ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ
លេខ.៧៤៣៦.....សហវ.ប្រក.

ប្រកាស

ស្តីពី

ការដាក់ឱ្យប្រើប្រាស់ឯកសារស្តីពី

ការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

ទេសរដ្ឋមន្ត្រី រដ្ឋមន្ត្រីក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

- បានឃើញរដ្ឋធម្មនុញ្ញនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកត/០៩១៣/៩០៣ ចុះថ្ងៃទី២៤ ខែកញ្ញា ឆ្នាំ២០១៣ ស្តីពីការតែងតាំងរាជរដ្ឋាភិបាលនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកត/១២១៣/១៣៩៣ ចុះថ្ងៃទី២១ ខែធ្នូ ឆ្នាំ២០១៣ ស្តីពីការកែសម្រួល និងបំពេញបន្ថែមសមាសភាពរាជរដ្ឋាភិបាលនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រមលេខ ០២/នស/៩៤ ចុះថ្ងៃទី២០ ខែកក្កដា ឆ្នាំ១៩៩៤ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីការរៀបចំនិងការប្រព្រឹត្តិទៅនៃគណៈរដ្ឋមន្ត្រី
- បានឃើញព្រះរាជក្រមលេខ នស/រកម/០១៩៦/១៨ ចុះថ្ងៃទី២៤ ខែមករា ឆ្នាំ១៩៩៦ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីការបង្កើតក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ
- បានឃើញព្រះរាជក្រមលេខ នស/រកម/០៣០០/១០ ចុះថ្ងៃទី០៣ ខែមីនា ឆ្នាំ២០០០ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីសវនកម្មនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រមលេខ នស/រកម/០៥០៨/០១៦ ចុះថ្ងៃទី១៣ ខែឧសភា ឆ្នាំ២០០៨ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីប្រព័ន្ធហិរញ្ញវត្ថុសាធារណៈ
- បានឃើញអនុក្រឹត្យលេខ ៤៨៨/អនក្រ/បក ចុះថ្ងៃទី១៦ ខែតុលា ឆ្នាំ២០១៣ ស្តីពីការរៀបចំនិងការប្រព្រឹត្តទៅនៃក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ
- បានឃើញអនុក្រឹត្យលេខ ៤០/អនក្រ/បក ចុះថ្ងៃទី១៥ ខែកុម្ភៈ ឆ្នាំ២០០៥ ស្តីពីការរៀបចំនិងការប្រព្រឹត្តិទៅនៃសវនកម្មផ្ទៃក្នុងនៅតាមបណ្តាស្ថាប័ន ក្រសួង និងសហគ្រាសសាធារណៈ
- បានឃើញប្រកាសលេខ ១៥៤៧ សហវ.ប្រក ចុះថ្ងៃទី៣១ ខែធ្នូ ឆ្នាំ២០១៣ ស្តីពីការរៀបចំនិងការប្រព្រឹត្តិទៅនៃនាយកដ្ឋាននិងអង្គភាពក្រោមឱវាទអគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុងនៃក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

ផ្លូវលេខ ៩២ សង្កាត់វត្តភ្នំ ខ័ណ្ឌដូនពេញ រាជធានីភ្នំពេញ កម្ពុជា
St,92, Sangkat Wat Phnom, Khan Daun Penh, Phnom Penh, CAMBODIA.
ទូរស័ព្ទ : ៨៥៥-២៣-៧២៤ ៦៦៤ ទូរសារ : ៨៥៥-២៣-៤២៧ ៧៨៩
Phone : 855-23-724 664 Fax : 855-23-427 789

- បានឃើញប្រកាសលេខ ៧៣៩ សហវ.ប្រក ចុះថ្ងៃទី២៣ ខែមិថុនា ឆ្នាំ២០១៦ ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃនាយកដ្ឋានសវនកម្មបច្ចេកវិទ្យាព័ត៌មាននៃអគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុងនៃក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ
- បានឃើញប្រកាសលេខ ៤០៥ សហវ ចុះថ្ងៃទី៣១ ខែឧសភា ឆ្នាំ២០០៦ ស្តីពីការដាក់ឱ្យប្រើប្រាស់ឯកសារក្រមសីលធម៌សម្រាប់សវនករផ្ទៃក្នុង និងស្តង់ដាវិជ្ជាជីវៈសវនកម្មផ្ទៃក្នុង
- បានឃើញប្រកាសលេខ ២៩៥ សហវ.ប្រក ចុះថ្ងៃទី១៩ ខែមីនា ឆ្នាំ២០១៣ ស្តីពីការដាក់ឱ្យប្រើប្រាស់ឯកសារបច្ចុប្បន្នកម្មនៃគោលនយោបាយស្តីពីការគ្រប់គ្រងផ្ទៃក្នុង
- បានឃើញសារាចរណែនាំលេខ ១២ សរណន ចុះថ្ងៃទី២៥ ខែវិច្ឆិកា ឆ្នាំ២០១១ ស្តីពីការបន្តពង្រឹងមុខងារសវនកម្មផ្ទៃក្នុងតាមបណ្តាក្រសួង ស្ថាប័ន និងសហគ្រាសសាធារណៈ
- ផ្អែកតាមការចាំបាច់របស់ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

សម្រេច

ប្រការ ១.

ត្រូវបានដាក់ឱ្យប្រើប្រាស់នូវឯកសារស្តីពី "ការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន" សម្រាប់ការរៀបចំការគ្រប់គ្រង និងការត្រួតពិនិត្យលើប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាននៅតាមបណ្តាក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈរបស់រាជរដ្ឋាភិបាលពាក់ព័ន្ធ ដូចមានភ្ជាប់ជាមួយប្រកាសនេះ។

ប្រការ ២.

គ្រប់ក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈរបស់រាជរដ្ឋាភិបាលត្រូវទទួលអនុវត្តប្រកាសនេះឱ្យមានប្រសិទ្ធភាពខ្ពស់។

ប្រការ ៣.

ប្រកាសនេះមានប្រសិទ្ធភាពអនុវត្តចាប់ពីថ្ងៃចុះហត្ថលេខាតទៅ។

រាជធានីភ្នំពេញ ថ្ងៃទី០៨ ខែកុម្ភៈ ឆ្នាំ២០១៦

ទេសរដ្ឋមន្ត្រី

រដ្ឋមន្ត្រីក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

បណ្ឌិត. អូន ព័ន្ធមុនីរ័ត្ន

កន្លែងទទួល:
-ទីស្តីការគណៈរដ្ឋមន្ត្រី
-អគ្គលេខាធិការរាជរដ្ឋាភិបាល
-ខុទ្ទកាល័យសម្តេច អគ្គមហាសេនាបតីតេជោនាយករដ្ឋមន្ត្រី
-ខុទ្ទកាល័យសម្តេច ឯកឧត្តម លោកជំទាវឧបនាយករដ្ឋមន្ត្រី
-គ្រប់ក្រសួង ស្ថាប័ន
-ដូចប្រការ ២
-រាជកិច្ច
-ឯកសារ-កាលប្បវត្តិ

ព្រះរាជាណាចក្រកម្ពុជា

ជាតិ សាសនា ព្រះមហាក្សត្រ

ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

អគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុង

ការគ្រប់គ្រងប្រព័ន្ធ

ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកទិទ្យាព័ត៌មាន

ឆ្នាំ ២០១៦

មាតិកា

ទំព័រ

សេចក្តីផ្តើម

ក្នុងបរិការណ៍បច្ចុប្បន្ន ដំណើរការគ្រប់គ្រងផ្ទៃក្នុងរបស់ក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈនៃរាជរដ្ឋាភិបាលនៅអនុវត្តដោយដៃភាគច្រើននៅឡើយ។ យ៉ាងណាមិញ ក្នុងគោលដៅទំនើបភាវូបនីយកម្មនិងធានាឱ្យបានន្លូវប្រសិទ្ធភាព តម្លាភាព ភាពឆាប់រហ័សនៃការត្រួតពិនិត្យផ្ទៃក្នុងនៃរាជរដ្ឋាភិបាលនាពេលខាងមុខ រាល់ដំណើរការគ្រប់គ្រងផ្ទៃក្នុងក៏ដូចជាកិច្ចបញ្ជិកានានានឹងត្រូវធ្វើឡើងដោយប្រព័ន្ធកុំព្យូទ័រ។

ការរីកចម្រើននៃស្ថ័យប្រវត្តកម្មដំណើរការធុរកិច្ច នឹងមិនធ្វើឱ្យមានការប្រែប្រួលដល់គោលបំណងនៃការគ្រប់គ្រងឬសវនកម្មផ្ទៃក្នុងទេ ក៏ប៉ុន្តែវានឹងនាំមកន្លូវហានិភ័យថ្មីៗដែលងាយនឹងក្លាយជាប្រភពកំហុសថ្មី។ ទន្ទឹមនឹងនេះ ភាពរូបីនៃចម្ងងការត្រូវបានកាត់បន្ថយ ដែលតម្រូវឱ្យថ្នាក់ដឹកនាំនិងសវនករអនុវត្តវិធីសាស្ត្រ និងបច្ចេកទេសត្រួតពិនិត្យថ្មី។ ក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈរបស់រាជរដ្ឋាភិបាល ត្រូវធ្វើការផ្លាស់ប្តូរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង ដែលមាននាពេលបច្ចុប្បន្ន ដើម្បីបង្ការនិងកាត់បន្ថយហានិភ័យ។

បន្ទាប់ពីការដាក់ឱ្យប្រើប្រាស់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (Information Technology System) ប្រព័ន្ធនេះនឹងក្លាយជាផ្នែកមួយដ៏សំខាន់នៃយន្តការត្រួតពិនិត្យផ្ទៃក្នុង ហើយអាចសម្រេចបានជោគជ័យអាស្រ័យជាចម្បងលើគុណភាពនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដែលពាក់ព័ន្ធ។

អាស្រ័យហេតុនេះ ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុបានរៀបចំឯកសារស្តីពីការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាននៃក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រើប្រាស់សម្រាប់ការតាក់តែង គ្រប់គ្រង និងវាយតម្លៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។ ម្យ៉ាងទៀត ឯកសារនេះ ក៏ផ្តល់ជូនសវនករផ្ទៃក្នុងន្លូវលក្ខណៈវិនិច្ឆ័យ សម្រាប់ការធ្វើសវនកម្មលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មានដែលបាន ដាក់អនុវត្តដោយថ្នាក់ដឹកនាំនៃក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈ។

ការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មានចែកជាពីរផ្នែក ÷

- ផ្នែក ក: គោលនយោបាយត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន
- ផ្នែក ខ: គោលការណ៍ និងស្តង់ដារត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន។

ផ្នែក ក: គោលនយោបាយត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

១. ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (បបព)

ព័ត៌មានគឺជាបណ្តុំនៃទិន្នន័យ ដែលអាចជាព័ត៌មានហិរញ្ញវត្ថុ និងមិនមែនហិរញ្ញវត្ថុ និងត្រូវបានផ្តល់ជូនថ្នាក់ដឹកនាំដើម្បីធ្វើការសម្រេចចិត្ត។ ទន្ទឹមនឹងនេះ ព័ត៌មានគឺជាទ្រព្យសកម្មមួយដូចទ្រព្យសកម្មនៃធុរកិច្ចសំខាន់ៗដទៃទៀតដែលមានតម្លៃដល់អង្គភាព និងទាមទារកិច្ចការពារឱ្យបានហ្មត់ចត់។

បបព សំដៅដល់អ្នកពាក់ព័ន្ធ ដំណើរការ និងបច្ចេកវិទ្យាដែលអាចផ្តល់នូវព័ត៌មានតាមតម្រូវការដោយស្វ័យប្រវត្តិ។ ដូច្នេះ បបព ក៏តម្រូវឱ្យមានកិច្ចការពារដូចប្រព័ន្ធព័ត៌មានដទៃទៀតដែរ។ គោលនយោបាយនេះ ផ្តោតសំខាន់ទៅលើការចាត់ចែងរបស់ថ្នាក់ដឹកនាំ នៅក្នុងការតាក់តែង ការដាក់អនុវត្ត ការថែរក្សា ដើម្បីទទួលបាន បបព មួយដែលមានប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងសមស្រប និងគ្រប់គ្រាន់។

២. និយមន័យនៃការត្រួតពិនិត្យផ្ទៃក្នុង

ការត្រួតពិនិត្យផ្ទៃក្នុងគឺជាដំណើរការអនុវត្តដោយថ្នាក់ដឹកនាំ និងបុគ្គលិកផ្សេងទៀតត្រូវបានរៀបចំឡើងដើម្បីផ្តល់ការធានាដល់ការសម្រេចបាននូវគោលដៅដូចខាងក្រោម ÷

- របាយការណ៍ហិរញ្ញវត្ថុដែលអាចជឿទុកចិត្តបាន
- ប្រសិទ្ធភាព និងប្រសិទ្ធផលនៃប្រតិបត្តិការ
- អនុលោមភាពជាមួយច្បាប់ និងបទប្បញ្ញត្តិ ។

៣. គោលបំណងនៃការត្រួតពិនិត្យផ្ទៃក្នុង

គោលបំណងនៃការត្រួតពិនិត្យផ្ទៃក្នុង គឺដើម្បីធានាឱ្យបាននូវគោលដៅ ឬលក្ខខណ្ឌដែលអាចកាត់បន្ថយដល់កម្រិតអប្បបរមាលើការខ្ជះខ្ជាយ ការបាត់បង់ ការប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត ឬការបែងចែកមិនសមស្រប។ ម្យ៉ាងទៀត ដើម្បីឱ្យគោលបំណងនៃការត្រួតពិនិត្យសម្រេចបានប្រកបដោយប្រសិទ្ធភាព សកម្មភាព អនុលោមតាមគោលបំណងត្រូវតែអាចវាស់វែង និងសង្កេតបាន។

ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងរបស់ បបព ត្រូវរៀបចំឡើង ដើម្បីជួយដល់ថ្នាក់ដឹកនាំសម្រេចបាននូវគោលបំណងដូចខាងក្រោម ÷

ការអនុញ្ញាត : ធានាថាចម្លងការទាំងអស់ត្រូវបានទទួលការឯកភាពពីមន្ត្រីទទួលខុសត្រូវ ស្របតាមសិទ្ធិសម្រេចជាទូទៅឬដោយឡែកមុនពេលដែលចម្លងការត្រូវបានកត់ត្រា។

ភូរណភាព : ធានាថារាល់ចម្លងការមានសុពលភាពទាំងអស់ត្រូវបានកត់ត្រាក្នុងប្រព័ន្ធគណនេយ្យ។

សុក្រឹតភាព : ធានាថារាល់ចម្ងាយការគឺត្រឹមត្រូវ មានសង្គតិភាពជាមួយព័ត៌មាននិងទិន្នន័យប្រតិបត្តិការដើម ហើយត្រូវបានកត់ត្រាទាន់ពេលវេលា។

សុពលភាព : ធានាថាចម្ងាយការទាំងអស់ដែលបានកត់ត្រា បានឆ្លុះបញ្ចាំងអំពីព្រឹត្តិការណ៍សេដ្ឋកិច្ចពិត ដែលកើតឡើង មានការអនុញ្ញាតរបស់ថ្នាក់ដឹកនាំ និងស្របតាមបទប្បញ្ញត្តិជាធរមាន។

សុវត្ថិភាព និងសន្តិសុខរូបវន្ត : ធានាថាការប្រើប្រាស់ទ្រព្យសកម្មរូបវន្តនិងប្រព័ន្ធព័ត៌មានត្រូវបានត្រួតពិនិត្យ និងសម្រាប់តែមន្ត្រីដែលមានការអនុញ្ញាតប៉ុណ្ណោះ។

ការដោះស្រាយកំហុស : ធានាថាកំហុស ដែលបានរកឃើញនៅដំណាក់កាលនីមួយៗនៃប្រតិបត្តិការត្រូវទទួលបានការកែតម្រូវ និងរាយការណ៍ជូនថ្នាក់ដឹកនាំពាក់ព័ន្ធបានទាន់ពេលវេលា។

វិសមិតភាពមុខងារ : មន្ត្រីគ្រប់រូបមិនអនុញ្ញាតឱ្យមានមុខងារពីរក្នុងពេលតែមួយ គឺមុខងារកត់ត្រា និងគ្រប់គ្រងលើនីតិវិធីដំណើរការចម្ងាយការ។

ដំណើរការដែលតាក់តែងបានល្អ ប្រកបដោយប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងសមស្រប គួរបញ្ចូលនូវគោលបំណងខាងលើឱ្យបានច្រើនប្រសិនជាមិនអាចបានទាំងអស់។

៤. ការទទួលខុសត្រូវលើការត្រួតពិនិត្យផ្ទៃក្នុង

ថ្នាក់ដឹកនាំក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈ ត្រូវទទួលខុសត្រូវលើការតាក់តែង និងការដាក់ឱ្យអនុវត្តប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងទាំងអស់ រួមទាំងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងសម្រាប់ បបព ដើម្បីធានាថា ÷

- បបព ដែលបានអនុវត្តកន្លងមក និងបានស្នើឡើងត្រូវមានរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងគ្រប់គ្រាន់
- ការអភិវឌ្ឍន៍ និងការដាក់អនុវត្តហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និងកម្មវិធីស្រេចនៅគ្រប់ដំណាក់កាលត្រូវមានប្រព័ន្ធត្រួតពិនិត្យគ្រប់គ្រាន់
- ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងកាន់តែពឹងផ្អែកលើស្វ័យប្រវត្តកម្មច្រើនជាងដោយដៃ
- ស្តង់ដារអប្បបរមានៃការត្រួតពិនិត្យផ្ទៃក្នុងត្រូវបានអនុវត្ត (លម្អិតចំណុច ៦.៧)
- ប្រព័ន្ធត្រួតពិនិត្យគន្លឹះត្រូវបានដាក់អនុវត្តជាប្រចាំ ដោយមានភស្តុតាងបញ្ជាក់អត្ថិភាពនៃប្រតិបត្តិការទាំងនោះ
- ប្រព័ន្ធត្រួតពិនិត្យការពារ ត្រូវបានអនុវត្តយ៉ាងយកចិត្តទុកដាក់ ដោយមានការគាំទ្រពីប្រព័ន្ធត្រួតពិនិត្យស្វែងរក និងប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវសមស្រប
- នៅពេលប្រព័ន្ធត្រួតពិនិត្យដោយស្វ័យប្រវត្តពុំទាន់ជឿជាក់បាន ប្រព័ន្ធត្រួតពិនិត្យដោយដៃត្រូវដាក់បន្ថែម

- រចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចុប្បន្នត្រូវផ្លាស់ប្តូរជាបណ្តើរៗ ទៅជាប្រព័ន្ធត្រួតពិនិត្យចម្រុះសមស្របរវាងប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ និងដោយដៃ
- បច្ចេកទេសសវនកម្មបច្ចេកវិទ្យាព័ត៌មានត្រូវបានបញ្ចូលទៅក្នុងស្ថាប័នរបស់ខ្លួន
- ប្រសិទ្ធភាពសវនកម្មផ្ទៃក្នុងត្រូវបានបង្កើនឱ្យខិតទៅរកគម្រិតស្តង់ដារ
- សវនករផ្ទៃក្នុងតាមស្ថាប័ន ត្រូវបានបណ្តុះបណ្តាលលើការរៀបចំផែនការ ការវាយតម្លៃ និងការធ្វើរបាយការណ៍អំពីការត្រួតពិនិត្យផ្ទៃក្នុងនៅក្នុងបរិស្ថាន បបព។

សវនកម្មផ្ទៃក្នុងមានតួនាទីពិនិត្យតាមដានការត្រួតពិនិត្យផ្ទៃក្នុង ដែលរៀបចំដោយថ្នាក់ដឹកនាំក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈ ហើយផ្តល់ការអះអាងដើម្បីជួយដល់ថ្នាក់ដឹកនាំក្នុងការអនុវត្ត និងការរក្សាបាននូវភាពគ្រប់គ្រាន់ និងត្រឹមត្រូវនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង បបព។

៥. បច្ចុប្បន្នភាពឯកសារការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

អគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុង (អសក) នៃក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ (កសហវ) ត្រូវពិនិត្យឡើងវិញ ជារៀងរាល់ឆ្នាំនូវឯកសារស្តីពី “ការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន” នេះ និងធ្វើការកែតម្រូវតាមការចាំបាច់។

ផ្នែក ខ: គោលការណ៍ និងស្តង់ដារប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

ខាងក្រោមនេះ គឺជាគោលការណ៍ និងស្តង់ដារដែលថ្នាក់ដឹកនាំក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈត្រូវអនុវត្តដើម្បីបង្កើត ពង្រឹង និងអភិវឌ្ឍន៍នូវរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងគ្រប់គ្រាន់មួយសម្រាប់ បបព។

១. ការទទួលខុសត្រូវលើការត្រួតពិនិត្យផ្ទៃក្នុង

ថ្នាក់ដឹកនាំក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈ ជាអ្នកទទួលខុសត្រូវលើការតាក់តែង ការដាក់អនុវត្ត និងការថែរក្សារចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។ ថ្នាក់ដឹកនាំ រួមទាំងមន្ត្រីទាំងអស់ត្រូវទទួលខុសត្រូវក្នុងការអនុវត្តការត្រួតពិនិត្យផ្ទៃក្នុងស្របតាមបទប្បញ្ញត្តិពាក់ព័ន្ធ។ សវនកម្មផ្ទៃក្នុង ត្រូវផ្តល់នូវការអះអាងជូនថ្នាក់ដឹកនាំអំពីគុណភាពនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង និងប្រសិទ្ធភាពនៃការអនុវត្តប្រព័ន្ធនេះ។

២. តួនាទី និងភារកិច្ចរបស់សវនកម្មផ្ទៃក្នុង ក្នុងការអនុវត្តប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

សវនកម្មផ្ទៃក្នុង ត្រូវផ្តល់ការអះអាងលើប្រសិទ្ធភាព និងសក្តិសិទ្ធភាពដំណើរការអភិវឌ្ឍន៍ និងប្រតិបត្តិការនៃដំណើរការគន្លឹះរបស់ បបព និងមានតួនាទី និងភារកិច្ចសំខាន់ៗដូចខាងក្រោម÷

- ត្រួតពិនិត្យលើការទទួលខុសត្រូវ សិទ្ធិ សេរីភាព និងករណីលើកលែងដែលបានស្នើឡើង
- ត្រួតពិនិត្យអំពីបច្ច័យរបស់ប្រព័ន្ធត្រួតពិនិត្យនៃការអនុវត្តអង្គភាពថវិកា ជាមួយការបែងចែកការទទួលខុសត្រូវ
- ត្រួតពិនិត្យម៉ាទ្រីសក្របខ័ណ្ឌហានិភ័យសម្រាប់ដំណើរការធុរកិច្ចទាំងមូល
- ត្រួតពិនិត្យលើផ្នែកពាក់ព័ន្ធក្នុងអង្គភាពដែលបានដាក់ឱ្យប្រើប្រាស់ បបព ដើម្បីជួយដល់ថ្នាក់ដឹកនាំពង្រឹងបរិស្ថានគ្រប់គ្រង
- ត្រួតពិនិត្យប្រព័ន្ធគ្រប់គ្រងលើហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន
- វាយតម្លៃហានិភ័យមុនដាក់ដំណើរការ និងភាពរួចរាល់នៃប្រព័ន្ធត្រួតពិនិត្យដែលបានត្រៀមនៅតាមទីតាំងប្រើប្រាស់ បបព សំខាន់ៗ
- ត្រួតពិនិត្យការតាក់តែង និងប្រសិទ្ធភាពប្រតិបត្តិការនៃប្រព័ន្ធត្រួតពិនិត្យរួម ក្នុងបរិស្ថានដែលនឹងត្រូវប្រើប្រាស់ បបព
- ត្រួតពិនិត្យភាពគ្រប់គ្រាន់នៃប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវ និងប្រព័ន្ធត្រួតពិនិត្យបង្កប់នៅក្នុង បបព
- ត្រួតពិនិត្យប្រតិបត្តិការជាក់ស្តែងនៃប្រព័ន្ធត្រួតពិនិត្យដែលមាននៅតាមទីតាំងដែលត្រូវប្រើប្រាស់ បបព
- ត្រួតពិនិត្យភាពអាចដំណើរការបាននៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងតាមប្រព័ន្ធព័ត៌មានវិទ្យា

- ផ្តល់អនុសាសន៍កែលម្អលើបញ្ហាប្រឈម ពាក់ព័ន្ធការបង្កើត ការអនុវត្ត និងការអភិវឌ្ឍ បបព។

លើសពីនេះទៀត អសក នៃ កសហវ ទទួលខុសត្រូវលើការធានាសង្គតិភាពនៃស្តង់ដារ និងការពង្រឹងវិជ្ជាជីវៈសវនកម្មផ្ទៃក្នុងជូនក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈ ព្រមទាំងផ្តល់ជូនថ្នាក់ដឹកនាំនូវការធានា÷

- ពង្រឹងសវនកម្មបច្ចេកវិទ្យាព័ត៌មានតាមក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈ
- ត្រួតពិនិត្យការរៀបចំផែនការសកម្មភាពដើម្បីផ្លាស់ប្តូរជាបណ្តើរៗ ចេញពីការគ្រប់គ្រងបែបមជ្ឈការរបស់កសហវ
- ត្រួតពិនិត្យរាល់ការបញ្ចូលការប្រមូលចំណូល និងចំណាយទៅក្នុងប្រព័ន្ធទូទាត់ទូទៅ
- ត្រួតពិនិត្យលើការរៀបចំគោលការណ៍ត្រួតពិនិត្យអប្បបរមា
- ផ្តល់ប្រឹក្សាលើអភិក្រមពាក់ព័ន្ធនឹងគណនីនៃប្តង់គណនេយ្យសាធារណៈ។

សវនករផ្ទៃក្នុងអាចចុះពិនិត្យផ្តល់ការធានាអះអាងលើ បបព នៅមុន និងក្រោយពេលដាក់ឱ្យអនុវត្តដោយមានកិច្ចសហការពីសវនដ្ឋាន។

៣. លក្ខណៈនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងល្អ

ជាទូទៅប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដែលល្អ គួររួមបញ្ចូលនូវលក្ខណៈដូចខាងក្រោម÷

- ការបែងចែកភារកិច្ចបានសមស្រប
- ការត្រួតពិនិត្យលើការគ្រប់គ្រង
- ជំហានដំណើរការមានលំដាប់លំដោយត្រឹមត្រូវ
- ការងារបាននិងកំពុងធ្វើ នៅតាមទីកន្លែង និងពេលវេលាដែលត្រឹមត្រូវតាមលំដាប់លំដោយ និងជំនាញ
- ចំណុចរួមនៃការទទួលខុសត្រូវរបស់ថ្នាក់គ្រប់គ្រងត្រូវបានកំណត់
- ចំណុចដោះស្រាយ និងពាក់ព័ន្ធមានតិចបំផុត
- លំហូរការងារត្រឡប់ក្រោយមានតិចបំផុត
- សកម្មភាពជាយថាហេតុមានតិចបំផុត។

៤. ស្តង់ដារនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

ក្របខ័ណ្ឌសវនកម្មកំណត់ដោយគណៈកម្មាធិការនៃអង្គការគាំទ្ររបស់ស្នងការទ្រីដវេ (COSO) ត្រូវបានយកមកប្រើប្រាស់ដើម្បីវាយតម្លៃលើភាពគ្រប់គ្រាន់នៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។ COSO ផ្តោតលើផ្នែកចំនួនប្រាំដើម្បីសម្រេចគោលបំណងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង រួមមានបរិស្ថានត្រួតពិនិត្យ ការវាយតម្លៃហានិភ័យ សកម្មភាពត្រួតពិនិត្យព័ត៌មាននិងគមនាគមន៍ និងការតាមដាន។

ក្របខ័ណ្ឌ COSO មិនអាចប្រើប្រាស់សម្រាប់ធ្វើសវនកម្មប្រព័ន្ធព័ត៌មានបានពេញលេញទេ គឺត្រូវប្រើប្រាស់ក្របខ័ណ្ឌ "គោលបំណងប្រព័ន្ធត្រួតពិនិត្យព័ត៌មាន និងបច្ចេកវិទ្យាពាក់ព័ន្ធ" (Control Objectives for Information and Related Technology-COBIT) នៃវិទ្យាស្ថានអភិបាលកិច្ចប្រព័ន្ធព័ត៌មាន (Information System Governance Institute)។ នៅក្នុងការអនុវត្ត COBIT សម្រាប់ធ្វើសវនកម្មប្រព័ន្ធព័ត៌មាន ពិសេសការវាយតម្លៃលើភាពគ្រប់គ្រាន់នៃការត្រួតពិនិត្យផ្ទៃក្នុងនៃ បបព ត្រូវគោរពគោលបំណងរបស់ COSO ខាងលើ។

៥. ការវាយតម្លៃហានិភ័យប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

គោលការណ៍ត្រួតពិនិត្យ: ការវាយតម្លៃហានិភ័យត្រូវអនុវត្តជាប្រចាំ ហើយប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងត្រូវតាក់តែង ដើម្បីកាត់បន្ថយហានិភ័យដែលបានកត់សម្គាល់ឃើញ។

"ហានិភ័យ" គឺជាស្ថានភាពដែលព្រឹត្តិការណ៍ ឬសកម្មភាព (រួមទាំងដំណើរគ្មានសកម្មភាព) បណ្តាលឱ្យប៉ះពាល់ទៅលើការសម្រេចគោលដៅធុរកិច្ច ឬកំហុសឆ្គងនៅក្នុងរបាយការណ៍ហិរញ្ញវត្ថុ។ កម្រិតហានិភ័យអាចវាស់វែងដោយលទ្ធភាព និងផលប៉ះពាល់នៃព្រឹត្តិការណ៍ដែលអាចកើតឡើង។ ហានិភ័យអាចកើតឡើងនៅក្នុងដំណើរការធុរកិច្ច និងដំណើរការផ្សេងទៀត ដែលពាក់ព័ន្ធនឹងការអភិវឌ្ឍន៍ និងប្រតិបត្តិការប្រចាំថ្ងៃនៃ បបព។

ហានិភ័យដែលទាក់ទងនឹងដំណើរការ បបព ត្រូវបានកំណត់ បន្ទាប់មកប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងត្រូវតាក់តែងឡើង ហើយចំណុចចាប់ផ្តើមសំខាន់គឺវាយតម្លៃរចនាសម្ព័ន្ធត្រួតពិនិត្យដែលមានស្រាប់ ដើម្បីកែតម្រូវក្នុងករណីមិនឆ្លើយតបក្នុងបរិស្ថានស្វ័យប្រវត្តិ។

៦. គោលការណ៍ត្រួតពិនិត្យប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

៦.១. ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និងការត្រួតពិនិត្យផ្ទៃក្នុង

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងត្រូវមានរចនាសម្ព័ន្ធដែលមានលក្ខណៈគ្រប់គ្រាន់ និងត្រូវដាក់ឱ្យអនុវត្តក្នុងអំឡុងពេលនៃខួបក្នុងការកសាង បបព។

បបព នឹងក្លាយជាផ្នែកមួយយ៉ាងសំខាន់នៅក្នុងរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងរបស់រាជរដ្ឋាភិបាល នៅពេលដែលបានដាក់ឱ្យប្រើប្រាស់ពេញលេញ។ ដូច្នេះ រចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងត្រូវរៀបចំឱ្យបានរឹងមាំ នៅតាមទីតាំងសាកល្បងជាមុន មុននឹងដាក់ឱ្យដំណើរការ បបព និងការពង្រីកបន្ថែមជាបន្តបន្ទាប់។

៦.២. អត្ថប្រយោជន៍នៃស្វ័យប្រវត្តកម្មប្រព័ន្ធត្រួតពិនិត្យ

គោលការណ៍ត្រួតពិនិត្យ: ជំរុញការផ្លាស់ប្តូរជាបណ្តើរៗពីរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដោយដៃទៅជាប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ។

អត្ថប្រយោជន៍នៃការត្រួតពិនិត្យផ្ទៃក្នុងស្វ័យប្រវត្តមាន÷

- កាត់បន្ថយលទ្ធភាពអាចកើតឡើងនូវកំហុស និងការកេងបន្លំដែលបង្កដោយមនុស្ស
- ចំណាយពេលតិចជាងក្នុងការងារ ឬការគ្រប់គ្រងដែលបំពេញដោយដៃ
- បង្កើនវិសាលភាពនិងគុណភាពការអនុវត្តសាកល្បងសវនកម្មតាមរយៈការទាញយកនិងការបម្លែងកំណត់ត្រា និងទិន្នន័យអេឡិចត្រូនិច
- បង្កើនប្រសិទ្ធភាពសវនកម្មតាមរយៈការជំនួសការអនុវត្តសាកល្បងដោយដៃ ដែលយឺតយ៉ាវនិងងាយកើតមានកំហុសដោយកម្មវិធីស្រេច។

ដើម្បីទទួលបានអត្ថប្រយោជន៍ពេញលេញពី បបព សវនកម្មផ្ទៃក្នុងត្រូវការសិទ្ធិចូលដល់ដំណើរការជាក់ស្តែង (គ្មានសិទ្ធកែប្រែ) និងមានលទ្ធភាពទាញយកទិន្នន័យពីប្រព័ន្ធ និងកម្មវិធីជាក់លាក់សម្រាប់បម្លែងទិន្នន័យទាំងនេះ។

៦.៣. គោលការណ៍ទូទៅសម្រាប់តាក់តែងប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន

គោលការណ៍ត្រួតពិនិត្យ: គោលការណ៍មួយចំនួនត្រូវចងចាំក្នុងពេលតាក់តែងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។

ការតាក់តែងប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន ត្រូវគោរពគោលការណ៍ទូទៅមួយចំនួនដូចជា÷

- ការបង្កើតប្រព័ន្ធត្រួតពិនិត្យនៅក្នុងកម្មវិធីស្រេច មានប្រសិទ្ធភាពជាងការរង់ចាំសង្កេត និងធ្វើសវនកម្មក្រោយពេលអនុវត្ត
- ប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវក្នុងកម្មវិធីស្រេចអាចជឿទុកចិត្តជាងប្រព័ន្ធត្រួតពិនិត្យដោយដៃ
- កម្រិតរឹងមាំនៃការត្រួតពិនិត្យផ្ទៃក្នុងទូទៅ អាចបង្កើនតាមរយៈការជំនួសប្រព័ន្ធដោយដៃជាមួយប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវជាបណ្តើរៗ។

ក្នុងដំណាក់កាលតាក់តែងកម្មវិធីស្រេច សវនករត្រូវវាយតម្លៃលើប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវដែលចាត់ទុកជាមូលដ្ឋានគោល ក្នុងការធានាភាពគ្រប់គ្រាន់នៃប្រព័ន្ធត្រួតពិនិត្យនៅមុនដំណាក់កាលដាក់ឱ្យអនុវត្ត បបព។ ដោយឡែក នៅដំណាក់កាលក្រោយការដាក់ឱ្យអនុវត្តគួរវាយតម្លៃលើប្រព័ន្ធត្រួតពិនិត្យជាក់ស្តែង ដើម្បីផ្តល់ការធានាថាប្រព័ន្ធត្រួតពិនិត្យត្រូវបានប្រើប្រាស់ប្រកបដោយប្រសិទ្ធភាព។

ការអនុវត្តសាកល្បងលើប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវមិនចាំបាច់ធ្វើជាប្រចាំឆ្នាំនោះទេ ប្រសិនបើការគ្រប់គ្រងការផ្លាស់ប្តូរ និងប្រព័ន្ធត្រួតពិនិត្យគ្រប់គ្រងសុវត្ថិភាពដំណើរការប្រកបដោយប្រសិទ្ធភាព។

៦.៤. ទស្សនទាននៃប្រព័ន្ធត្រួតពិនិត្យ

គោលការណ៍ត្រួតពិនិត្យ: ទស្សនទាននៃប្រព័ន្ធត្រួតពិនិត្យជាលាយលក្ខណ៍អក្សរត្រូវរៀបចំ ដើម្បីជួយក្នុងការតាក់តែងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងឱ្យមានភាពប្រទាក់គ្នា សង្គតិភាព និងប្រសិទ្ធភាព។

ការអនុវត្ត បបព ដោយជោគជ័យត្រូវអនុលោមតាមទស្សនទាននៃប្រព័ន្ធត្រួតពិនិត្យ និងអភិក្រមជាលាយលក្ខណ៍អក្សរច្បាស់លាស់ ជាអាទិ៍÷

- ការកំណត់ហានិភ័យគន្លឹះ
- រចនាសម្ព័ន្ធត្រួតពិនិត្យសមស្របដែលត្រូវអនុវត្ត
- ជម្រើសពាក់ព័ន្ធនឹងគោលការណ៍ទូទៅនៃការតាក់តែងប្រព័ន្ធត្រួតពិនិត្យ ដែលបានបង្ហាញនៅផ្នែកខាងលើ (ពិនិត្យចំណុច ៥.៣)
- ប្រព័ន្ធត្រួតពិនិត្យជាមូលដ្ឋានដែលត្រូវជ្រើសយកមានប្រព័ន្ធត្រួតពិនិត្យការពារ ប្រព័ន្ធត្រួតពិនិត្យ ស្វែងរក និងប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវ
- កំណត់ "ស្តង់ដារប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា" ដែលត្រូវដាក់អនុវត្ត
- តុល្យភាពសមស្របរវាងប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្ត និងដោយដៃ
- ចាត់ចែងការគ្រប់គ្រងការផ្លាស់ប្តូរសម្រាប់រចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។

៦.៥. ប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្ត និងដោយដៃ

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្ត និងដោយដៃគួរត្រូវដាក់អនុវត្តរួមគ្នាជាមួយតុល្យភាពសមស្រប។

ប្រព័ន្ធត្រួតពិនិត្យនិងរចនាសម្ព័ន្ធនៃកម្មវិធីស្រេច ជាបន្សំរវាងប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្ត និងដោយដៃ។

តម្រូវការជាគន្លឹះ ដើម្បីទទួលបានស្តង់ដារប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា គឺត្រូវធានាថារចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យទាំងមូលបានបញ្ចូលប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្ត និងបំពេញបន្ថែមនូវប្រព័ន្ធត្រួតពិនិត្យដោយដៃ ប្រកបដោយតុល្យភាពសមស្រប។ ប្រការនេះមានសារៈសំខាន់ក្នុងអំឡុងពេលនៃការផ្លាស់ប្តូរប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។

៦.៦. ប្រភេទប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យការពារដោយស្វ័យប្រវត្តគួរអនុវត្តនៅតាមទីកន្លែងដែលអាចធ្វើបាន។

ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានអាចចែកជាបីប្រភេទទៅតាមគោលបំណងត្រួតពិនិត្យ ÷

- ការពារ
- ស្វែងរក
- កែតម្រូវ

ទន្ទឹមនេះ ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានក៏អាចចែកជាបីប្រភេទតាមមធ្យោបាយដាក់ឱ្យប្រើប្រាស់÷

- រដ្ឋបាល
- រូបវន្ត
- បច្ចេកទេស/ប្រព័ន្ធ

ប្រព័ន្ធត្រួតពិនិត្យការពារស្ងួយប្រវត្តិជារឿយៗ ត្រូវបានចាត់ទុកថាជាប្រព័ន្ធត្រួតពិនិត្យរឹងមាំបំផុត ព្រោះក្រោយពេលបង្កើត ប្រសិទ្ធភាពប្រតិបត្តិការនៃប្រព័ន្ធនេះមិនអាស្រ័យលើអន្តរាគមន៍របស់មនុស្សទៀតទេ និងមានសកម្មភាពមុនពេលកំហុសកើតឡើង។ ផ្ទុយមកវិញប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវដោយដៃមានលក្ខណៈទន់ខ្សោយ។

៦.៧. ស្តង់ដារប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា

គោលការណ៍ត្រួតពិនិត្យ: ស្តង់ដារប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងអប្បបរមា ត្រូវប្រកាន់ខ្ជាប់ឱ្យបានគ្រប់ពេលវេលា។

ប្រព័ន្ធត្រួតពិនិត្យដែលរឹងមាំបំផុត ត្រូវមានសមាសធាតុប្រាំបួន រួមមាន: ប្រព័ន្ធត្រួតពិនិត្យការពារ ប្រព័ន្ធត្រួតពិនិត្យស្វែងរក និងប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវ ដែលប្រព័ន្ធត្រួតពិនិត្យនីមួយៗ ត្រូវបានដាក់ឱ្យប្រើប្រាស់តាមវិធីសាស្ត្រ រដ្ឋបាល រូបវន្ត និងបច្ចេកទេស/ប្រព័ន្ធ។ ប្រសិទ្ធភាពអប្បរមានៃប្រព័ន្ធត្រួតពិនិត្យទាមទារឱ្យអនុដំណើរការនីមួយៗ ត្រូវមានប្រព័ន្ធត្រួតពិនិត្យនីមួយៗនៃប្រព័ន្ធត្រួតពិនិត្យទាំងបី។ គោលការណ៍ណែនាំណាដែលមិនមានយន្តការការពារ ស្វែងរក ឬកែតម្រូវ មិនគួរដាក់ឱ្យប្រតិបត្តិការទេ។ ប្រព័ន្ធត្រួតពិនិត្យមិនគ្រប់គ្រាន់អាចកត់សម្គាល់ឃើញតាមរយៈការតាក់តែង (Design) ឬការអនុវត្តជាក់ស្តែងរបស់ប្រព័ន្ធដែលមិនមានប្រសិទ្ធភាព។

ជាទូទៅ÷

ប្រព័ន្ធត្រួតពិនិត្យខ្លាំង = ពហុប្រព័ន្ធត្រួតពិនិត្យការពារ + ពហុប្រព័ន្ធត្រួតពិនិត្យស្វែងរក + ពហុប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវ

ប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា = ប្រព័ន្ធត្រួតពិនិត្យការពារមួយ + ប្រព័ន្ធត្រួតពិនិត្យស្វែងរកមួយ + ប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវមួយ + ប្រសិទ្ធភាពប្រតិបត្តិការនៃប្រព័ន្ធត្រួតពិនិត្យទាំងអស់

ប្រព័ន្ធត្រួតពិនិត្យខ្សោយ = តិចជាងកម្រិតប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា + ប្រតិបត្តិការប្រព័ន្ធត្រួតពិនិត្យមានចំណុចសង្ស័យ ឬអសង្គតិភាព។

៧. រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន

គោលការណ៍ត្រួតពិនិត្យ: រចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដែលមានលក្ខណៈគ្រប់ជ្រុងជ្រោយ ត្រូវដាក់ឱ្យអនុវត្តលើ បបព ។

ជាទូទៅរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងពេញលេញសម្រាប់ បបព ត្រូវមានលក្ខណៈដូចខាងក្រោម÷

ក. ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅ

ក.១. ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានរួម : គឺជាប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅដែលត្រូវបានរៀបចំឡើងដើម្បីគ្រប់គ្រង និងពិនិត្យតាមដានលើបរិស្ថានបច្ចេកវិទ្យាព័ត៌មាន ហើយមានឥទ្ធិពលលើកម្មវិធីស្រេចទាំងអស់។ ប្រព័ន្ធត្រួតពិនិត្យនេះផ្តោតសំខាន់លើការគ្រប់គ្រង និងការតាមដានលើ បបព។

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានរួមដែលគ្រប់គ្រាន់ ត្រូវដាក់ឱ្យអនុវត្តដើម្បីគាំទ្រដល់ហេដ្ឋារចនាសម្ព័ន្ធ និងប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេចនៃ បបព។

ប្រសិទ្ធភាពនៃការត្រួតពិនិត្យផ្ទៃក្នុងដោយស្វ័យប្រវត្តិ អាស្រ័យមួយផ្នែកលើស្តង់ដារនៃការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យនៅក្នុងបរិស្ថានដែលកំពុងអនុវត្តនោះ។

បរិស្ថានត្រួតពិនិត្យទូទៅនៅក្នុងអង្គភាព បានបង្កើតមូលដ្ឋានគ្រឹះសម្រាប់ការត្រួតពិនិត្យផ្ទៃក្នុងប្រកបដោយប្រសិទ្ធភាព និងបានបង្កើតនូវ "ភាពម៉ឺងម៉ាត់" និងតំណាងឱ្យចំណុចកំពូលនៃរចនាសម្ព័ន្ធអភិបាលកិច្ចអង្គភាព។

បបព រួមត្រូវគាំទ្រដោយប្រព័ន្ធត្រួតពិនិត្យនៅតាមផ្នែកនានា ដូចខាងក្រោម÷

- ការរៀបចំផែនការយុទ្ធសាស្ត្ររបស់បច្ចេកវិទ្យាព័ត៌មាននិងគមនាគមន៍ និង បបព
- ការកំណត់ការរៀបចំ ទំនាក់ទំនង និងដំណើរការបច្ចេកវិទ្យាព័ត៌មាននិងគមនាគមន៍
- គមនាគមន៍គោលបំណង និងទិសដៅនៃការគ្រប់គ្រងបច្ចេកវិទ្យាព័ត៌មាន
- ការគ្រប់គ្រងធនធានមនុស្សផ្នែកបច្ចេកវិទ្យាព័ត៌មាននិងគមនាគមន៍
- ការគ្រប់គ្រងគុណភាពបច្ចេកវិទ្យាព័ត៌មាន
- ការវាយតម្លៃ និងគ្រប់គ្រងហានិភ័យបច្ចេកវិទ្យាព័ត៌មាននិងគមនាគមន៍
- ការគ្រប់គ្រងគម្រោង
- ការផ្គត់ផ្គង់ និងគាំទ្រ (ប្រតិបត្តិការកុំព្យូទ័រ និងសិទ្ធិចូលដល់កម្មវិធី និងទិន្នន័យ)
- ការកំណត់ និងការគ្រប់គ្រងកម្រិតសេវាកម្ម
- ការផ្គត់ផ្គង់សេវាកម្មបច្ចេកវិទ្យាព័ត៌មាននិងគមនាគមន៍
- ការគ្រប់គ្រងការអនុវត្ត និងសមត្ថភាពបច្ចេកវិទ្យាព័ត៌មាននិងគមនាគមន៍
- ការអប់រំ និងបណ្តុះបណ្តាលអ្នកប្រើប្រាស់បច្ចេកវិទ្យាព័ត៌មាន
- ការតាមដាន និងវាយតម្លៃលើការអនុវត្ត
- អភិបាលកិច្ចបច្ចេកវិទ្យាព័ត៌មាននិងគមនាគមន៍។

ក.២.ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានកម្រិតដំណើរការ : គឺជាប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅ កម្រិតដំណើរការ ដែលមិនរាប់បញ្ចូលប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានរួមខាងលើទេ ព្រោះវាសំដៅដោយឡែក តែលើប្រព័ន្ធត្រួតពិនិត្យ បបព ជាក់លាក់មួយ។

គោលការណ៍ត្រួតពិនិត្យ: កម្មវិធីស្រេចកម្រិតដំណើរការត្រូវគាំទ្រដោយយន្តការត្រួតពិនិត្យផ្ទៃក្នុង ដែលតាក់តែងឡើង ដើម្បីធានាឱ្យមាននីតិវិធីគ្រប់គ្រាន់សម្រាប់អភិវឌ្ឍន៍ប្រព័ន្ធ និងការផ្លាស់ប្តូរប្រព័ន្ធត្រួតពិនិត្យ ក៏ដូចជានីតិវិធីសមស្របសម្រាប់ការផ្តល់សេវា បបព។

បបព កម្រិតដំណើរការត្រូវបានគាំទ្រដោយយន្តការត្រួតពិនិត្យផ្ទៃក្នុងនៅតាមផ្នែកនានា ដូចខាងក្រោម÷

- ការអភិវឌ្ឍន៍ បបព
- ការទទួលយក និងការថែរក្សាផ្នែកទន់នៃកម្មវិធីស្រេច
- ការទទួលយក និងការថែរក្សាហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យា
- ការបង្កើតប្រតិបត្តិការ និងការប្រើប្រាស់
- ការគ្រប់គ្រងការផ្លាស់ប្តូរ
- ការតម្លើង ការបង្កើតដំណោះស្រាយ និងការផ្លាស់ប្តូរ
- ការផ្តល់សេវាកម្មប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន
- ការកំណត់ និងគ្រប់គ្រងកម្រិតសេវាកម្ម
- ការគ្រប់គ្រងសេវាកម្មរបស់ភាគីទីបី
- ការការពារសុវត្ថិភាពលើការផ្តល់សេវាកម្មបច្ចេកវិទ្យាព័ត៌មាន
- ការធានាសុវត្ថិភាពប្រព័ន្ធ
- ការគ្រប់គ្រងការរៀបគម្រោង
- ការគ្រប់គ្រងបញ្ហា
- ការគ្រប់គ្រងសេវាកម្មដោះស្រាយបញ្ហា និងឧបទ្ទវហេតុ
- ការគ្រប់គ្រងទិន្នន័យ
- និរន្តរភាពធុរកិច្ច និងការស្តារឡើងវិញក្រោយពេលខូចខាត។

ខ.ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីលម្អិត:

ខ.១.ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច : ជាប្រព័ន្ធត្រួតពិនិត្យ មាននៅក្នុង បបព ស្រាប់រួមជាមួយប្រព័ន្ធត្រួតពិនិត្យដោយដៃបន្ថែម។

គោលការណ៍ត្រួតពិនិត្យ:កម្មវិធីស្រេចនីមួយៗ ត្រូវគាំទ្រដោយការអនុវត្តយន្តការត្រួតពិនិត្យដែលគ្រប់គ្រាន់។

គោលបំណងចម្បងនៃប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច គឺដើម្បីធានាសុវត្ថិភាព ភាពគ្រប់គ្រាន់ ភាពត្រឹមត្រូវ និង ប្រសិទ្ធភាពនៃការរៀបចំធាតុចូល ដំណើរការ និងធាតុចេញ។

ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេចត្រូវបានកំណត់ដោយកម្មវិធីស្វ័យប្រវត្តិ ឬដោយដៃតាមការចាត់ចែងរបស់អ្នកប្រើប្រាស់ ឬនាយកដ្ឋានព័ត៌មានវិទ្យា។

ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេចត្រូវអនុវត្តនៅតាមផ្នែកដូចខាងក្រោម÷

- សុវត្ថិភាពកម្មវិធីស្រេច
- ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេចទាក់ទងនិងការបែងចែកមុខងារប្រើប្រាស់
- ប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវ
- កម្មវិធីប្រព័ន្ធត្រួតពិនិត្យផ្សេងៗ
- ប្រព័ន្ធត្រួតពិនិត្យផ្នែកប្រតិបត្តិការ
- ប្រព័ន្ធត្រួតពិនិត្យលើដំណើរការធុរកិច្ចជាក់លាក់
- ប្រព័ន្ធត្រួតពិនិត្យដោយដៃដែលអាចប្តូរជាស្វ័យប្រវត្តបាន។

ផ្នែកទាំងអស់ខាងលើគឺជាកម្មវត្ថុនៃសវនកម្ម ដើម្បីធានាចំពោះថ្នាក់ដឹកនាំថាប្រព័ន្ធត្រួតពិនិត្យបានតាក់តែងល្អ អនុវត្តប្រកបដោយប្រសិទ្ធភាព អាចផ្តល់នូវសក្តានុពលសម្រាប់ធ្វើឱ្យប្រសើរឡើងនូវកម្រិតប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដែលមានស្រាប់ ព្រមទាំងទទួលបានអត្ថប្រយោជន៍ពេញលេញពី បបព។

ខ.១.១ សុវត្ថិភាពកម្មវិធីស្រេច

គោលការណ៍ត្រួតពិនិត្យ: ការរៀបចំសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន ត្រូវផ្តោតលើការរក្សាការសម្ងាត់ បូរណភាព និងលទ្ធភាពនៃការប្រើប្រាស់ទិន្នន័យ។

ហានិភ័យសំខាន់ពាក់ព័ន្ធនឹងសុវត្ថិភាពនៃការផ្តល់សិទ្ធិចូល គឺអាចមានការផ្សាយទិន្នន័យសម្ងាត់ដោយគ្មានការអនុញ្ញាត ឬបូរណភាពទិន្នន័យអាចទទួលរងការបំពាន ឬ បបព មិនអាចប្រើប្រាស់បាននៅពេលដែលត្រូវការ។

ដំណើរការ និងប្រព័ន្ធត្រួតពិនិត្យត្រូវបង្កើតសម្រាប់ត្រួតពិនិត្យលើការផ្តល់សិទ្ធិចូលជូនអ្នកប្រើប្រាស់ និងការលុប ឬការកែប្រែសិទ្ធិចូលនៅពេលដែលអ្នកប្រើប្រាស់បានផ្លាស់ប្តូរ ឬលាលែងពីការងារ។ ម្យ៉ាងទៀត ការចូលប្រើប្រាស់ បបព របស់ភាគីទីបីក៏ត្រូវមានប្រព័ន្ធត្រួតពិនិត្យផងដែរ។

ខ.១.២ ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេចទាក់ទងនិងការបែងចែកមុខងារប្រើប្រាស់

គោលការណ៍ត្រួតពិនិត្យ: មុខងាររបស់អ្នកប្រើប្រាស់នៅក្នុង បបព ត្រូវបានកម្រិតទៅតាមការកំណត់ ដើម្បីរក្សាប្រសិទ្ធភាពនៃការបែងចែកមុខងារ។

នៅក្នុងបរិស្ថានស្វ័យប្រវត្តិ ការបែងចែកមុខងារត្រូវបានធានាដោយការកម្រិតសិទ្ធិរបស់អ្នកប្រើប្រាស់តាមស្ត្រីន ដោយឡែកពីគ្នានៅក្នុងប្រព័ន្ធ។ ដើម្បីភាពងាយស្រួល និងសង្គតិភាព ការចូលដល់ស្ត្រីនជាក់លាក់នីមួយៗ ត្រូវបានភ្ជាប់ទៅក្រុមការងារ ដែលអ្នកប្រើប្រាស់នីមួយៗបានភ្ជាប់ជាមួយសិទ្ធិចូល និងសម្រេចតាមការកំណត់។

តម្រូវការគន្លឹះ គឺ បបព ត្រូវរក្សាការបែងចែកមុខងារសមស្របមួយ ដែលរារាំងអ្នកប្រើប្រាស់មិនឱ្យមានសិទ្ធិត្រួតពិនិត្យទាំងស្រុងលើដំណើរការទាំងអស់នៃចម្ងាយការនីមួយៗ។

ខ.១.៣ ប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវកម្មវិធីស្រេច

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យ "រៀបតម្រូវ" ត្រូវគាំទ្រគោលការណ៍នានា ដែលបានអនុម័តដោយថ្នាក់ដឹកនាំ។

ប្រព័ន្ធត្រួតពិនិត្យ "រៀបតម្រូវ" គឺជាចំណែកនៃប្រព័ន្ធត្រួតពិនិត្យដំណើរការស្វ័យប្រវត្តិ ដែលរៀបចំឡើងពាក់ព័ន្ធនឹងដែនកំណត់និងទំហំគំលាត ការឆែកបូរណភាពទិន្នន័យ ការឆែកលើទម្រង់ទិន្នន័យក្នុងប្រឡង់ និងការអនុម័តលើលំហូរការងារជាដើម។ ប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវជាប្រព័ន្ធត្រួតពិនិត្យដែលរៀបចំតាមជម្រើស។

ជម្រើសនៅក្នុងប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវ ត្រូវតែធ្វើឡើងដោយប្រុងប្រយ័ត្នដើម្បីជៀសវាងការទទួលបានលទ្ធផលមិនសមតាមបំណង។ យន្តការអនុម័តស្វ័យប្រវត្តិ ជាធម្មតាត្រូវកំណត់អ្នកប្រើប្រាស់ដែលមានសិទ្ធិអនុម័តទៅតាមកម្រិតនិងដែនកំណត់។ ដោយឡែក នៅក្នុងបរិស្ថានដោយដៃអ្នកប្រើប្រាស់ដែលជាអ្នកគ្រប់គ្រងមិនត្រូវបានអនុញ្ញាតឱ្យប្រតិបត្តិចម្ងាយការទេ។ ផ្ទុយទៅវិញ ការផ្តល់តួនាទីឱ្យអ្នកគ្រប់គ្រងប្រព័ន្ធ មានសិទ្ធិអនុម័តនៅក្នុងកម្មវិធីស្រេច នឹងផ្តល់លទ្ធភាពឱ្យអ្នកទាំងនោះអាចលុបការសម្រេច និងអនុម័តលើចម្ងាយការដែលហាមឃាត់បាន។

សវនកម្មផ្ទៃក្នុងមានកាតព្វកិច្ចធានាចំពោះថ្នាក់ដឹកនាំ លើជម្រើសដែលបានជ្រើសរើស ឱ្យឆ្លើយតបទៅនឹងគោលនយោបាយបានកំណត់ មុនពេលប្រព័ន្ធត្រួតពិនិត្យ "រៀបតម្រូវ" ត្រូវបានដាក់អនុវត្ត ។

ខ.១.៤. ប្រព័ន្ធត្រួតពិនិត្យបង្កប់កម្មវិធីស្រេច

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យបង្កប់កម្មវិធីស្រេច ត្រូវអនុវត្តដោយវេទយិតភាព ដើម្បីរក្សាកម្រិតនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដែលមានស្រាប់ និងកែលម្អបន្ថែម ប៉ុន្តែជៀសវាងការចំណាយហួសហេតុ។

កម្មវិធីស្រេចបច្ចេកវិទ្យាព័ត៌មានអាចបំពាក់ប្រព័ន្ធត្រួតពិនិត្យបង្កប់មួយចំនួន ដូចជា: ប្រព័ន្ធត្រួតពិនិត្យបង្កប់លើការផ្ទៀងផ្ទាត់ឯកសារ (ការបញ្ជាទិញ វិក័យប័ត្រ របាយការណ៍ទទួលទំនិញ) ការពិនិត្យនិងចុះហត្ថលេខាលើមូលប្បទានប័ត្រ និងការតម្រូវឱ្យទិន្នានុប្បវត្តិមានតុល្យភាពរវាងឥណពន្ធ និងឥណទាន ។

ប្រព័ន្ធត្រួតពិនិត្យបង្កប់មិនដូចប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវទេ គឺអ្នកប្រើប្រាស់ពុំមានជម្រើសក្នុងការសម្រេចឱ្យប្រព័ន្ធត្រួតពិនិត្យបង្កប់នេះត្រូវប្រតិបត្តិតាមគោលបំណងរបស់ខ្លួនឡើយ។ អាស្រ័យហេតុនេះ តម្រូវឱ្យមានការ

ប្រុងប្រយ័ត្នខ្ពស់ ក្នុងការបន្សុីគ្នារវាងប្រព័ន្ធត្រួតពិនិត្យទាំងនេះ នៅក្នុងរចនាសម្ព័ន្ធត្រួតពិនិត្យរួមដែលចង់បាន។ ប្រសិនបើប្រព័ន្ធត្រួតពិនិត្យបង្កប់មិនទាន់បំពេញបានតាមតម្រូវការនៃការត្រួតពិនិត្យផ្ទៃក្នុង ប្រព័ន្ធត្រួតពិនិត្យដោយដៃត្រូវបំពេញបន្ថែម ហើយក្នុងករណីចាំបាច់បំផុត ត្រូវពិចារណាកែតម្រូវកម្មវិធីកុំព្យូទ័រ។

ខ.១.៥. ប្រព័ន្ធត្រួតពិនិត្យប្រតិបត្តិការ

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យប្រតិបត្តិការ ត្រូវធានានូវភាពពេលវេលា សុក្រឹតភាព សុវត្ថិភាព និងប្រសិទ្ធភាពនៃធាតុចូល ដំណើរការ និងធាតុចេញ។

ប្រព័ន្ធត្រួតពិនិត្យប្រតិបត្តិការត្រូវមានក្នុងផ្នែកខាងក្រោម÷

- ធាតុចូល (ការអនុញ្ញាត ការឆែកសំណេរ គោលការណ៍ត្រួតពិនិត្យជាដើម)
- កិច្ចដំណើរការ
- ធាតុចេញ (ស្តង់ដារ របាយការណ៍ចំពោះកិច្ច ជាដើម)
- សន្ធានកម្មជាមួយប្រព័ន្ធកុំព្យូទ័រផ្សេងទៀត
- ការរៀបចំឯកសារ (សៀវភៅណែនាំប្រព័ន្ធ ប្រតិបត្តិការ និងអ្នកប្រើប្រាស់ជាដើម)
- គន្លងសវនកម្ម (Audit Trail) និងភាពអាចធ្វើសវនកម្មបាន
- ការអប់រំ និងការបណ្តុះបណ្តាលអ្នកប្រើប្រាស់
- និរន្តរភាព។

ខ.២.ប្រព័ន្ធត្រួតពិនិត្យដំណើរការធុរកិច្ចដោយឡែក : ជាប្រព័ន្ធត្រួតពិនិត្យដែលទាក់ទងទៅនឹងដំណើរការធុរកិច្ចដោយឡែក ហើយត្រូវបានគ្រប់គ្រងតាមរយៈ បបព។

គោលការណ៍ត្រួតពិនិត្យ: រាល់ដំណើរការធុរកិច្ចទាំងអស់ដែលប្រតិបត្តិដោយ បបព ត្រូវមានប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងគ្រប់គ្រាន់។

ដំណើរការធុរកិច្ច និងតម្រូវការប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងគន្លឹះមានដូចខាងក្រោម÷

ខ.២.១. ខួបសំណើចំណាយដល់ការទូទាត់

ដំណើរការនៃការស្នើសុំចំណាយរហូតដល់ការទូទាត់ រួមបញ្ចូលនូវសកម្មភាពទាក់ទងនឹងការស្នើសុំ ការធានាចំណាយ ការបញ្ជាទិញ ការទទួលទំនិញ ឬសេវាកម្ម និងការទូទាត់លើទំនិញ ឬសេវាកម្មជាមួយអ្នកផ្គត់ផ្គង់។

សកម្មភាពទាំងនេះរួមមាន÷

- ការកត់ត្រាឯកសារមេអំពីទំនិញ និងអ្នកផ្គត់ផ្គង់
- ដំណើរការស្នើសុំ ធានាចំណាយ និងបញ្ជាទិញ
- ដំណើរការទទួលទំនិញ ឬសេវាកម្ម និងផ្សឹងផ្ទាត់

- ការកត់ត្រាវិក័យប័ត្រ និងការផ្គូផ្គង
- ដំណើរការទូទាត់ និងចេញលិខិតប្រកាសឥណទាន
- ការធ្វើបច្ចុប្បន្នភាពសៀវភៅធំ និងសៀវភៅធំរង។

ប្រព័ន្ធត្រួតពិនិត្យដែលត្រូវយកចិត្តទុកដាក់នៅក្នុងផ្នែកនេះមាន÷

ទីត្រួតពិនិត្យគន្លឹះ	ប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវ
ចម្ងាយការទិញ	វិធីសាស្ត្រផ្សៀងផ្គាត់÷ -លិខិតបញ្ជាទិញ និងវិក័យប័ត្រ -លិខិតបញ្ជាទិញ ទំនិញដែលបានទទួល និងវិក័យប័ត្រ -លិខិតបញ្ជាទិញ ទំនិញដែលបានទទួល អធិការកិច្ច និងវិក័យប័ត្រ
ការកត់ត្រាវិក័យប័ត្រ	ការព្រមានអំពីលេខវិក័យប័ត្រស្ងួន
ការផ្គូផ្គងវិក័យប័ត្រ	ចំនួនទឹកប្រាក់ល្អៀងសមស្របដែលអាចអនុញ្ញាតឱ្យទូទាត់
ដំណើរការទូទាត់	ដំណើរការអនុម័តលើការទូទាត់ និងកម្រិតកំណត់

ខ.២.២. ខ្លឹបនៃការផ្គត់ផ្គង់ដល់ការទទួលសាច់ប្រាក់

ខ្លឹបនៃការផ្គត់ផ្គង់រហូតដល់ការទទួលសាច់ប្រាក់ រួមបញ្ចូលនូវសកម្មភាពដែលទាក់ទងទៅនឹងការលក់ ការផ្គត់ផ្គង់ និងការចេញវិក័យប័ត្រនៃការផ្តល់សេវាកម្មរបស់រដ្ឋាភិបាល។ សកម្មភាពទាំងនេះរួមមាន÷

- ការធ្វើបច្ចុប្បន្នភាពសៀវភៅធំ និងសៀវភៅធំរង
- ការកត់ត្រាឯកសារមេអំពីអតិថិជន
- ការសួរតម្លៃ ការប៉ាន់តម្លៃ ការកំណត់តម្លៃ និងការគ្រប់គ្រងកិច្ចសន្យា
- ដំណើរការបញ្ជាលក់ និងការគ្រប់គ្រងឥណទាន
- ដំណើរការផ្គត់ផ្គង់ទំនិញ ឬសេវាកម្ម
- ការប្រគល់ទំនិញត្រលប់មកវិញ
- ដំណើរការចេញវិក័យប័ត្រ និងការបង់ប្រាក់។

ប្រព័ន្ធត្រួតពិនិត្យដែលត្រូវយកចិត្តទុកដាក់នៅក្នុងផ្នែកនេះរួមមាន÷ ការគ្រប់គ្រងលើការធ្វើបច្ចុប្បន្នភាពឯកសារមេអំពីអតិថិជន ការឆែកភាពស្ទួន តម្លៃល្បៀងអនុញ្ញាត ការអនុញ្ញាតកត់ត្រាទំហំល្បៀងក្នុងវិភ័យប័ត្រ ការឆែកវិភ័យប័ត្រស្ទួន អាយុកាលបំណុល កម្រិតកំណត់ឥណទាន ដំណើរការបញ្ជូលទិន្នន័យទៅក្នុងទិន្នានុប្បវត្តិ ការផ្សឹងផ្ទាត់ចម្ងការ ការទទួលស្គាល់ចំណូល និងការបែងចែកតាមគណនី។

ខ.៣.ប្រព័ន្ធត្រួតពិនិត្យដោយដៃសម្រាប់គោលដៅស្វ័យប្រវត្តកម្ម ៖ជាប្រព័ន្ធត្រួតពិនិត្យដោយដៃដែលអាចជាជម្រើសសម្រាប់បង្កើតប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្ត។

គោលការណ៍ត្រួតពិនិត្យ: ដំណើរការស្វ័យប្រវត្តកម្មនៃប្រព័ន្ធត្រួតពិនិត្យដោយដៃត្រូវបញ្ចូលក្នុងផែនការ និងគ្រប់គ្រងច្បាស់លាស់ ដើម្បីកាត់បន្ថយការចំណាយនិងពេលវេលាការងាររបស់មន្ត្រី ព្រមទាំងបង្កើនប្រសិទ្ធភាពប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង ។

ការជំរុញរចនាសម្ព័ន្ធ និងការអនុវត្តសាកល្បងពាក់ព័ន្ធនៃប្រព័ន្ធត្រួតពិនិត្យ ឆ្ពោះទៅរកការផ្តល់ភាពជឿជាក់លើប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្ត គឺជាដំណើរការសន្សឹមៗ និងទាមទារពេលវេលា។

ស្វ័យប្រវត្តកម្មប្រព័ន្ធត្រួតពិនិត្យត្រូវរៀបចំក្នុងករណី÷

- បបព មានជម្រើសបន្ថែមសម្រាប់ស្វ័យប្រវត្តកម្មប្រព័ន្ធត្រួតពិនិត្យ
- ប្រព័ន្ធត្រួតពិនិត្យកំពុងដំណើរការនៅផ្នែកមានហានិភ័យ ដែលប៉ះពាល់ខ្លាំងលើប្រតិបត្តិការ និងឬរបាយការណ៍ហិរញ្ញវត្ថុ
- ប្រព័ន្ធត្រួតពិនិត្យបច្ចុប្បន្នដែលទាមទារចំណាយខ្ពស់ និងឬពេលវេលាច្រើនសម្រាប់ប្រតិបត្តិការ
- ដំណើរការអនុវត្តបច្ចុប្បន្នងាយនឹងមានកំហុស និងឬខ្វះចន្លោះ
- នីតិវិធីបច្ចុប្បន្នមានលក្ខណៈដដែលៗ និងត្រូវការការវិនិច្ឆ័យតិចតួចពីអ្នកពាក់ព័ន្ធ។

នៅពេលប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តពុំទាន់បានធ្វើការអនុវត្តសាកល្បងពេញលេញ និងពិនិត្យដោយសវនកម្មផ្ទៃក្នុង ប្រព័ន្ធត្រួតពិនិត្យដោយដៃនៅអនុញ្ញាតឱ្យបន្តអនុវត្ត។

៨. ការតាមដានលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង បបព គឺជាកម្មវត្ថុនៃការពិនិត្យតាមដានបន្ត។

ការតាមដាន គឺជាដំណើរការនៃការវាយតម្លៃដោយមន្ត្រីទទួលបន្ទុកលើការគាក់តែង និងប្រតិបត្តិការនៃប្រព័ន្ធត្រួតពិនិត្យក្នុងពេលវេលាសមស្រប និងចាត់វិធានការតាមការចាំបាច់។ ការតាមដាននេះត្រូវធ្វើលើគ្រប់សកម្មភាពនៅក្នុងអង្គភាព និងពេលខ្លះជាមួយភាគីកិច្ចសន្យាខាងក្រៅផងដែរ។

ការតាមដានអាចអនុវត្តបានតាមពីររបៀប÷

- សកម្មភាពជាប្រចាំ: សំដៅដល់សកម្មភាពតាមដានប្រសិទ្ធភាពនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងនៃប្រតិបត្តិការជាធម្មតា ដែលរួមមានការត្រួតពិនិត្យ និងគ្រប់គ្រងទៀងទាត់ដោយថ្នាក់ដឹកនាំ ការប្រៀបធៀប ការផ្សំផ្គង និង សកម្មភាពជាប្រចាំផ្សេងទៀត
- ការវាយតម្លៃដោយឡែក: សំដៅដល់ការវាយតម្លៃលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដោយថ្នាក់ដឹកនាំ និងឬដោយ សវនកម្មផ្ទៃក្នុង។ ចំពោះប្រព័ន្ធត្រួតពិនិត្យទាក់ទងនឹងហានិភ័យកម្រិតខ្ពស់និងសំខាន់ ត្រូវវាយតម្លៃឱ្យបានញឹកញាប់។

រាល់សកម្មភាពតាមដានលើប្រសិទ្ធភាពប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងនៃប្រតិបត្តិការប្រចាំថ្ងៃ ត្រូវបញ្ចូលជារចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង បបព។

សន្ទានុក្រម

ការគ្រប់គ្រងការផ្លាស់ប្តូរ: Change Management	ដំណើរការនៃការរៀបចំផែនការ សហប្រតិបត្តិការ ការត្រួតពិនិត្យ និងគមនាគមន៍លើការផ្លាស់ប្តូរ
ការគ្រប់គ្រងហានិភ័យ: Risk Management	ការអនុវត្តជាប្រព័ន្ធនូវគោលការណ៍គ្រប់គ្រង នីតិវិធី និងការអនុវត្តផ្សេងៗ ទៅលើការវិភាគ វាយតម្លៃ និងគ្រប់គ្រងហានិភ័យ
ការច្នៃតម្រូវ : Customization	ការបង្កើតដោយច្នៃតម្រូវលើប្រព័ន្ធស្តង់ប្រវត្តកម្មវិធីកុំព្យូទ័រ
ការពិនិត្យឡើងវិញ: Review	សកម្មភាពអនុវត្តដើម្បីកំណត់នូវភាពសមស្រប ភាពគ្រប់គ្រាន់ និងប្រសិទ្ធិភាពនៃប្រធានបទ ដើម្បីសម្រេចបានតាមគោលបំណងរំពឹងទុក
ការត្រួតពិនិត្យលើការផ្លាស់ប្តូរ: Change Control	ដំណើរការ សិទ្ធិអំណាច និងនីតិវិធីដែលត្រូវប្រើសម្រាប់ការផ្លាស់ប្តូរទៅលើប្រព័ន្ធកុំព្យូទ័រឬទិន្នន័យ
ការសម្ងាត់: Confidentiality	ការពារពីការចូលដោយគ្មានការអនុញ្ញាត
ការរៀបតម្រូវ: Configuration	ការកំណត់នូវចំនួន លក្ខណៈ និងអន្តរទំនាក់ទំនងនៃប្រព័ន្ធកុំព្យូទ័រ
ការវិភាគហានិភ័យ: Risk Analysis	ការប្រើប្រាស់លក្ខណៈជាប្រព័ន្ធលើព័ត៌មានដែលមានដើម្បីកំណត់គ្រោះថ្នាក់ និងប៉ាន់ស្មានហានិភ័យ
ការវាយតម្លៃហានិភ័យ: Risk Assessment	ការវាយតម្លៃពេញលេញលើហានិភ័យ រួមទាំងផលប៉ះពាល់របស់វា
ការអនុវត្ត: Implementation	ដំណើរការបញ្ចូលការតាក់តែងទៅក្នុងធាតុផ្សំផ្នែករឹង ផ្នែកទន់ ឬក្នុងផ្នែកទាំងពីរ
ការអនុវត្តសាកល្បងសុវត្ថិភាព: Security Testing	ការអនុវត្តសាកល្បងសុវត្ថិភាពលើផ្នែកផ្សេងៗនៃប្រព័ន្ធ
កំហុស: Error	ភាពខុសគ្នារវាងតម្លៃឬលក្ខខណ្ឌដែលបានគណនា អង្កេត ឬវាស់វែង ធៀបនឹងតម្លៃ ឬលក្ខខណ្ឌដែលត្រឹមត្រូវ
កម្មវិធីកុំព្យូទ័រ ឬផ្នែកទន់: Software	កម្មវិធី នីតិវិធី វិធាន និងឯកសារផ្សេងៗពាក់ព័ន្ធទៅនឹងប្រតិបត្តិការរបស់ប្រព័ន្ធ ដែលខុសពីផ្នែករឹង

កម្មវិធីស្រេច: Application (Software)	កម្មវិធីកុំព្យូទ័រដែលតាក់តែងឡើងដើម្បីបំពេញតម្រូវការជាក់លាក់របស់អ្នកប្រើប្រាស់។ ឧទាហរណ៍ កម្មវិធីសម្រាប់នាំផ្លូវ កម្មវិធីគ្រប់គ្រងប្រាក់បៀវត្ស កម្មវិធីត្រួតពិនិត្យដំណើរការ
កម្មវិធីរៀបតម្រូវ: Configurable software	កម្មវិធីរៀបតម្រូវផ្តល់នូវសន្ធានកម្ម និងមុខងារជាស្តង់ដារដែលអាចឱ្យអ្នកប្រើប្រាស់កំណត់បាននូវដំណើរការនិងការត្រួតពិនិត្យដ៏ជាក់លាក់
គន្លងសវនកម្ម: Audit trail	ទិន្នន័យដែលប្រើប្រាស់សម្រាប់តាមដានប្រតិបត្តិការដែលប៉ះពាល់ទិន្នន័យបានកត់ត្រា។ គន្លងសវនកម្មអាចរួមបញ្ចូល ឈ្មោះអ្នកកែចម្លងការ និងពេលវេលាកែ ជាដើម
ដំណើរការ: Processing	ការអនុវត្តនូវប្រតិបត្តិការដែលកំណត់ទុកជាមុនតាមលំដាប់បន្តគ្នាលើទិន្នន័យបញ្ចូលដើម្បីបញ្ចេញជា ទិន្នន័យ ឬព័ត៌មាន
តម្រូវការ: Requirement	ការរំពឹងទុកដែលបានបញ្ជាក់ជាកាតព្វកិច្ចច្បាស់លាស់ ឬដោយប្រយោល
តម្រូវការជាក់លាក់នៃអ្នកប្រើប្រាស់: User Requirements Specification (URS)	ឯកសារពណ៌នាអំពីសេចក្តីត្រូវការរបស់អ្នកប្រើប្រាស់
ទិន្នន័យ: Data	លេខ តួអក្សរ រូបភាព ឬកំណត់ត្រាតាមវិធីសាស្ត្រផ្សេងៗ ក្នុងទម្រង់ដែលអាចវាយតម្លៃបានដោយមនុស្ស ឬអាចបញ្ចូលក្នុងកុំព្យូទ័រ។ ត្រឹមតែជាទិន្នន័យ នៅពុំទាន់មានអត្ថន័យនៅឡើយ លើកលែងទិន្នន័យនោះត្រូវបានបកប្រែដោយប្រព័ន្ធដំណើរការទិន្នន័យ ទើបមានអត្ថន័យ ហើយក្លាយទៅជាព័ត៌មាន
ធាតុចូល: Input	ក. ទិន្នន័យដែលបញ្ចូលក្នុងកុំព្យូទ័រសម្រាប់ដំណើរការ ខ. ដំណើរការបញ្ចូលទិន្នន័យទៅក្នុងប្រព័ន្ធកុំព្យូទ័រ
ធាតុចេញ/ទិន្នន័យបញ្ចេញ: Output	ទិន្នន័យបញ្ជូនពីប្រព័ន្ធកុំព្យូទ័រទៅខាងក្រៅតាមរយៈឧបករណ៍បញ្ចេញទិន្នន័យ ឬព័ត៌មានផ្សេងៗ
ធាតុផ្សំសំខាន់: Critical Component	ធាតុផ្សំនៅក្នុងប្រព័ន្ធដែលប្រតិបត្តិការ ទំនាក់ទំនង ទិន្នន័យ ការត្រួតពិនិត្យ ការផ្តល់សញ្ញា ឬការខ្វះខាតរបស់វា អាចនឹងមានផលប៉ះពាល់ផ្ទាល់លើការសម្រេចបាននៃគោលបំណងធុរកិច្ច
ធនធានឌីជីថល: Digital Assets	រាល់សម្ភារៈឌីជីថលរួមមានអត្ថបទ ក្រាហ្វិក អូឌីយ៉ូ និងវីដេអូចលនា ដែលគ្រប់គ្រងដោយបុគ្គលឬសហគ្រាស
បូរណភាព: Integrity	ការការពារ ឬការស្វែងរកលើការកែប្រែដែលគ្មានការអនុញ្ញាត។ ឧទាហរណ៍ ការកែប្រែលើទិន្នន័យ

បូរណភាពទិន្នន័យ: Data Integrity	សូមមើលពាក្យ "បូរណភាព" ខាងក្រោម
បន្ទាត់មូលដ្ឋាន: Baseline	មូលដ្ឋាន ឬចំណុចគោលសម្រាប់ប្រៀបធៀប ដើម្បីធ្វើការវាយតម្លៃ។ ឧទាហរណ៍: ប្រព័ន្ធសុវត្ថិភាពជាមូលដ្ឋាន
ប្រព័ន្ធកុំព្យូទ័រ: Computerized System	ដំណើរការ ឬប្រតិបត្តិការបញ្ចូលជាមួយប្រព័ន្ធកុំព្យូទ័រ រួមមានផ្នែករឹង ផ្នែកទន់ ឧបករណ៍កុំព្យូទ័រ បុគ្គលិក និងឯកសារ (សៀវភៅណែនាំ និងស្តង់ដារប្រតិបត្តិ ឬនីតិវិធី)
ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច: Application controls	នីតិវិធីត្រួតពិនិត្យផ្ទៃក្នុងលើប្រព័ន្ធកម្មវិធីស្រេច ដែលធានាថាចម្ងាយការទាំងអស់ត្រូវបានអនុញ្ញាត កត់ត្រា និងត្រូវបានដំណើរការដោយពេញលេញ ត្រឹមត្រូវ និងទាន់ពេលជាមួយលទ្ធផលតាមការកំណត់
ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន: IT controls	នីតិវិធី ឬគោលនយោបាយដែលផ្តល់ការធានាសមស្របថាបច្ចេកវិទ្យាព័ត៌មានប្រើប្រាស់ដោយអង្គភាពប្រព្រឹត្តទៅតាមការរំពឹងទុក ទិន្នន័យជឿទុកចិត្តបាន ហើយអនុលោមតាមច្បាប់និងបទប្បញ្ញត្តិជាធរមាន។ ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានចែកជា ប្រព័ន្ធត្រួតពិនិត្យរួម និងប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច
ប្រព័ន្ធត្រួតពិនិត្យហានិភ័យ: System Risk Control	ដំណើរការនាំឱ្យឈានដល់ការសម្រេចចិត្ត និងអនុវត្តវិធានការការពារ ដើម្បីកាត់បន្ថយហានិភ័យ ឬរក្សាហានិភ័យឱ្យស្ថិតក្នុងកម្រិតមួយដែលបានកំណត់
ផែនការស្តារឡើងវិញ: Disaster Recovery Plan	ផែនការស្តារឡើងវិញ ចែងលម្អិតអំពីសកម្មភាពបន្ទាន់ ក្នុងករណីមានបញ្ហា និងមានគោលបំណង ផ្តល់លទ្ធភាពដោះស្រាយបញ្ហាដោយរលូន និងមានប្រសិទ្ធិភាព
ផ្នែករឹង: Hardware	ធាតុផ្សំរូបវន្តដែលត្រូវបានប្រើប្រាស់ក្នុងប្រព័ន្ធកុំព្យូទ័រ។ ឧបករណ៍រូបវន្តមិនមែនជាកម្មវិធី នីតិវិធី វិធាន និងឯកសារពាក់ព័ន្ធផ្សេងៗ
ព័ត៌មានលម្អិត: Specification	ព័ត៌មានចែងអំពីតម្រូវការជាក់លាក់
មជ្ឈមណ្ឌលទិន្នន័យ: Data Centres	ទីតាំងដែលបំពាក់ដោយ ឬភ្ជាប់ជាមួយកុំព្យូទ័រមួយ ឬច្រើនសម្រាប់ដំណើរការ ឬបញ្ជូនទិន្នន័យ
សុវត្ថិភាព: Security	ការពារាំងចំពោះការចូលដំណើរការ និងការផ្លាស់ប្តូរដោយគ្មានការអនុញ្ញាត ព្រមទាំងការបាត់បង់ភាពប្រើប្រាស់បាននៃព័ត៌មាន និងប្រព័ន្ធ
សកម្មភាពកែតម្រូវ: Corrective action	សកម្មភាពដើម្បីលប់បំបាត់ឫសគល់នៃភាពមិនអនុលោម ឬស្ថានភាពមិនសមស្របផ្សេងៗដែលបានរកឃើញ

សវនកម្មបច្ចេកវិទ្យាព័ត៌មាន: IT Audit	ដំណើរការមានលក្ខណៈជាប្រព័ន្ធ ឯករាជ្យ និងចងក្រងឯកសារ ដើម្បីប្រមូល និងវាយតម្លៃភស្តុតាង ក្នុងគោលបំណងបញ្ជាក់អំពីកម្រិតសមស្របជាមួយលក្ខណៈវិនិច្ឆ័យនៃសវនកម្មបច្ចេកវិទ្យាព័ត៌មាន
សវនករបច្ចេកវិទ្យាព័ត៌មាន: IT Auditor	សវនករដែលមានសមត្ថកិច្ចធ្វើផែនការ អនុវត្ត និងរាយការណ៍អំពីការងារសវនកម្មបច្ចេកវិទ្យាព័ត៌មាន
ហានិភ័យ: Risk	ឱកាសដែលព្រឹត្តិការណ៍ ឬសកម្មភាព (រួមទាំងការមិនមានសកម្មភាព) នាំឱ្យមានលទ្ធផលមិនគាប់បំណង ដូចជាផលប៉ះពាល់អវិជ្ជមានលើការសម្រេចបាននូវគោលបំណងធុរកិច្ច ឬកំហុសឆ្គងក្នុងរបាយការណ៍ហិរញ្ញវត្ថុ
ហេដ្ឋារចនាសម្ព័ន្ធ: Infrastructure	ប្រព័ន្ធសម្ភារៈ ឧបករណ៍ និងសេវាកម្មផ្សេងៗសម្រាប់ដំណើរការរបស់អង្គភាព។ សូមមើលហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន
ហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន: IT Infrastructure	បណ្តាញ ម៉ាស៊ីនបម្រើ ម៉ាស៊ីនភ្ជៀវ ម៉ាស៊ីនបោះពុម្ព ជាដើម សូមមើលពាក្យ“ហេដ្ឋារចនាសម្ព័ន្ធ”ខាងលើ
អាយុកាលកម្មវិធីកុំព្យូទ័រ ឬផ្នែកទន់:Software Life Cycle	រយៈពេលរាប់ចាប់តាំងពីផលិតផលកម្មវិធីកុំព្យូទ័រត្រូវបានផលិតរហូតដល់ពេលដែលកម្មវិធីកុំព្យូទ័រ នោះមិនអាចប្រើប្រាស់បានតទៅទៀត។ អាយុកាលនៃកម្មវិធីចែកចេញជាដំហានៗតាមសកម្មភាពផ្សេងៗដូចជា តម្រូវការ ការតាក់តែង ការសរសេរកូដបង្កើតកម្មវិធី ការអនុវត្តសាកល្បង ការតម្លើង និងការប្រតិបត្តិនិងថែរក្សា
អាយុកាលប្រព័ន្ធ: System Life Cycle	រយៈពេលនៃការផ្លាស់ប្តូរប្រែប្រួលដែលប្រព័ន្ធមួយបានឆ្លងកាត់ចាប់តាំងពីការផ្តួចផ្តើមគំនិតដំបូងរហូតដល់ពេលបញ្ឈប់ការប្រើប្រាស់
អត្តសញ្ញាណសំគាល់អ្នកប្រើប្រាស់: User ID	“ឈ្មោះ” របស់អ្នកប្រើប្រាស់នៅក្នុងប្រព័ន្ធកុំព្យូទ័រ ដែលអាចជាឈ្មោះពេញ ឬជាឈ្មោះបង្កើតដោយអក្សរកាត់
អ្នកប្រើប្រាស់: User	មនុស្ស អង្គភាព ឬក្រុមបំពេញការងារដែលប្រើប្រាស់ប្រព័ន្ធព័ត៌មានក្នុងគោលបំណងដំណើរការទិន្នន័យ
ឧបករណ៍បញ្ចូលទិន្នន័យ: Input device	ឧបករណ៍ដែលប្រើប្រាស់ ដើម្បីបញ្ជូនទិន្នន័យពីខាងក្រៅចូលទៅក្នុងប្រព័ន្ធកុំព្យូទ័រ ឧទាហរណ៍ ក្តារចុច ដុំចុច អេក្រង់ពាល់ មីក្រូហ្វូន