៦.៥.៧. ការស្វែងរកព័ត៌មានលើបណ្តាញអ៊ីនធឺណិត

(ក) វិធាន

ទិដ្ឋភាពទូទៅ

(ក១) មិនត្រូវទាញយក (Download) ឯកសារដែលអាចដំណើរការបាន (Executable File) ក្នុងប្រព័ន្ធប្រតិបត្តិការកុំព្យូទ័រ ដោយគ្មានការអនុញ្ញាតពីប្រធានគ្រប់គ្រងសន្តិសុខព័ត៌មានឡើយ។

(ក២) អាចទាញយក (Download) តែឯកសារណា ដែលមានវិញ្ញាបនប័ត្រ ឬអាជ្ញាប័ណ្ណប៉ុណ្ណោះ។

(ក៣) មិនត្រូវចុចភ្ជាប់បន្ត (Link) ទៅកាន់គេហទំព័រ ឬសារអេឡិចត្រូនិចណាមួយផ្សេងទៀត ដែលមិនបានស្គាល់ច្បាស់លាស់ឡើយ។

(ក៤) វាជាការប្រសើរបំផុត ដែលអាចជៀសវាងការរក្សាទុកឃុគឃី (Cookies) ដែលអាចធ្វើឲ្យមានការលេចធ្លាយនូវព័ត៌មានទាក់ទងនឹងអត្តសញ្ញាណអ្នកប្រើប្រាស់ (User ID) និងលេខ ឬពាក្យសម្ងាត់ (Password)។

(ក៥) កំណត់នៅក្នុងកម្មវិធីមើលគេហទំព័រ (Web Browser) ដែលទាក់ទងទៅនឹងចំនុចដែលបានរៀបរាប់ខាងលើ។

បញ្ហាមិនសមរម្យ

(ក៦) ការិយាល័យសន្តិសុខព័ត៌មាននៃ អ.អ.ប.គ.ព ក៏ដូចជាការិយាល័យសន្តិសុខព័ត៌មាន

តាមបណ្តាស្តាប័ន មិនអនុញ្ញាតអោយមានប្រើប្រាស់ឯកសារ រូបភាព រូបភាពវីដេអូ ឬសារអេឡិចត្រូនិចមិនសមរម្យ ដែលបង្ហាញពីភាពអាសគ្រាម ការប្រកាន់ពូជសាសន៍ ការបង្ខូចកេរ្តិ៍ឈ្មោះ ឬការរំខាននានា ដែលអាចបង្កឲ្យមានការអាក់អន់ចិត្ត ឬភាពអាម៉ាស់ឡើយ។ មិនត្រូវរក្សាទុក ចំលង ប្រើប្រាស់ ឬចរាចរនូវអ្វីដែលបានរៀបរាប់ខាងលើ និងជៀសវាងចូលទៅប្រើប្រាស់ គេហទំព័រណាមួយដែលគួរឲ្យសង្ស័យ។ ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវត្រួតពិនិត្យបណ្តាញកុំព្យូទ័រ និងប្រព័ន្ធផ្សេងៗជាប្រចាំដើម្បីការពារកុំឲ្យមានការប្រើប្រាស់ ឬចរាចរនូវអ្វីដែលបានរៀបរាប់ខាងលើ និងធ្វើការតាមដានរាល់ការប្រើប្រាស់អ៊ីនធឺណិត បើរកឃើញនៅកំហុសណាមួយ ការិយាល័យនេះនឹងរាយការណ៍ដោយផ្ទាល់អំពីសកម្មភាពរបស់អ្នកដែលបានប្រព្រឹត្តខុសធ្ងន់ធ្ងរ ឬច្រំដែរ ទៅកាន់នាយកផ្នែកសន្តិសុខព័ត៌មាន មុននឹងមានការចាត់វិធានការដាក់វិន័យកើតឡើង។

- ប្រសិនបើលោកអ្នកទទួលបាននូវឯកសារណាមួយ មិនសមរម្យតាមរយៈសារអេឡិចត្រូនិច ឬតាមមធ្យោបាយផ្សេងៗ ត្រូវលុបចោលរបស់ឯកសារទាំងនោះជាបន្ទាន់។
- ប្រសិនបើលោកអ្នកបានចូលទៅកាន់គេហទំព័រណាមួយ មិនសមរម្យដោយចៃដន្យ ត្រូវចុចលើប៊ូតុង ត្រលប់ក្រោយ (Back) ឬបិទផ្ទាំងកម្មវិធីវីនដូ (Window) តែម្តង។
- ប្រសិនបើលោកអ្នកទទួលបានស្ពែម (Spam) ជាប្រចាំ ត្រូវរាយការណ៍ទៅកាន់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានដើម្បីត្រួតពិនិត្យ និងផ្តល់នីតិវិធីដោះស្រាយ។

(ខ) នីតិវិធី(សំរាប់ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន)

កំណត់មុខងារត្រួតពិនិត្យលើ កម្មវិធីមើលគេហទំព័រ (Web Browser)

(ខ១) នីតិវិធីខាងក្រោមនេះត្រូវបានបង្កើតឡើង ដើម្បីត្រួតពិនិត្យការកំណត់ក្នុងកម្មវិធីបើកមើលគេហទំព័រ (Web Browser)

ជំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	ដាក់ចេញនូវផែនការ និងរៀបចំការត្រួតពិនិត្យលើមុខងារក្នុងកម្មវិធីមើលគេហទំព័រដូចជា កាលបរិច្ឆេទ និងកុំព្យូទ័រដែលត្រូវប្រើជាគំរូ។ហើយធ្វើការណែនាំ មុនពេលធ្វើការត្រួតពិនិត្យ។	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.២	ដាក់ចេញនូវផែនការ និងរៀបចំការត្រួតពិនិត្យលើមុខងារក្នុងកម្មវិធីមើលគេហទំព័រម្តងមួយៗ។ នៅពេលដែលរកឃើញនូវចំនុចដែលមិនសមស្រប ត្រូវណែនាំម្ចាស់កុំព្យូទ័រឲ្យធ្វើការកែតម្រូវ។	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.៣	ដាក់ជូននូវរបាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មានប្រសិនបើបានរកឃើញនូវចំនុចដែលមិនសមរម្យ	អ្នកប្រើប្រាស់	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន
ខ១.៤	តម្កល់ទុករបាយការណ៍ទាំងនេះ និងរក្សាទុកសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

៦.៦. <u>សន្តិសុខបណ្តាញ កុំព្យូទ័រ និង ម៉ាស៊ីនកុំព្យូទ័រមេ (Server) ដែលនឹងត្រូវកំណត់ដោយពេញលេញនាពេលអនាគត</u>

៦.៦.១. <u>បណ្តាញកុំព្យូទ័រខាងក្នុង (LAN) និងប្រព័ន្ធអ៊ីនធឺណិត</u>

(ក) ទិដ្ឋាន

ពន្យារការអនុវត្តន៍

ផ្នែកនេះនឹងអនុវត្តនៅលើ ប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យានៃរាជរដ្ឋាភិបាលកម្ពុជា នៃអាជ្ញាធរជាតិ អ.អ.ប.គ.ព។ ឯកសារណែនាំស្តីអំពីការគ្រប់គ្រងប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យា និងបណ្តាញជាតិ និងត្រូវបង្កើតឡើង។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៦.២. <u>ម៉ាស៊ីនកុំព្យូទ័រមេ (Server)</u>

(ក) ទិដ្ឋាន

ពន្យារការអនុវត្តន៍

ផ្នែកនេះនឹងអនុវត្តនៅលើប្រព័ន្ធរដ្ឋបាលព័ត៌មានវិទ្យានៃរាជរដ្ឋាភិបាលកម្ពុជា នៃអាជ្ញាធរជាតិ អ.អ.ប.គ.ព។ ឯកសារណែនាំស្តីអំពីការគ្រប់គ្រងប្រព័ន្ធ រដ្ឋបាលព័ត៌មានវិទ្យានិងបណ្តាញជាតិ និងត្រូវបង្កើតឡើង។

(ខ) នីតិវិធី

(មិនមាននីតិវិធីដែលបានអនុវត្តណាមួយ ត្រូវបានរៀបរាប់នៅក្នុងផ្នែកនេះទេ)

៦.៧. <u>សន្តិសុខកម្មវិធីប្រើប្រាស់ (Application) នឹងត្រូវបានកំណត់នាពេលអនាគត់</u>

(ក) ទិដ្ឋាន

(ផ្នែកនេះធ្វើការកំណត់អំពីតម្រូវការសន្តិសុខព័ត៌មាន និងអំពីបញ្ហានានានៃគំរោងបង្កើតកម្ម

វិធីប្រើប្រាស់)

៧. ការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មាន

៧.១. ដំណើរការនៃការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មាន

មន្ត្រីគ្រប់រូបត្រូវទទួលការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មាន យ៉ាងតិចម្តងជារៀងរាល់ឆ្នាំ។ នីតិវិធីខាងក្រោមកំណត់នូវការរៀបចំផែនការ និងការអនុវត្តន៍ការងារបណ្តុះបណ្តាល ផ្នែកសន្តិសុខព័ត៌មាន។

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ១.១	រៀបចំផែនការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មានសំរាប់ទាំងមន្ត្រីដែលមានបទពិសោធន៍ និងមន្ត្រីដែលទើបជ្រើសរើសថ្មី	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.២	អនុវត្តការបណ្តុះបណ្តាល	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន
ខ១.៣	កត់ត្រាព័ត៌មានទាក់ទងនឹងមន្ត្រីដែលបានចូលរួមក្នុងវគ្គបណ្តុះបណ្តាល និងរក្សាទុកកំណត់ត្រានេះសំរាប់រយៈកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	កំណត់ត្រាអំពីការបណ្តុះបណ្តាល

៧.២. ការផ្តល់លិខិតកិច្ចសន្យា

មន្ត្រីទាំងអស់ត្រូវការផ្តល់លិខិតកិច្ចសន្យាយ៉ាងតិចម្តង ដើម្បីការពារសន្តិសុខព័ត៌មាន។ វាជាការប្រសើរមួយ ដែលលោកអ្នកបានចុះហត្ថលេខា រាល់ពេលចូលរួមវគ្គបណ្តុះបណ្តាល។ នីតិវិធីខាងក្រោមធ្វើការកំណត់អំពីបែបបទនៃការផ្តល់លិខិតកិច្ចសន្យា។

ដំណាក់កាល	សេចក្តីអធិប្បាយ	អ្នកអនុវត្ត	បញ្ជីព័ត៌មាន
ខ២.១	ចែកចាយលិខិតសន្យាដែលមិនទាន់បំពេញព័ត៌មាន	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	មិនមាន
ខ២.២	អានអត្ថន័យក្នុងលិខិតទាំងមូល ចុះហត្ថលេខាក្នុងលិខិត និងដាក់បញ្ចូនលិខិត	អ្នកប្រើប្រាស់	លិខិតសន្យា
ខ២.៣	តម្កល់ ឬក្សាទុកលិខិតទាំងនេះសំរាប់រយៈពេលកំណត់ណាមួយ	មន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន	មិនមាន

៨. ការវាយតំលៃ

បញ្ហាមួយចំនួនខាងក្រោម នឹងត្រូវបានវាយតំលៃពីមន្ត្រីទទួលខុសត្រូវផ្នែកសន្តិសុខព័ត៌មាន និងរាយការណ៍ទៅ ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មានយ៉ាងតិចម្តងក្នុងមួយឆ្នាំ។ របាយការណ៍នេះនឹងជំរុញការលើកកម្ពស់ប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន យោងតាមសេចក្តីលំអិតនៃទិសដៅនីមួយៗ។

ល.រ	បញ្ហាដែលត្រូវវាស់វែត	និយមន័យ	អនុញ្ញាតដោយ
១	កំរិតនៃការបញ្ចប់ការបណ្តុះបណ្តាល	% នៃមន្ត្រីដែលបានបញ្ចប់វគ្គបណ្តុះបណ្តាល ក្នុងចំណោមមន្ត្រីស្ថាប័នដែលបានចូលរួម	ប្រធានស្ថាប័ននិងផ្នែកពាក់ព័ន្ធ
២	ហេតុការណ៍នៃសន្តិសុខព័ត៌មានស្របពេលនិងការបញ្ចប់ដំណើរការតាមប្រភេទហេតុការណ នីមួយៗ	រូបមន្តនៃការបូកបញ្ចូល (ពេលវេលាសំរាប់បញ្ចប់ដំណើរការដោះស្រាយបញ្ហា ដកចំនួនពេលវេលាដែលកើតហេតុការណ៍) ហើយចែកនឹងចំនួនហេតុការណ៍ដែលបានបែងចែកតាមប្រភេទគុណនិងចំនួន(ប្រភេទហេតុការណ៍	នាយកផ្នែកសន្តិសុខព័ត៌មាន

		នីមួយៗត្រូវបានកំណត់នៅក្នុងរបាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន ដែលមិនទាន់បំពេញព័ត៌មាន)	
៣	កំរិតនៃប្រតិបត្តិការរុករក (Scan) មេរោគ	% នៃមន្ត្រីក្នុងចំណោមមន្ត្រី អ.អ.ប.គ.ព ទាំងអស់ដែលបានបំពេញការងាររុករក (Scan) មេរោគ ក្នុងកំឡុងពេលអនុវត្តនីតិវិធីការពារការឆ្លងមេរោគ	នាយកផ្នែកសន្តិសុខព័ត៌មាន
៤	កំរិតនៃការឆ្លង លិខិតកិច្ចសន្យា	% នៃមន្ត្រីដែលបានឆ្លងលិខិតកិច្ចសន្យា ក្នុងចំណោមមន្ត្រី អ.អ.ប.គ.ព ទាំងអស់	នាយកផ្នែកសន្តិសុខព័ត៌មាន
	-ផ្នែកចុងក្រោយនៃបញ្ជី-		

៩. ទោសប្បញ្ញត្តិ (នឹងត្រូវបានកំណត់នាពេលអនាគត)

(ក) ទិដ្ឋាន

(ផ្នែកនេះធ្វើការកំណត់អំពីទោសប្បញ្ញត្តិ ទាក់ទងនឹងការបំពានច្បាប់សន្តិសុខព័ត៌មាន។ វាតម្រូវឲ្យមានការរៀបចំរបៀបរៀបរយ ធនធានមនុស្សផ្ទៃក្នុង សំរាប់មន្ត្រីរាជការទាំងអស់។)

១០. បញ្ជីកំណត់ត្រាព័ត៌មាន

ល.រ	ឈ្មោះបញ្ជី	ឯកសារយោង	ធ្វើសេចក្តីព្រាងដោយ	អនុញ្ញាតដោយ
១	បញ្ជីព័ត៌មានស្តីអំពីការបណ្តុះបណ្តាល	ជំពូកទី ៧.១៖ ដំណើរការនៃការបណ្តុះបណ្តាលផ្នែកសន្តិសុខព័ត៌មាន	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	ប្រធានស្ថាប័ន និងផ្នែកពាក់ព័ន្ធ

២	របាយការណ៍ស្តីអំពីហេតុការណ៍ទាក់ទងនឹងសន្តិសុខព័ត៌មាន	(១) នីតិវិធីនៃចំណាត់ការក្នុងការចាប់មេរោគនៅក្នុងជំពូកទី៦.៥.១៖ កុំព្យូទ័រលើតុ (២) នីតិវិធីនៃវិធានការគ្រប់គ្រង សម្ភារៈដែលបានបាត់បង់ឬត្រូវបានលួចនៅក្នុងជំពូកទី ៦.៥.២៖ កុំព្យូទ័រយួរដៃ ឬ កុំព្យូទ័រចល័ត (៣) នីតិវិធីនៃការពិនិត្យមើលអំពីការកំណត់ព័ត៌មានរបស់កម្មវិធី (កុំព្យូទ័រ) នៅក្នុងជំពូកទី ៦.៥.៥៖ កម្មវិធី (ប្រព័ន្ធកុំព្យូទ័រ) (៤) នីតិវិធីនៃវិធានការទូទៅសំរាប់ដោះស្រាយបញ្ហាទាក់ទងនឹងសន្តិសុខព័ត៌មាននៅក្នុងជំពូកទី ៦.៥.៦៖សារអេឡិចត្រូនិច (E-mail) (៥) នីតិវិធីនៃការពិនិត្យមើលអំពីការកំណត់ព័ត៌មានរបស់មុខងារសំរាប់ស្វែងរកព័ត៌មាន	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	ប្រធានស្តាប័ន និងផ្នែកពាក់ព័ន្ធ

		លើបណ្តាញអ៊ីនធឺណិត (web browser) នៅក្នុងជំពូកទី៦.៥.៦៖ ការស្វែងរកព័ត៌មានលើបណ្តាញអ៊ីនធឺណិត		
៣	បញ្ជីព័ត៌មានស្តីអំពីការរុករក (Scan) មេរោគ	នីតិវិធីនៃចំណាត់ការក្នុងការចាប់មេរោគនៅក្នុងជំពូកទី៦.៥.១៖ កុំព្យូទ័រលើតុ	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	ប្រធានស្តាប័ន និងផ្នែកពាក់ព័ន្ធ
៤	លិខិតសន្យា	ជំពូកទី ៧.២៖ ការដាក់ជូនលិខិតសន្យា	ការិយាល័យគ្រប់គ្រងសន្តិសុខព័ត៌មាន	ប្រធានស្តាប័ន និងផ្នែកពាក់ព័ន្ធ
	-ផ្នែកចុងក្រោយនៃបញ្ជី			