរដ្ឋបាល÷

អង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** នឹងចាត់វិធានការខាងវិន័យរដ្ឋបាលចំពោះបុគ្គលទាំងឡាយដែលអនុវត្តន៍ផ្ទុយពីខ្លឹមសារនៃសេចក្តីណែនាំខាងលើ។

មន្ត្រីក្រោមឱវាទអង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.** ទាំងអស់ត្រូវអនុវត្តន៍នូវសេចក្តីណែនាំស្តីពីសន្តិសុខព័ត៌មាន របស់អង្គភាពសវនកម្មផ្ទៃក្នុងនៃអាជ្ញាធរសេវាហិរញ្ញវត្ថុមិនមែនធនាគារឱ្យមានប្រសិទ្ធភាពចាប់ពីថ្ងៃចុះហត្ថលេខាតទៅ។

ថ្ងៃ ព្រហស្បតិ៍ ១១កើត ខែ ផល្គុន ឆ្នាំថោះ បញ្ចស័ក ព.ស. ២៥៦៧

រាជធានីភ្នំពេញ ថ្ងៃទី ៣០ ខែ មេសា ឆ្នាំ២០២៣

អង្គភាពសវនកម្មផ្ទៃក្នុង

ប្រធាន

ឈុន សម្បត្តិ

ចម្លងជូន÷

- ឯកឧត្តមប្រធានអង្គភាព
- លោកអនុប្រធានអង្គភាព
- គ្រប់នាយកដ្ឋានអង្គភាពសវនកម្មផ្ទៃក្នុងនៃ **អ.ស.ហ.**
- ឯកសារ-កាលប្បវត្តិ