ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ
MINISTRY OF ECONOMY AND FINANCE

ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ
លេខ.១០៦៧...សហវ...

ប្រកាស
ស្តីពី
ការជាក់ឱ្យប្រើប្រាស់គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកទិទ្យាព័ត៌មាន

ឧបនាយករដ្ឋមន្ត្រី
រដ្ឋមន្ត្រីក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

- បានឃើញរដ្ឋធម្មនុញ្ញនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកត/០៩១៨/៩២៥ ចុះថ្ងៃទី០៦ ខែកញ្ញា ឆ្នាំ២០១៨ ស្តីពីការតែងតាំងរាជរដ្ឋាភិបាលនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកត/០៣២០/៤២១ ចុះថ្ងៃទី៣០ ខែមីនា ឆ្នាំ២០២០ ស្តីពីការតែងតាំង និងកែសម្រួលសមាសភាពរាជរដ្ឋាភិបាលនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រមលេខ នស/រកម/០៦១៨/០១២ ចុះថ្ងៃទី២៨ ខែមិថុនា ឆ្នាំ២០១៨ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃគណៈរដ្ឋមន្ត្រី
- 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 ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ
- បានឃើញអនុក្រឹត្យលេខ ៧៥ អនក្រ.បក ចុះថ្ងៃទី២៥ ខែឧសភា ឆ្នាំ២០១៧ ស្តីពីការកែសម្រួលអនុក្រឹត្យលេខ ៤៨៨ អនក្រ.បក ចុះថ្ងៃទី១៦ ខែតុលា ឆ្នាំ២០១៣ ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

ផ្លូវលេខ ៩២ សង្កាត់វត្តភ្នំ ខណ្ឌដូនពេញ រាជធានីភ្នំពេញ កម្ពុជា
St.92, Sangkat Wat Phnom, Khan Daun Penh, Phnom Penh, CAMBODIA.
ទូរស័ព្ទ: (+៨៥៥)២៣ ៨៩០ ៦៦៦
Phone: (+855) 23 890 666

- បានឃើញអនុក្រឹត្យលេខ ៤០ អនក្រ.បក ចុះថ្ងៃទី១៥ ខែកុម្ភៈ ឆ្នាំ២០០៥ ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃសវនកម្មផ្ទៃក្នុងនៅតាមបណ្តាស្ថាប័ន ក្រសួង និងសហគ្រាសសាធារណៈ
- បានឃើញប្រកាសលេខ ១៥៤៧ សហវ.ប្រក ចុះថ្ងៃទី៣១ ខែធ្នូ ឆ្នាំ២០១៣ ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃនាយកដ្ឋាន និងអង្គភាពក្រោមឱវាទអគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុងនៃក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ
- បានឃើញប្រកាសលេខ ៧៣៩ សហវ.ប្រក ចុះថ្ងៃទី២៣ ខែមិថុនា ឆ្នាំ២០១៦ ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃនាយកដ្ឋានសវនកម្មបច្ចេកវិទ្យាព័ត៌មាននៃអគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុង នៃក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ
- បានឃើញប្រកាសលេខ ១៦៧៣ សហវ.ប្រក ចុះថ្ងៃទី៣០ ខែធ្នូ ឆ្នាំ២០១៦ ស្តីពីការដាក់ឱ្យប្រើប្រាស់សៀវភៅណែនាំសវនកម្មផ្ទៃក្នុង
- បានឃើញប្រកាសលេខ ៥៤៣ សហវ.ប្រក ចុះថ្ងៃទី៣០ ខែមិថុនា ឆ្នាំ២០២០ ស្តីពីការដាក់ឱ្យប្រើប្រាស់គោលការណ៍ណែនាំសវនកម្មបច្ចេកវិទ្យាព័ត៌មាន
- បានឃើញសារាចរណែនាំលេខ ១២ សរណន ចុះថ្ងៃទី២៥ ខែវិច្ឆិកា ឆ្នាំ២០១១ ស្តីពីការបន្តពង្រឹងមុខងារសវនកម្មផ្ទៃក្នុងតាមបណ្តាក្រសួង ស្ថាប័ន និងសហគ្រាសសាធារណៈ
- យោងតាមតម្រូវការចាំបាច់របស់ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

សម្រេច

ប្រការ១.–

ត្រូវបានដាក់ឱ្យប្រើប្រាស់គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន ជាក្របខណ្ឌសម្រាប់រៀបចំ គ្រប់គ្រង និងត្រួតពិនិត្យលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មានតាមក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែលរបស់រាជរដ្ឋាភិបាល។

ប្រការ២.–

គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន ត្រូវភ្ជាប់ជាឧបសម្ព័ន្ធនៃប្រកាសនេះ។

ប្រការ៣.–

ប្រកាសលេខ ១៤៣៦ សហវ.ប្រក ចុះថ្ងៃទី០៨ ខែធ្នូ ឆ្នាំ២០១៦ ស្តីពីការដាក់ឱ្យប្រើប្រាស់ឯកសារស្តីពីការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន និងបទប្បញ្ញត្តិទាំងឡាយណា ដែលផ្ទុយនឹងប្រកាសនេះ ត្រូវចាត់ជានិរាករណ៍។

ប្រការ៤._

នាយកខុទ្ទកាល័យ អគ្គលេខាធិការ ប្រតិភូរាជរដ្ឋាភិបាលទទួលបន្ទុកជាអគ្គនាយកនៃអគ្គនាយកដ្ឋាន អគ្គនាយកនៃអគ្គនាយកដ្ឋាន អគ្គាធិការនៃអគ្គាធិការដ្ឋាន នាយកនៃវិទ្យាស្ថានសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ ប្រធានអង្គភាពក្រោមឱវាទក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ អង្គភាពនៃក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែលរបស់រាជរដ្ឋាភិបាល ត្រូវទទួលបន្ទុកអនុវត្តប្រកាសនេះតាមភារកិច្ចរៀងៗខ្លួនឱ្យមានប្រសិទ្ធភាព ចាប់ពីថ្ងៃចុះហត្ថលេខាតទៅ។

ថ្ងៃ[illegible] ខែ[illegible] ឆ្នាំឆ្លូវ ត្រីស័ក ព.ស. ២៥៦៥
រាជធានីភ្នំពេញ ថ្ងៃទី[illegible] ខែ[illegible] ឆ្នាំ២០២១

ឧបនាយករដ្ឋមន្ត្រី
រដ្ឋមន្ត្រីក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

អគ្គបណ្ឌិតសភាចារ្យ អូន ព័ន្ធមុនីរ័ត្ន

កន្លែងទទួល៖
-ទីស្តីការគណៈរដ្ឋមន្ត្រី
-ខុទ្ទកាល័យសម្តេចអគ្គមហាសេនាបតីតេជោនាយករដ្ឋមន្ត្រី
-ខុទ្ទកាល័យសម្តេច ឯកឧត្តម លោកជំទាវ ឧបនាយករដ្ឋមន្ត្រី
-គ្រប់ក្រសួង ស្ថាប័ន
-ដូចប្រការ ៤
-រាជកិច្ច
-ឯកសារ-កាលប្បវត្តិ

ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

អគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុង

គោលការណ៍

ក្រមតពិនិត្យផ្ទៃក្នុងបច្ចេកទិទ្យាព័ត៌មាន

ឆ្នាំ ២០២១

រៀបចំដោយអគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុង

មាតិកា

ទំព័រ

សេចក្តីផ្តើម

ក្នុងបរិការណ៍បច្ចុប្បន្ន ការប្រើប្រាស់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានក្នុងដំណើរការគ្រប់គ្រងផ្ទៃក្នុងរបស់ក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែលនៃរាជរដ្ឋាភិបាលនៅមានកម្រិតនៅឡើយ។ នាពេលអនាគត ក្នុងគោលដៅទំនើបភាវូបនីយកម្ម ដើម្បីធានាឱ្យបាននូវប្រសិទ្ធភាព តម្លាភាព និងភាពឆាប់រហ័សនៃការត្រួតពិនិត្យរបស់រាជរដ្ឋាភិបាល រាល់ដំណើរការ ក៏ដូចជាកិច្ចបញ្ជិកានានានឹងត្រូវពឹងផ្អែកកាន់តែច្រើនឡើងលើប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។

ការរីកចម្រើនស្ទ័យប្រវត្តិកម្មនៃដំណើរការធុរកិច្ចនឹងមិនធ្វើឱ្យប្រែប្រួលដល់គោលបំណងនៃការគ្រប់គ្រង ឬសវនកម្មផ្ទៃក្នុងទេ ក៏ប៉ុន្តែនឹងនាំមកនូវហានិភ័យថ្មីៗដែលងាយនឹងក្លាយជាប្រភពកំហុសថ្មី។ ទន្ទឹមនឹងនេះ ភាពរួបីនៃចម្ងល់ការត្រូវបានកាត់បន្ថយ ដែលតម្រូវឱ្យថ្នាក់ដឹកនាំនិងសវនករអនុវត្តវិធីសាស្ត្រនិងបច្ចេកទេសត្រួតពិនិត្យថ្មី និងត្រូវធ្វើការផ្លាស់ប្តូរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង ដែលមានពេលបច្ចុប្បន្ន ដើម្បីបង្ការនិងកាត់បន្ថយហានិភ័យ។

បន្ទាប់ពីការដាក់ឱ្យប្រើប្រាស់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ប្រព័ន្ធនេះនឹងក្លាយជាផ្នែកមួយដ៏សំខាន់នៃយន្តការត្រួតពិនិត្យផ្ទៃក្នុង ហើយអាចសម្រេចបានជោគជ័យអាស្រ័យជាចម្បងលើគុណភាពនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងផ្សេងៗទៀតដែលពាក់ព័ន្ធ។

ក្នុងបរិបទនេះ អគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុងនៃក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ បានរៀបចំ “គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន” សម្រាប់ក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែលប្រើប្រាស់ដើម្បីតាក់តែងនិងវាយតម្លៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។ ម្យ៉ាងទៀតគោលការណ៍នេះ ក៏ផ្តល់ជូនសវនករនូវលក្ខណៈវិនិច្ឆ័យសម្រាប់វាយតម្លៃលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មានដែលបានដាក់អនុវត្តដោយថ្នាក់ដឹកនាំ។

គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន ចែកជាពីរផ្នែក÷

- ផ្នែក ក: ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន
- ផ្នែក ខ: គោលការណ៍ និងស្តង់ដារប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

ផ្នែក ក: ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

១. ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (បបព)

ព័ត៌មានគឺជាបណ្តុំនៃទិន្នន័យ ដែលអាចជាព័ត៌មានហិរញ្ញវត្ថុ និងមិនមែនហិរញ្ញវត្ថុ និងត្រូវបានផ្តល់ជូនថ្នាក់ដឹកនាំ ដើម្បីធ្វើការសម្រេចចិត្ត។ ទន្ទឹមនឹងនេះ ព័ត៌មានគឺជាទ្រព្យសកម្មមួយដូចទ្រព្យសកម្មនៃធុរកិច្ចសំខាន់ៗដទៃទៀត ដែលមានតម្លៃដល់អង្គភាព និងទាមទារកិច្ចការពារឱ្យបានហ្មត់ចត់។

បបព ត្រូវបានកំណត់ថាជាការរួមបញ្ចូលគ្នានៃយុទ្ធសាស្ត្រ ការគ្រប់គ្រង និងសកម្មភាពប្រតិបត្តិការ រួមទាំងដំណើរការដែលពាក់ព័ន្ធនឹងការប្រមូល កិច្ចដំណើរការ ការរក្សាទុក ការចែកចាយ និងការប្រើប្រាស់ព័ត៌មាននិងបច្ចេកវិទ្យាពាក់ព័ន្ធ។ ដូច្នេះ បបព ក៏តម្រូវឱ្យមានកិច្ចការពារផងដែរ តាមរយៈការចាត់ចែងរបស់ថ្នាក់ដឹកនាំ នៅក្នុងការតាក់តែង ការដាក់អនុវត្ត ការថែរក្សា ដើម្បីទទួលបាន បបព មួយដែលមានប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងសមស្រប និងគ្រប់គ្រាន់។

២. និយមន័យ និងគោលបំណងនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង គឺជាដំណើរការអនុវត្តដោយថ្នាក់ដឹកនាំ និងបុគ្គលិកផ្សេងទៀតដែលត្រូវបានរៀបចំឡើង ដើម្បីធានាដល់ការសម្រេចបាននូវគោលដៅដូចខាងក្រោម÷

- របាយការណ៍ហិរញ្ញវត្ថុដែលអាចជឿទុកចិត្តបាន
- ប្រសិទ្ធភាព និងប្រសិទ្ធផលនៃប្រតិបត្តិការ
- អនុលោមភាពជាមួយច្បាប់ និងបទប្បញ្ញត្តិ
- ការពារសុវត្ថិភាពទ្រព្យសម្បត្តិ

(ប្រភព: ផ្អែកលើនិយមន័យនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង របស់ COSO)

គោលបំណងនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង គឺដើម្បីធានាឱ្យបាននូវគោលដៅ ឬលក្ខខណ្ឌដែលអាចកាត់បន្ថយដល់កម្រិតអប្បបរមាលើការខ្ជះខ្ជាយ ការបាត់បង់ ការប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត ឬការបែងចែកមិនសមស្រប។ ម៉្យាងទៀត ដើម្បីឱ្យគោលបំណងនៃការត្រួតពិនិត្យសម្រេចបានប្រកបដោយប្រសិទ្ធភាព សកម្មភាពអនុលោមតាមគោលបំណងត្រូវតែអាចវាស់វែង និងសង្កេតបាន។

ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងរបស់ បបព ត្រូវរៀបចំឡើងដើម្បីជួយដល់ថ្នាក់ដឹកនាំសម្រេចបាននូវគោលបំណង ដូចខាងក្រោម÷

- **ការពារសុវត្ថិភាពទ្រព្យសម្បត្តិ:** ព័ត៌មាននៅលើប្រព័ន្ធស្ងួយប្រវត្តិបានធ្វើបច្ចុប្បន្នភាព និងធានាបានសុវត្ថិភាពពីការចូលដោយគ្មានការអនុញ្ញាត
- **ធានាបូរណភាពនៃបរិស្ថានប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរសើប និងសំខាន់:**
    - ការអនុញ្ញាត - ធានាថាចម្លងការទាំងអស់ត្រូវបានទទួលការឯកភាពពីមន្ត្រីទទួលខុសត្រូវ ស្របតាមសិទ្ធិសម្រេចជាទូទៅ ឬដោយឡែកមុនពេលដែលចម្លងការត្រូវបានទាត់ត្រា

- សុពលភាព - មានតែប្រតិបត្តិការដែលបានអនុញ្ញាតហើយដែលកើតឡើងពិតប្រាកដ និងពាក់ព័ន្ធនឹងអង្គភាពប៉ុណ្ណោះត្រូវបានកត់ត្រា
- ភាពពេញលេញ - រាល់ប្រតិបត្តិការដែលកើតឡើងត្រូវបានបញ្ចូល និងទទួលយកសម្រាប់ដំណើរការនៅក្នុងប្រព័ន្ធតែមួយលើក
- សុក្រឹតភាព - ប្រតិបត្តិការត្រូវបានកត់ត្រាន្លូវចំនួន និងក្នុងគណនីត្រឹមត្រូវជាមួយពេលសមស្រប។

- **ការកំណត់អត្តសញ្ញាណ និងការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវ:** ដើម្បីធានាបាននូវភាពសមស្របលើការគ្រប់គ្រងការកំណត់អត្តសញ្ញាណ និងផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវនៃអ្នកប្រើប្រាស់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (ទាំងអ្នកប្រើប្រាស់ចុងក្រោយ និងអ្នកគាំទ្រហេដ្ឋារចនាសម្ព័ន្ធ)។
- **ប្រសិទ្ធភាព និងប្រសិទ្ធផលនៃប្រតិបត្តិការ:** ដើម្បីធានាបាននូវប្រសិទ្ធភាព និងប្រសិទ្ធផលនៃប្រតិបត្តិការដែលគាំទ្រដោយប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។
- **លទ្ធភាពប្រើប្រាស់នៃសេវាកម្មបច្ចេកវិទ្យាព័ត៌មាន:** រៀបចំផែនការបន្តធុរកិច្ច (BCP) និងផែនការស្តារគ្រោះមហន្តរាយ (DRP) ប្រកបដោយប្រសិទ្ធភាព ដែលរួមមានដំណើរការចម្លងទុក និងស្តារឡើងវិញ។
- **ការឆ្លើយតបនុប្បត្តិហេតុ:** ធានាថានុប្បត្តិហេតុទាំងអស់គ្រប់គ្រងបានត្រឹមត្រូវ និងកំហុសដែលបានរកឃើញនៅគ្រប់ដំណាក់កាលនៃដំណើរការត្រូវបានកែតម្រូវទាន់ពេល និងរាយការណ៍ទៅថ្នាក់គ្រប់គ្រងសមស្រប។
- **បូរណភាព និងភាពជឿជាក់នៃប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន:** ធានាបាននូវប្រសិទ្ធភាពនៃការអនុវត្តនីតិវិធីគ្រប់គ្រងការផ្លាស់ប្តូរ។
- **ដំណើរការ និងសេវាកម្មប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានផ្តល់ពីខាងក្រៅ:** ធានាថាដំណើរការ និងសេវាកម្មប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌បានកំណត់ច្បាស់នូវកិច្ចព្រមព្រៀងកម្រិតសេវាកម្ម (SLA) និងលំតូខ័ណ្ឌនៃកិច្ចសន្យាដើម្បីធានាថាទ្រព្យសម្បត្តិអង្គភាពត្រូវបានការពារត្រឹមត្រូវ ហើយបំពេញតាមគោលដៅ និងគោលបំណងធុរកិច្ច។

ដំណើរការដែលតាក់តែងបានល្អ ប្រកបដោយប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងសមស្រប គួរបញ្ចូលនូវគោលបំណងខាងលើឱ្យបានច្រើនប្រសិនជាមិនអាចបានទាំងអស់។

៣. ការទទួលខុសត្រូវលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

ថ្នាក់ដឹកនាំក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែល ត្រូវទទួលខុសត្រូវលើការតាក់តែង និងការដាក់ឱ្យអនុវត្តប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងទាំងអស់ រួមទាំងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងសម្រាប់ បបព ដើម្បីធានាថា÷

- បបព ដែលបានអនុវត្តកន្លងមក និងស្នើឡើងត្រូវមានរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងគ្រប់គ្រាន់
- ការអភិវឌ្ឍ និងការដាក់អនុវត្តហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និងកម្មវិធីប្រើប្រាស់នៅគ្រប់ដំណាក់កាលត្រូវមានប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងគ្រប់គ្រាន់

- ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងមានការពឹងផ្អែកលើស្វ័យប្រវត្តិកម្មច្រើនជាងដោយដៃ
- ស្តង់ដារអប្បបរមានៃការត្រួតពិនិត្យផ្ទៃក្នុងត្រូវបានអនុវត្ត (លម្អិតចំណុច ៥.៧)
- ប្រព័ន្ធត្រួតពិនិត្យគន្លឹះត្រូវបានដាក់អនុវត្តជាប្រចាំ ដោយមានភស្តុតាងបញ្ជាក់អត្ថិភាពនៃប្រតិបត្តិការទាំងនោះ
- ប្រព័ន្ធត្រួតពិនិត្យការពារ ត្រូវបានអនុវត្តយ៉ាងយកចិត្តទុកដាក់ ដោយមានការគាំទ្រពីប្រព័ន្ធត្រួតពិនិត្យស្វែងរក និងប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវសមស្រប
- នៅពេលប្រព័ន្ធត្រួតពិនិត្យដោយស្វ័យប្រវត្តិពុំទាន់ជឿជាក់បាន ការអនុវត្តប្រព័ន្ធត្រួតពិនិត្យដោយដៃត្រូវដាក់បន្ថែម
- រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចុប្បន្នត្រូវផ្លាស់ប្តូរជាបណ្តើរៗ ទៅជាប្រព័ន្ធត្រួតពិនិត្យចម្រុះសមស្រប រវាងប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ និងដោយដៃ
- បច្ចេកទេសសវនកម្មបច្ចេកវិទ្យាព័ត៌មានត្រូវបានបញ្ចូលទៅក្នុងស្ថាប័នរបស់ខ្លួន
- ប្រសិទ្ធភាពសវនកម្មផ្ទៃក្នុងត្រូវបានបង្កើនឱ្យខិតទៅរកគម្រិតស្តង់ដារ
- សវនករផ្ទៃក្នុងតាមក្រសួង ស្ថាប័ន ត្រូវបានបណ្តុះបណ្តាលលើការរៀបចំផែនការ ការវាយតម្លៃ និងការធ្វើរបាយការណ៍អំពីការត្រួតពិនិត្យផ្ទៃក្នុងនៅក្នុងបរិស្ថាន បបព។

សវនកម្មផ្ទៃក្នុងមានតួនាទីពិនិត្យតាមដានការត្រួតពិនិត្យផ្ទៃក្នុង ដែលរៀបចំដោយថ្នាក់ដឹកនាំក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែល ហើយផ្តល់ការអះអាងដើម្បីជួយដល់ថ្នាក់ដឹកនាំក្នុងការអនុវត្ត និងការរក្សាបាននូវភាពគ្រប់គ្រាន់ និងត្រឹមត្រូវនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង បបព។

៤. បច្ចុប្បន្នភាពគោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

អគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុង (អសក) នៃក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ (កសហវ) ត្រូវពិនិត្យឡើងវិញជារៀងរាល់ឆ្នាំនូវ "គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន" និងធ្វើការកែតម្រូវតាមការចាំបាច់។

ផ្នែក ខ: គោលការណ៍ និងស្តង់ដារប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

ខាងក្រោមនេះ គឺជាគោលការណ៍ និងស្តង់ដារដែលថ្នាក់ដឹកនាំក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែល ត្រូវអនុវត្តដើម្បីបង្កើត ពង្រឹង និងអភិវឌ្ឍន៍នូវរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងគ្រប់គ្រាន់មួយសម្រាប់ បបព។

១. ការទទួលខុសត្រូវលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

ថ្នាក់ដឹកនាំក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែល ជាអ្នកទទួលខុសត្រូវលើការតាក់តែង ការដាក់អនុវត្ត និងការថែរក្សារចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង (លម្អិតផ្នែក ក ចំណុច ៣) ។ ថ្នាក់ដឹកនាំ រួមទាំងមន្ត្រីទាំងអស់ត្រូវទទួលខុសត្រូវក្នុងការ អនុវត្តលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងស្របតាមបទប្បញ្ញត្តិពាក់ព័ន្ធ។ សវនកម្មផ្ទៃក្នុង ត្រូវផ្តល់នូវការអះអាងជូនថ្នាក់ដឹកនាំអំពីគុណភាពនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង និងប្រសិទ្ធភាពនៃការអនុវត្តប្រព័ន្ធនេះ។

២. លក្ខណៈនៃប្រព័ន្ធត្រួតពិនិត្យល្អ

- ការបែងចែកភារកិច្ចឱ្យបានសមស្រប
- ការត្រួតពិនិត្យលើការគ្រប់គ្រង
- ជំហានដំណើរការមានលំដាប់លំដោយត្រឹមត្រូវ
- ការងារបានធ្វើ និងកំពុងធ្វើ នៅតាមទីកន្លែង និងពេលវេលាដែលត្រឹមត្រូវតាមលំដាប់លំដោយនិងជំនាញ
- ចំណុចរួមនៃការទទួលខុសត្រូវរបស់ថ្នាក់គ្រប់គ្រង
- ចំណុចដោះស្រាយ និងពាក់ព័ន្ធមានតិចបំផុត
- ចលនានៃលំហូរការងារត្រឡប់ក្រោយមានតិចបំផុត
- សកម្មភាពជាយថាហេតុមានតិចបំផុត។

៣. ស្តង់ដារនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

ក្របខ័ណ្ឌសវនកម្មកំណត់ដោយគណៈកម្មាធិការនៃអង្គការគាំទ្ររបស់ស្នងការទ្រីដវ៉ៃ (COSO) ត្រូវបានយកមកប្រើប្រាស់ដើម្បីវាយតម្លៃលើភាពគ្រប់គ្រាន់នៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។ COSO ផ្តោតលើផ្នែកចំនួន ៥ សម្រាប់សម្រេចគោលបំណងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង រួមមានបរិស្ថានត្រួតពិនិត្យ ការវាយតម្លៃហានិភ័យ សកម្មភាពត្រួតពិនិត្យ ព័ត៌មាននិងគមនាគមន៍ និងការតាមដាន ។

ក្របខ័ណ្ឌ COSO មិនអាចប្រើប្រាស់សម្រាប់ធ្វើសវនកម្មប្រព័ន្ធព័ត៌មានបានពេញលេញទេ គឺត្រូវប្រើប្រាស់ក្របខ័ណ្ឌ "គោលបំណងប្រព័ន្ធត្រួតពិនិត្យព័ត៌មាន និងបច្ចេកវិទ្យាពាក់ព័ន្ធ" (Control Objectives for Information and Related Technology-COBIT) នៃសមាគមសវនកម្ម និងត្រួតពិនិត្យប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (ISACA)។ នៅក្នុងការអនុវត្ត COBIT សម្រាប់ធ្វើសវនកម្មប្រព័ន្ធព័ត៌មាន ពិសេសការវាយតម្លៃលើភាពគ្រប់គ្រាន់នៃប្រព័ន្ធត្រួតពិនិត្យ ផ្នែកក្នុងនៃ បបព ត្រូវគោរពគោលបំណងរបស់ COSO ខាងលើ។

៤. ការវាយតម្លៃហានិភ័យប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ការវាយតម្លៃហានិភ័យត្រូវអនុវត្តជាប្រចាំ ហើយប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងត្រូវតាក់តែង ដើម្បីកាត់បន្ថយហានិភ័យដែលបានកត់សម្គាល់ឃើញ។

"ហានិភ័យ" គឺជាស្ថានភាពដែលព្រឹត្តិការណ៍ ឬសកម្មភាព (រួមទាំងដំណើរគ្មានសកម្មភាព) បានផ្តល់ផលប៉ះពាល់ទៅលើការសម្រេចគោលបំណងធុរកិច្ច ឬកំហុសឆ្គងនៅក្នុងរបាយការណ៍ហិរញ្ញវត្ថុ។ កម្រិតហានិភ័យអាចវាស់វែងដោយផ្អែកលើលទ្ធភាព និងផលប៉ះពាល់នៃព្រឹត្តិការណ៍ដែលអាចកើតឡើង។ ហានិភ័យអាចកើតឡើងនៅក្នុងដំណើរការធុរកិច្ច និងដំណើរការផ្សេងទៀត ដែលពាក់ព័ន្ធនឹងការអភិវឌ្ឍន៍ និងប្រតិបត្តិការប្រចាំថ្ងៃនៃ បបព។

ហានិភ័យដែលទាក់ទងនឹងដំណើរការ បបព ត្រូវបានកំណត់ បន្ទាប់មកប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងត្រូវតាក់តែងឡើងដោយចំណុចចាប់ផ្តើមសំខាន់ គឺវាយតម្លៃរចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យដែលមានស្រាប់ ដើម្បីកែតម្រូវក្នុងករណីមិនឆ្លើយតបក្នុងបរិស្ថានស្ងួយប្រវត្តិ។

៥. គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

៥.១. ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងត្រូវមានរចនាសម្ព័ន្ធដែលមានលក្ខណៈគ្រប់គ្រាន់ និងត្រូវដាក់ឱ្យអនុវត្តពីដើមទីក្នុងគ្រប់ដំណាក់កាលនៃវដ្តកសាង បបព។

បបព នឹងក្លាយជាផ្នែកមួយយ៉ាងសំខាន់នៅក្នុងរចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងរបស់រាជរដ្ឋាភិបាល នៅពេលបានដាក់ឱ្យប្រើប្រាស់ពេញលេញ។ ហេតុនេះមុនដាក់អនុវត្ត និងពង្រីកបន្ថែម បបព ត្រូវមានរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងប្រទាក់ក្រឡា និងរឹងមាំដែលអាចសម្រេចបាន ដូចជាតាមរយៈការដាក់អនុវត្តពីដើមទីនៅតាមទីតាំងសាកល្បងជាដើម។

៥.២. អត្ថប្រយោជន៍នៃស្ងួយប្រវត្តិកម្មប្រព័ន្ធត្រួតពិនិត្យ

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ជំរុញការផ្លាស់ប្តូរជាបណ្តើរៗពីរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដោយដៃទៅជាប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងស្ងួយប្រវត្តិ។ ផលប្រយោជន៍នៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងស្ងួយប្រវត្តិ មាន:

- កាត់បន្ថយលទ្ធភាពអាចកើតឡើងនូវកំហុស និងការកេងបន្លំដែលបង្កដោយមនុស្ស
- ចំណាយពេលតិចជាងក្នុងការងារ ឬការគ្រប់គ្រងដែលបំពេញដោយដៃ
- បង្កើនវិសាលភាពនិងគុណភាពនៃការធ្វើតេស្តសវនកម្មតាមរយៈការទាញយកនិងការប្រមូលកំណត់ត្រា និងទិន្នន័យអេឡិចត្រូនិក

- បង្កើនប្រសិទ្ធភាពសវនកម្មតាមរយៈការជំនួសការធ្វើតេស្តសវនកម្មដោយដៃ ដែលយឺតយ៉ាវនិងងាយកើតមានកំហុស ដោយកម្មវិធីស្រេច។

ដើម្បីទទួលបានអត្ថប្រយោជន៍ពេញលេញពី បបព សវនកម្មផ្ទៃក្នុងត្រូវមានសិទ្ធិចូលដល់ដំណើរការជាក់ស្តែង (គ្មានសិទ្ធិកែប្រែ) និងមានលទ្ធភាពទាញយកទិន្នន័យពីប្រព័ន្ធ និងកម្មវិធីជាក់លាក់សម្រាប់បម្លែងទិន្នន័យទាំងនេះ។

៥.៣. គោលការណ៍ទូទៅនៃការគាក់តែង និងធានាប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ការគាក់តែងប្រព័ន្ធត្រួតពិនិត្យលើប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ត្រូវគោរពគោលការណ៍ទូទៅមួយចំនួនដូចជា÷

- ការបង្កើតប្រព័ន្ធត្រួតពិនិត្យនៅក្នុងកម្មវិធីស្រេច មានប្រសិទ្ធភាពជាងការរង់ចាំសង្កេត និងធ្វើសវនកម្មក្រោយពេលអនុវត្ត
- ប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវក្នុងកម្មវិធីស្រេចអាចជឿទុកចិត្តជាងប្រព័ន្ធត្រួតពិនិត្យដោយដៃ
- កម្រិតរឹងមាំនៃការត្រួតពិនិត្យផ្ទៃក្នុង អាចបង្កើនតាមរយៈការជំនួសប្រព័ន្ធត្រួតពិនិត្យដោយដៃជាមួយប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវក្នុងកម្មវិធីស្រេចជាបណ្តើរៗ។

ក្នុងដំណាក់កាលគាក់តែងកម្មវិធីស្រេច សវនករត្រូវវាយតម្លៃលើប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវដែលចាត់ទុកជាមូលដ្ឋានគោល ក្នុងការធានាភាពគ្រប់គ្រាន់នៃប្រព័ន្ធត្រួតពិនិត្យនៅមុនដំណាក់កាលដាក់ឱ្យអនុវត្ត បបព។ ដោយឡែក នៅដំណាក់កាលក្រោយការដាក់ឱ្យអនុវត្ត គួរវាយតម្លៃលើប្រព័ន្ធត្រួតពិនិត្យជាក់ស្តែង ដើម្បីផ្តល់ការធានាថាប្រព័ន្ធត្រួតពិនិត្យត្រូវបានប្រើប្រាស់ប្រកបដោយប្រសិទ្ធភាព។

ការធ្វើតេស្តលើប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវមិនចាំបាច់ធ្វើជាប្រចាំឆ្នាំនោះទេ ប្រសិនបើការគ្រប់គ្រងការផ្លាស់ប្តូរនិងសុវត្ថិភាព ដំណើរការប្រកបដោយប្រសិទ្ធភាព។

៥.៤. ទស្សនទាននៃប្រព័ន្ធត្រួតពិនិត្យ

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ទស្សនទាននៃប្រព័ន្ធត្រួតពិនិត្យជាលាយលក្ខណ៍អក្សរត្រូវរៀបចំ ដើម្បីជួយក្នុងការគាក់តែងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងឱ្យមានភាពប្រទាក់ក្រឡា សង្គតិភាព និងប្រសិទ្ធភាព។ ការអនុវត្ត បបព ដោយជោគជ័យត្រូវអនុលោមតាមទស្សនទាន និងអភិក្រមប្រព័ន្ធត្រួតពិនិត្យជាលាយលក្ខណ៍អក្សរច្បាស់លាស់ ជាអាទិ៍÷

- ការកំណត់ហានិភ័យគន្លឹះ
- រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យសមស្របដែលត្រូវអនុវត្ត
- ជម្រើសពាក់ព័ន្ធនឹងគោលការណ៍ទូទៅនៃការគាក់តែងប្រព័ន្ធត្រួតពិនិត្យ ដែលបានបង្ហាញនៅផ្នែកខាងលើ (ពិនិត្យចំណុច ៥.៣)

- ប្រព័ន្ធត្រួតពិនិត្យជាមូលដ្ឋានដែលត្រូវជ្រើសយកមានប្រព័ន្ធត្រួតពិនិត្យការពារ ប្រព័ន្ធត្រួតពិនិត្យស្វែងរក និងប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវ
- កំណត់ "ស្តង់ដារប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា" ដែលត្រូវដាក់អនុវត្ត
- តុល្យភាពសមស្របរវាងប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ និងដោយដៃ
- ចាត់ចែងលើការគ្រប់គ្រងការផ្លាស់ប្តូរសម្រាប់រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។

៥.៥. ប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ និងដោយដៃ

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ និងដោយដៃ គួរត្រូវដាក់អនុវត្តរួមគ្នាជាមួយតុល្យភាពសមស្រប។ ប្រព័ន្ធត្រួតពិនិត្យ និងរចនាសម្ព័ន្ធនៃកម្មវិធីស្រេច ជាបន្សំរវាងប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ និងដោយដៃ។

តម្រូវការគន្លឹះដើម្បីទទួលបានប្រព័ន្ធត្រួតពិនិត្យអប្បបរមាស្តង់ដារ គឺត្រូវធានាថារចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យទាំងមូលបានបញ្ចូលប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ និងបំពេញបន្ថែមនូវប្រព័ន្ធត្រួតពិនិត្យដោយដៃជាមួយតុល្យភាពសមស្រប។ ប្រការនេះមានសារៈសំខាន់ក្នុងអំឡុងពេលនៃការផ្លាស់ប្តូរប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។

៥.៦. ប្រភេទនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ គួរអនុវត្តនៅតាមទីកន្លែងដែលអាចធ្វើបាន។ ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទៅតាមគោលបំណងត្រួតពិនិត្យអាចចែកជាបីប្រភេទ÷

- ការពារ
- ស្វែងរក
- កែតម្រូវ

ទន្ទឹមនេះ ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានក៏អាចចែកជាបីប្រភេទតាមមធ្យោបាយដាក់ឱ្យប្រើប្រាស់÷

- រដ្ឋបាល
- បច្ចេកទេស/ប្រព័ន្ធ
- រូបវន្ត

ប្រព័ន្ធត្រួតពិនិត្យការពារស្វ័យប្រវត្តិជារឿយៗ ត្រូវបានចាត់ទុកថាជាប្រព័ន្ធត្រួតពិនិត្យ[illegible] ពេលបង្កើត ប្រសិទ្ធភាពប្រតិបត្តិការនៃប្រព័ន្ធនេះមិនអាស្រ័យលើអន្តរាគមន៍របស់មនុស្សទេ និងមានសកម្មភាពមុនពេលកំហុសកើតឡើង។ ផ្ទុយមកវិញប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវដោយដៃមានលក្ខណៈទន់ខ្សោយ។

៥.៧. ប្រព័ន្ធត្រួតពិនិត្យអប្បបរមាស្តង់ដារ

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងអប្បបរមាស្តង់ដារ ត្រូវប្រកាន់ខ្ជាប់ឱ្យបានគ្រប់ពេលវេលា។ ប្រព័ន្ធត្រួតពិនិត្យដែលរឹងមាំបំផុត ត្រូវមានសមាសធាតុប្រាំបួន រួមមាន: ប្រព័ន្ធត្រួតពិនិត្យការពារ ប្រព័ន្ធត្រួតពិនិត្យស្វែងរក និងប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវ ដែលប្រព័ន្ធត្រួតពិនិត្យនីមួយៗ ត្រូវបានដាក់ឱ្យប្រើប្រាស់តាមវិធីសាស្ត្រ រដ្ឋបាល រូបវន្ត និងបច្ចេកទេស/ប្រព័ន្ធ។ ប្រសិទ្ធភាពអប្បរមានៃប្រព័ន្ធត្រួតពិនិត្យទាមទារឱ្យអនុជំណើរការនីមួយៗ ត្រូវមានប្រព័ន្ធត្រួតពិនិត្យនីមួយៗនៃប្រព័ន្ធត្រួតពិនិត្យទាំងបី។ គោលការណ៍ណែនាំណាដែលមិនមានយន្តការការពារ ស្វែងរក ឬកែតម្រូវ មិនគួរដាក់ឱ្យប្រតិបត្តិការទេ។ ប្រព័ន្ធត្រួតពិនិត្យមិនគ្រប់គ្រាន់អាចកត់សំគាល់ឃើញតាមរយៈការតាក់តែង ឬការអនុវត្តជាក់ស្តែងរបស់ប្រព័ន្ធដែលមិនមានប្រសិទ្ធភាព។

ជាទូទៅ:

ប្រព័ន្ធត្រួតពិនិត្យខ្លាំង = ពហុប្រព័ន្ធត្រួតពិនិត្យការពារ + ពហុប្រព័ន្ធត្រួតពិនិត្យស្វែងរក + ពហុប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវ

ប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា = ប្រព័ន្ធត្រួតពិនិត្យការពារមួយ + ប្រព័ន្ធត្រួតពិនិត្យស្វែងរកមួយ + ប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវមួយ + ប្រសិទ្ធភាពប្រតិបត្តិការនៃប្រព័ន្ធត្រួតពិនិត្យនីមួយៗនេះ

ប្រព័ន្ធត្រួតពិនិត្យខ្សោយ = តិចជាងកម្រិតប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា + ប្រតិបត្តិការប្រព័ន្ធត្រួតពិនិត្យមានចំណុចសង្ស័យ ឬអសង្គតិភាព។

៦. រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

រចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដែលមានលក្ខណៈគ្រប់ជ្រុងជ្រោយ ត្រូវដាក់ឱ្យអនុវត្តលើ បបព ។ ព្រមទាំងរចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងពេញលេញសម្រាប់ បបព ត្រូវមានលក្ខណៈដូចខាងក្រោម÷

- **ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅ:** ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅ អនុវត្តគ្រប់សមាសធាតុប្រព័ន្ធបច្ចេកវិទ្យា ដំណើរការ និងទិន្នន័យទាំងអស់របស់អង្គភាព ឬបរិស្ថានប្រព័ន្ធ។ ប្រព័ន្ធត្រួតពិនិត្យទូទៅរួមមាន ការគ្រប់គ្រងប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ការគ្រប់គ្រងហានិភ័យ ការគ្រប់គ្រងធនធាន ប្រតិបត្តិការប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ការអភិវឌ្ឍកម្មវិធី និងថែទាំ ការគ្រប់គ្រងសុវត្ថិភាពអ្នកប្រើប្រាស់ ឡូជីខល និងរូបវន្ត ការគ្រប់គ្រងការផ្លាស់ប្តូរ ការចម្លងទុក និងការស្តារឡើងវិញ និងនិរន្តភាពធុរកិច្ច។
- **ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច:** ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច សំដៅដល់កម្មវិធីកុំព្យូទ័រជាក់លាក់ ដែលរួមបញ្ចូលទាំងការគ្រប់គ្រងលើការបញ្ចូលប្រតិបត្តិការ ការដំណើរការ លទ្ធផល និងទិន្នន័យមេ។

៧. ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅ

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅដែលគ្រប់គ្រាន់ ត្រូវដាក់ឱ្យអនុវត្តដើម្បីគាំទ្រដល់ហេដ្ឋារចនាសម្ព័ន្ធ និងប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេចនៃ បបព ។ ប្រសិទ្ធភាពនៃការត្រួតពិនិត្យផ្ទៃក្នុងដែលផ្តល់ដោយ បបព អាស្រ័យមួយផ្នែកលើស្តង់ដារនៃការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យនៅក្នុងបរិស្ថានដែលកំពុងអនុវត្តនោះ។

បរិស្ថានប្រព័ន្ធត្រួតពិនិត្យទូទៅនៅក្នុងអង្គភាព បានបង្កើតមូលដ្ឋានគ្រឹះសម្រាប់ការត្រួតពិនិត្យផ្ទៃក្នុងប្រកបដោយប្រសិទ្ធភាព និងបានបង្កើតនូវ "ភាពម៉ឺងម៉ាត់" (Tone at the Top) និងតំណាងឱ្យចំណុចកំពូលនៃរចនាសម្ព័ន្ធអភិបាលកិច្ចអង្គភាព។

បបព ត្រូវគាំទ្រដោយប្រព័ន្ធត្រួតពិនិត្យនៅតាមផ្នែកនានា ដូចខាងក្រោម÷

៧.១. ស្តង់ដារបច្ចេកវិទ្យាព័ត៌មាន គោលនយោបាយ និងគោលការណ៍ណែនាំ

គោលបំណង: ដើម្បីផ្តល់ទិសដៅការគ្រប់គ្រង និងគាំទ្រប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានស្របតាមតម្រូវការធុរកិច្ច ច្បាប់ និងបទប្បញ្ញត្តិពាក់ព័ន្ធ។ អង្គភាពត្រូវកំណត់គោលដៅ និងគោលបំណង តាមរយៈផែនការយុទ្ធសាស្ត្រ និងស្តង់ដារបច្ចេកវិទ្យាព័ត៌មាន គោលនយោបាយ និងគោលការណ៍ណែនាំ។ បើគ្មានគោលនយោបាយ និងបទដ្ឋានសម្រាប់កំណត់ទិសដៅច្បាស់លាស់ទេ អង្គភាពអាចមានភាពមិនច្បាស់លាស់និងអនុវត្តមិនមានប្រសិទ្ធភាព។

ស្តង់ដារបច្ចេកវិទ្យាព័ត៌មាន គោលនយោបាយ និងគោលការណ៍ណែនាំទាំងនេះ គួរតែជាក្របខ័ណ្ឌដែលអាចជួយគាំទ្រដល់ប្រតិបត្តិការប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។ ក្របខ័ណ្ឌនេះត្រូវមានការត្រួតពិនិត្យជាប្រចាំឆ្នាំដោយគិតគូរពីការផ្លាស់ប្តូរផែនការធុរកិច្ចរបស់អង្គភាព និងបរិស្ថានបច្ចេកវិទ្យាព័ត៌មាន។

៧.២. រចនាសម្ព័ន្ធរបស់ស្ថាប័ន

គោលបំណង: បង្កើតក្របខ័ណ្ឌគ្រប់គ្រងដើម្បីផ្តួចផ្តើម និងត្រួតពិនិត្យការអនុវត្ត និងប្រតិបត្តិការប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និងសុវត្ថិភាពព័ត៌មាននៅក្នុងអង្គភាព ដែលគួរបញ្ចូលនៅចំណុចដូចខាងក្រោម÷

- កំណត់ និងរៀបចំរចនាសម្ព័ន្ធស្ថាប័ន
- បង្កើតតួនាទី និងការទទួលខុសត្រូវ (កំណត់ និងផ្សព្វផ្សាយតួនាទី និងការទទួលខុសត្រូវផ្នែកបច្ចេកវិទ្យាព័ត៌មាន រួមទាំងឋានានុក្រមនៃសិទ្ធិទទួលខុសត្រូវ និងគណនេយ្យភាព...)
- កំណត់ព័ត៌មាន (ទិន្នន័យ) និងម្ចាស់ប្រព័ន្ធ (គោលការណ៍ណែនាំចំណាត់ថ្នាក់ទិន្នន័យ សុវត្ថិភាពទិន្នន័យ និងគោលការណ៍ណែនាំលើការត្រួតពិនិត្យ និតិវិធីសុចរិតភាពទិន្នន័យ)
- ។ល។

៧.៣. ការគ្រប់គ្រងធនធានបច្ចេកវិទ្យាព័ត៌មាន (មនុស្ស ជំនាញ និងសមត្ថភាព)

គោលបំណង: កំណត់នូវជំនាញ និងសមត្ថភាពដែលត្រូវការដើម្បីសម្រេចបាននូវគោលបំណងពាក់ព័ន្ធ។ បុគ្គលិក និងអ្នកម៉ៅការត្រូវមានសមត្ថភាព ជំនាញ និងបទពិសោធន៍ដើម្បីបំពេញតួនាទី និងការទទួលខុសត្រូវរបស់ខ្លួន។ ទីប្រឹក្សា និងបុគ្គលិកកិច្ចសន្យា ដែលមានជំនាញបច្ចេកវិទ្យាព័ត៌មានត្រូវយល់ដឹង និងគោរពតាមគោលនយោបាយរបស់អង្គភាព និងបំពេញតាមតម្រូវការកិច្ចសន្យាដែលបានព្រមព្រៀង។ ផ្នែកខាងក្រោមនេះ ជាចំណុចគួរពិចារណា÷

- មុនពេលដំណើរការការងារ (ដំណើរការពិនិត្យ លក្ខន្តិក:ការងារ...)
- អំឡុងពេលធ្វើការ (និយោជិត និងអ្នកម៉ៅការយល់ពីតួនាទី/ការទទួលខុសត្រូវរបស់ខ្លួន អាចបន្តការរៀនសូត្រ និងមានឱកាសដើម្បីរក្សាចំណេះដឹង ជំនាញ និងគុណវុឌ្ឍរបស់ពួកគេ អាចទទួលបានការយល់ដឹងអំពីសុវត្ថិភាពព័ត៌មាន ការអប់រំ និងការបណ្តុះបណ្តាល និងដំណើរការវិន័យ...)
- ការបញ្ចប់ ឬការផ្លាស់ប្តូរការទទួលខុសត្រូវការងារ
- ។ល។

៧.៤. ការគ្រប់គ្រងអ្នកផ្គត់ផ្គង់ និងកិច្ចព្រមព្រៀងសេវាកម្ម

គោលបំណង: ផលិតផល និងសេវាកម្មប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានផ្តល់ជូនដោយអ្នកផ្គត់ផ្គង់គ្រប់ប្រភេទ ត្រូវបំពេញតាមតម្រូវការរបស់អង្គភាព និងកាត់បន្ថយហានិភ័យដែលអ្នកផ្គត់ផ្គង់មិនអាចអនុវត្ត ឬមិនគោរពតាមកិច្ចសន្យា ព្រមទាំងធានាតម្លៃប្រកួតប្រជែង។ កិច្ចព្រមព្រៀងកម្រិតសេវាកម្មត្រូវបំពេញតាមតម្រូវការ និងការរំពឹងទុករបស់អង្គភាពទាំងពេលបច្ចុប្បន្ន និងអនាគត។ ចំណុចខាងក្រោមនេះគួរពិចារណា÷

- កំណត់ និងវាយតម្លៃទំនាក់ទំនងអ្នកផ្គត់ផ្គង់ និងកិច្ចសន្យា
- ជ្រើសរើសអ្នកផ្គត់ផ្គង់
- ការគ្រប់គ្រងកិច្ចសន្យា (កំណត់អត្តសញ្ញាណ ការបញ្ជាក់ ការចរចា កម្រិតសេវាកម្ម ...)
- ត្រួតពិនិត្យកិច្ចព្រមព្រៀងសេវាកម្ម និងកិច្ចសន្យា
- គ្រប់គ្រងហានិភ័យអ្នកផ្គត់ផ្គង់(ហានិភ័យទាក់ទងនឹងសមត្ថភាពរបស់អ្នកផ្គត់ផ្គង់ក្នុងការបន្តផ្តល់សេវាកម្មប្រកបដោយសុវត្ថិភាព ប្រសិទ្ធភាព និងប្រសិទ្ធផល)
- តាមដានការអនុវត្តរបស់អ្នកផ្គត់ផ្គង់ដើម្បីធានាប្រសិទ្ធភាព និងអនុលោមភាព
- ។ល។

៧.៥. ការគ្រប់គ្រងហានិភ័យ

គោលបំណង: កំណត់អត្តសញ្ញាណ វាយតម្លៃ និងកាត់បន្ថយហានិភ័យប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានជាប្រចាំក្នុងកម្រិតទទួលយកបានដែលកំណត់ដោយអ្នកគ្រប់គ្រងអង្គភាព។ ចំណុចទាំងនេះ គួរតែរួមបញ្ចូល÷

- ប្រមូលទិន្នន័យពាក់ព័ន្ធដើម្បីកំណត់អត្តសញ្ញាណហានិភ័យ
- វិភាគហានិភ័យ
- ចងក្រងព័ត៌មានហានិភ័យ
- កំណត់ស្ថានភាពហានិភ័យ
- កំណត់ការគ្រប់គ្រងហានិភ័យ
- ឆ្លើយតបទៅនឹងហានិភ័យ។

៧.៦. ប្រព័ន្ធគ្រប់គ្រងសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន (បគសប)

គោលបំណង: កំណត់ដំណើរការ និងត្រួតពិនិត្យប្រព័ន្ធគ្រប់គ្រងសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន។ រក្សាផលប៉ះពាល់និងការកើតឡើងនៃឧប្បត្តិហេតុសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មានក្នុងកម្រិតនៃហានិភ័យអាចទទួលបានដោយអង្គភាព។ ខាងក្រោមនេះជាចំណុចគួរត្រូវបានពិចារណា÷

- បង្កើត និងថែរក្សា បគសប (កំណត់វិសាលភាពរបស់ បគសប តាមលក្ខណៈនៃអង្គភាព ទ្រព្យសម្បត្តិ និងបច្ចេកវិទ្យា...)
- កំណត់ និងគ្រប់គ្រងសុវត្ថិភាពបច្ចេកវិទ្យាពត៌មាន និងការដោះស្រាយហានិភ័យ
- តាមដាន និងត្រួតពិនិត្យ បគសប (ការពិនិត្យឡើងវិញជាប្រចាំអំពីប្រសិទ្ធភាព ចាត់ថ្នាក់ និងធ្វើអាទិភាពឧប្បត្តិហេតុសម្រាប់ការកែលំអ...)

សេចក្តីណែនាំពាក់ព័ន្ធនឹងវិសាលភាពប្រព័ន្ធគ្រប់គ្រងសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (បគសប) គួរយោង ISO/IEC 27001:2013។

៧.៧. សុវត្ថិភាពទិន្នន័យ និងភាពអាចប្រើប្រាស់បាន

គោលបំណង: ធានានូវសុចរិតភាព និងភាពស៊ីសង្វាក់គ្នានៃទិន្នន័យទាំងអស់ដែលត្រូវបានរក្សាទុកជាទម្រង់អេឡិចត្រូនិក ដូចជាមូលដ្ឋានទិន្នន័យ ឃ្លាំងទិន្នន័យ និងបណ្ណសារទិន្នន័យ ព្រមទាំងដើម្បីសម្រេចបាន និងទ្រទ្រង់ការគ្រប់គ្រងប្រកបដោយប្រសិទ្ធភាពលើការរៀបចំទ្រព្យសម្បត្តិទិន្នន័យ តាមវដ្តទិន្នន័យចាប់តាំងពីការបង្កើតរហូតដល់ការចែកចាយ ការថែរក្សា និងការរក្សាទុកបណ្ណសារ។ ចំណុចខាងក្រោមនេះ គួរត្រូវពិចារណា÷

- កំណត់ និងផ្សព្វផ្សាយយុទ្ធសាស្ត្រគ្រប់គ្រងទិន្នន័យ/ចំណាត់ថ្នាក់ទិន្នន័យ តួនាទី និងការទទួលខុសត្រូវរបស់អង្គភាព
- ព័ត៌មានវេទយិតភាពដូចជាឯកសារប្រព័ន្ធ កូដរបស់កម្មវិធីស្រេច និងទិន្នន័យប្រតិបត្តិការផលិតកម្មគួរតែមានប្រព័ន្ធត្រួតពិនិត្យរឹងមាំជាងមុន ដើម្បីការពារការផ្លាស់ប្តូរគ្មានការអនុញ្ញាត (ឧ.ការត្រួតពិនិត្យសុចរិតភាព គ្រីបតូក្រាហ្វិច...)

- កំណត់ការរក្សាទុកបណ្ណសារ ការកាត់ទុក ការគ្រប់គ្រងឧបករណ៍ចម្លងទុក ការជម្រះ និងការបញ្ជូនទិន្នន័យ
- គ្រប់គ្រងលើការចម្លងទុកទិន្នន័យ និងរៀបចំការស្តារឡើងវិញ
- គ្រប់គ្រងលទ្ធភាពអាចប្រើប្រាស់បានរបស់ទិន្នន័យសំខាន់ៗ ដើម្បីធានាបាននូវនិរន្តរភាពប្រតិបត្តិការ
- ។ល។

៧.៨. ការទិញ ការអភិវឌ្ឍ និងការថែរក្សាប្រព័ន្ធ

ការអភិវឌ្ឍគម្រោង និងការគ្រប់គ្រងសេវាកម្មព័ត៌មាន គឺចាំបាច់សម្រាប់ការគាំទ្រដល់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន សេវាកម្ម និងប្រតិបត្តិការ ការគ្រប់គ្រងការផ្លាស់ប្តូរ ឧប្បត្តិហេតុក៏ដូចជាធានាស្ថិរភាពបរិស្ថានប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។ ដើម្បីសម្រេចបាននូវប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានមាំមួន អង្គភាពគួរតែមានផែនការត្រឹមត្រូវលើការអនុវត្ត ការផ្ទេរ ឬបំប្លែងប្រព័ន្ធ និងទិន្នន័យ ការធ្វើតេស្តទទួលយក ការទំនាក់ទំនង ការរៀបចំមុនដាក់អនុវត្ត ការដាក់អនុវត្តផលិតកម្មនៃដំណើរការធុរកិច្ចថ្មី ឬការផ្លាស់ប្តូរ និងសេវាកម្មប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ការគាំទ្រផលិតកម្មពីដើម និងការត្រួតពិនិត្យឡើងវិញក្រោយការអនុវត្ត។ វដ្តនៃការអភិវឌ្ឍប្រព័ន្ធ រួមមាន÷

ក. ការសិក្សាសមិទ្ធិលទ្ធភាព

គោលបំណង: កំណត់អត្ថប្រយោជន៍នៃការអភិវឌ្ឍប្រព័ន្ធទាំងការបង្កើនផលិតភាព ឬការចៀសវាងការចំណាយនាពេលអនាគត កំណត់ និងគណនាតម្លៃសន្សំបាននៃប្រព័ន្ធថ្មី។ សកម្មភាពការសិក្សាសមិទ្ធិលទ្ធភាពមានដូចខាងក្រោម÷

- កំណត់ពេលវេលាសម្រាប់អនុវត្តដំណោះស្រាយដែលត្រូវការ
- កំណត់ដំណោះស្រាយឧត្តមានុពលផ្សេងទៀតដោយផ្អែកលើហានិភ័យ សម្រាប់បំពេញតម្រូវការធុរកិច្ច និងការទាមទារធនធានព័ត៌មានទូទៅ (ឧ. គួរត្រូវអភិវឌ្ឍ ឬទិញប្រព័ន្ធ)
- ចូលរួមពីអ្នកប្រើប្រាស់លើការពិនិត្យលើជម្រើសដែលរួមមានតម្លៃ និងអត្ថប្រយោជន៍ ការវិភាគហានិភ័យ និងការអនុម័តលើតម្រូវការ និងដំណោះស្រាយដែលបានស្នើ
- សិក្សាសមិទ្ធិលទ្ធភាព និងបង្កើតដំណោះស្រាយជំនួសផ្សេងៗ
- កំណត់ថាតើដំណោះស្រាយសមស្របជាមួយយុទ្ធសាស្ត្រធុរកិច្ចដែរឬទេ
- ។ល។

ខ. តម្រូវការ

គោលបំណង: កំណត់ដំណោះស្រាយ និងវិភាគតម្រូវការមុនពេលទិញ ឬបង្កើត ដើម្បីធានាថាស្របតាមតម្រូវការយុទ្ធសាស្ត្ររបស់អង្គភាពពាក់ព័ន្ធនិងដំណើរការធុរកិច្ច កម្មវិធីស្រេច ព័ត៌មាន/ទិន្នន័យ ហេដ្ឋារចនាសម្ព័ន្ធ និងសេវាកម្ម។ ការគិតគូពីតម្រូវការ គួរបញ្ចូលនៅសកម្មភាពខាងក្រោម÷

- កំណត់អត្តសញ្ញាណ និងពិគ្រោះជាមួយភាគីពាក់ព័ន្ធដើម្បីកំណត់ពីតម្រូវការរបស់អ្នកប្រើប្រាស់
- កំណត់ និងរក្សាមុខងារធុរកិច្ច និងតម្រូវការបច្ចេកទេស
- កំណត់ពីតម្រូវការសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាដែលពាក់ព័ន្ធ
- គ្រប់គ្រងហានិភ័យតម្រូវការ
- ទទួលបានការយល់ព្រមលើតម្រូវការ និងដំណោះស្រាយ
- ។ល។

គ. ការជ្រើសរើសប្រព័ន្ធ ការទិញ និងការតាក់តែង

គោលបំណង: ប្រព័ន្ធដែលបានជ្រើសរើសស្របតាមការរំពឹងទុក និងតម្រូវការដែលបានកំណត់។ ធានាឱ្យការបង្កើត និងការថែរក្សាផលិតផល និងសេវាកម្មដែលបានកំណត់ (បច្ចេកវិទ្យា ដំណើរការធុរកិច្ច និងលំហូរការងារ) ស្របតាមតម្រូវការរបស់អង្គភាពដែលរួមមាន ការតាក់តែង ការអភិវឌ្ឍ លទ្ធកម្ម/ការផ្គត់ផ្គង់ និងការសហការជាមួយអ្នកផ្គត់ផ្គង់។ ការជ្រើសរើសប្រព័ន្ធ គួរពិចារណាលើសកម្មភាពដូចខាងក្រោម÷

ប្រព័ន្ធដែលទិញពីអ្នកផ្គត់ផ្គង់:

- រៀបចំផែនការទិញដោយផ្អែកលើតម្រូវការ និងការតាក់តែងលម្អិត
- រៀបចំសំណើសុំស្តីពីតម្រូវការរបស់អង្គភាពដើម្បីដាក់ដេញថ្លៃ
- អនុវត្តនីតិវិធីលទ្ធកម្ម និងកិច្ចសន្យា ទទួលបានការធានាគុណភាព និងការយល់ព្រម
- ។ល។

ការអភិវឌ្ឍដោយអង្គភាពផ្ទាល់:

- បង្កើត និងប្រមូលផ្តុំការតាក់តែងឯកសារសម្រាប់ឆ្លើយតបនឹងដំណោះស្រាយដែលបានកំណត់ (ឧ. ដំណើរការធុរកិច្ច លំហូរការងារ កម្មវិធីស្រេច ហេដ្ឋារចនាសម្ព័ន្ធ ...)
- ចងក្រងលំហូរការងារប្រព័ន្ធ និងបង្ហាញទំនាក់ទំនងដែលព័ត៌មាននឹងត្រូវដំណើរការនៅក្នុងប្រព័ន្ធ
- ពិពណ៌នាអំពីធាតុចូល និងធាតុចេញ ដូចជាច្រកចូលប្រព័ន្ធ របាយការណ៍...
- បង្កើតផែនការផ្ទេរ ឬបម្លែងទិន្នន័យពីប្រព័ន្ធចាស់ទៅប្រព័ន្ធថ្មី
- រៀបចំផែនការធ្វើតេស្តទៅតាមកម្រិតនីមួយៗ: តេស្តតាមផ្នែក (កម្មវិធី) អនុប្រព័ន្ធ (ម៉ូឌុល) សមាហរណកម្ម (ប្រព័ន្ធ) សន្ធានកម្ម ស្ត្រេសតេស្ត តេស្តសុវត្ថិភាព តេស្តលើការចម្លងទុក និងការស្តារឡើងវិញ
- ។ល។

ឃ. ការរៀបតម្រូវ/ការអភិវឌ្ឍ

គោលបំណង: តាក់តែង បង្កើត និងអនុវត្តនូវវិធីសាស្ត្រអភិវឌ្ឍន៍ប្រព័ន្ធ ស្របតាមយុទ្ធសាស្ត្រ និងតម្រូវការរួម (ឧ. ម៉ូដែលតាមដំណាក់ ម៉ូដែលអាជែល...)។

ប្រព័ន្ធដែលទិញពីអ្នកផ្គត់ផ្គង់:

- តម្លើង និងរៀបតម្រូវស្របជាមួយសកម្មភាពដំណើរការធុរកិច្ច
- អំឡុងពេលរៀបតម្រូវ និងសមាហរណកម្មផ្នែករឹងនិងហេដ្ឋារចនាសម្ព័ន្ធផ្នែកទន់ ត្រូវមានប្រព័ន្ធត្រួត-ពិនិត្យ សុវត្ថិភាព ឯកជនភាព និងអាចធ្វើសវនកម្មបាន ដើម្បីការពារធនធាន និងធានាលើការសម្ងាត់ ភាពអាចប្រើប្រាស់បាន និងសុចរិតភាពនៃទិន្នន័យ
- រៀបចំដំណើរការគ្រប់គ្រងការផ្លាស់ប្តូរ ដើម្បីធានាថាការផ្លាស់ប្តូរក្នុងប្រព័ន្ធផលិតកម្មត្រូវបានវាយតម្លៃ អនុម័ត អនុវត្ត និងត្រួតពិនិត្យត្រឹមត្រូវ
- ។ល។

ប្រព័ន្ធដែលអភិវឌ្ឍដោយអង្គភាពផ្ទាល់:

- ចាប់ផ្តើមសរសេរកម្មវិធីដោយប្រើប្រាស់នូវលក្ខណៈជាក់លាក់ដែលបានកំណត់
- កំណត់ និងបង្កើតបរិស្ថានដែលមានសុវត្ថិភាពសម្រាប់ធ្វើតេស្ត អភិវឌ្ឍ និងផលិតកម្ម
- ធ្វើតេស្តកម្រិតផ្សេងៗ ដូចជាការធ្វើតេស្តតាមផ្នែក ការធ្វើតេស្តប្រព័ន្ធ និងការធ្វើតេស្តលើការទទួលយករបស់អ្នកប្រើប្រាស់ ក៏ត្រូវបានអនុវត្តដើម្បីផ្ទៀងផ្ទាត់ និងបញ្ជាក់នូវអ្វីដែលបានបង្កើតឡើង។
- ។ល។

ង. ការធ្វើតេស្តចុងក្រោយ និងការដាក់អនុវត្ត

គោលបំណង: គ្រប់គ្រងការរចនា រៀបចំនិងធ្វើតេស្ត គ្រប់គ្រងតម្រូវការ និងថែរក្សាដំណើរការធុរកិច្ច កម្មវិធីស្រេច ព័ត៌មាន ទិន្នន័យ ហេដ្ឋារចនាសម្ព័ន្ធ និងសេវាកម្ម។

- ធ្វើតេស្តស្របតាមផែនការដែលបានកំណត់ មុនពេលផ្ទេរទៅបរិស្ថានផលិតកម្ម
- បញ្ជូលម្ចាស់ដំណើរការ ឬអ្នកប្រើប្រាស់ពាក់ព័ន្ធក្នុងក្រុមការងារធ្វើតេស្ត ហើយរាល់បញ្ហាឬកំហុសដែលរកឃើញក្នុងអំឡុងពេលធ្វើតេស្ត ត្រូវកត់ត្រានិងចាត់តាមអាទិភាពដើម្បីដោះស្រាយ
- ទទួលបាននូវការអនុម័តលើផែនការដាក់ឱ្យដំណើរការជាផ្លូវការ
- បន្តអនុវត្តប្រព័ន្ធចាស់ដំណាលគ្នាជាមួយប្រព័ន្ធថ្មីក្នុងរយៈពេលកំណត់មួយ ដើម្បីប្រៀបធៀបដំណើរការនិងលទ្ធផល។ ក្នុងករណីដែលប្រព័ន្ធថ្មីមានបញ្ហាធ្ងន់ធ្ងរ ត្រលប់ទៅដំណើរការប្រព័ន្ធចាស់វិញ ដោយផ្អែកតាមផែនការបម្រុងទុក
- ។ល។

ច. ការពិនិត្យឡើងវិញក្រោយការដាក់អនុវត្ត

គោលបំណង: ពិនិត្យ និងវាយតម្លៃលើលទ្ធផលនៃការអនុវត្តជាក់ស្តែង ធៀបនឹងការរំពឹងទុករបស់អ្នកប្រើប្រាស់ ព្រមទាំងរៀបចំផែនការសកម្មភាពផ្អែកតាមបទពិសោធន៍ទទួលបាន សម្រាប់អភិវឌ្ឍន៍ប្រព័ន្ធផ្សេងៗ។

៧.៩. ការគ្រប់គ្រងលទ្ធភាពប្រើប្រាស់បាន និងសមត្ថភាព

គោលបំណង: ធ្វើឱ្យមានគុណភាពនៃតម្រូវការលើភាពអាចប្រើប្រាស់បាន ដំណើរការ និងសមត្ថភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានទាំងពេលបច្ចុប្បន្ន និងអនាគត ប្រកបដោយភាពសមនឹងតម្លៃ ដូចជារក្សានូវភាពអាចប្រើប្រាស់បាននៃសេវាកម្ម ការគ្រប់គ្រងធនធានប្រកបដោយប្រសិទ្ធភាព និងការធ្វើឱ្យប្រសើរឡើងនូវដំណើរការប្រព័ន្ធ។ ខាងក្រោមនេះជាចំណុចគួរពិចារណា÷

- ការវាយតម្លៃលើសមត្ថភាពបច្ចុប្បន្ន ការព្យាករណ៍អំពីតម្រូវការនាពេលអនាគត ការវិភាគផលប៉ះពាល់ធុរកិច្ច និងការវាយតម្លៃហានិភ័យដើម្បីរៀបចំផែនការ និងអនុវត្ត
- ការរៀបចំផែនការសម្រាប់ការផ្លាស់ប្តូរតម្រូវការធុរកិច្ចដោយផ្តល់អាទិភាពតាមកម្រិតផលប៉ះពាល់លើភាពអាចប្រើប្រាស់បាន ដំណើរការ និងសមត្ថភាព
- ត្រួតពិនិត្យ វាស់វែង វិភាគ រៀបចំរបាយការណ៍ និងពិនិត្យភាពអាចប្រើប្រាស់បាន ដំណើរការ និងសមត្ថភាព
- ស៊ើបអង្កេត និងដោះស្រាយបញ្ហាទាក់ទងភាពអាចប្រើប្រាស់បាន ដំណើរការ និងសមត្ថភាព
- ។ល។

៧.១០. ការគ្រប់គ្រងលើការផ្លាស់ប្តូរប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

គោលបំណង: រាល់ការផ្លាស់ប្តូរជាធម្មតា និងបន្ទាន់នៃដំណើរការធុរកិច្ច កម្មវិធីស្រេច និងហេដ្ឋារចនាសម្ព័ន្ធ ត្រូវមានការគ្រប់គ្រង និងប្រព័ន្ធត្រួតពិនិត្យត្រឹមត្រូវ ដើម្បីផ្តល់នូវភាពរហ័ស និងអាចជឿទុកចិត្តបាន។ ខាងក្រោមនេះជាចំណុចគួរពិចារណា÷

- គោលនយោបាយ និងនីតិវិធីគ្រប់គ្រងការផ្លាស់ប្តូរ
- វាយតម្លៃផលប៉ះពាល់នៃការផ្លាស់ប្តូរ ការផ្តល់អាទិភាព និងការអនុញ្ញាតលើការផ្លាស់ប្តូរ
- ធានាថារាល់ការផ្លាស់ប្តូរទាំងអស់ត្រូវបានកត់ត្រាទុក វាយតម្លៃ កំណត់អាទិភាព ចាត់ថ្នាក់ប្រភេទការផ្លាស់ប្តូរ និងកំណត់កាលវិភាគផ្លាស់ប្តូរ
- គ្រប់គ្រងលើការផ្លាស់ប្តូរបន្ទាន់ ដើម្បីកាត់បន្ថយឧប្បត្តិហេតុ បន្ទាប់មកវាយតម្លៃ និងអនុម័តរាល់ការផ្លាស់ប្តូរដែលបានអនុវត្តរួច
- កត់ត្រា និងតាមដានរាល់ការផ្លាស់ប្តូរដែលមិនបានអនុម័ត បានអនុម័ត កំពុងដំណើរការ និងបានផ្លាស់ប្តូររួច ព្រមទាំងរាយការណ៍អំពីស្ថានភាពនៃការផ្លាស់ប្តូរទាំងនោះ

- ធ្វើបច្ចុប្បន្នភាពស្ថានភាពនៃការផ្លាស់ប្តូរ ចងក្រងឯកសារ និងនីតិវិធីអ្នកប្រើប្រាស់បន្ទាប់ពីបានផ្លាស់ប្តូររួច
- ។ល។

៧.១១. ការយល់ដឹង និងការបណ្តុះបណ្តាលដល់អ្នកប្រើប្រាស់

គោលបំណង: បុគ្គលិកទាំងអស់របស់អង្គភាព និងអ្នកពាក់ព័ន្ធ គួរតែទទួលបានការអប់រំ និងការបណ្តុះបណ្តាលគ្រប់គ្រាន់សមស្របជាប្រចាំលើគោលនយោបាយ និងនីតិវិធីពាក់ព័ន្ធនឹងមុខងារភារកិច្ចរបស់ខ្លួន ព្រមទាំងលើសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ការគំរាមកំហែង ភាពងាយរងគ្រោះ ឬក្របខ័ណ្ឌសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់អង្គភាព។ ខាងក្រោមនេះជាចំណុចគួរពិចារណា÷

- ការបណ្តុះបណ្តាលអំពីគោលនយោបាយ នីតិវិធី ដំណើរការ និងសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន
- ការធ្វើតេស្តលើការយល់ដឹងអំពីសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន (ឧ. ហ្វីស៊ីង...)
- ការរក្សាកំណត់ត្រានៃការបណ្តុះបណ្តាល ជំនាញ បទពិសោធន៍ និងគុណវុឌ្ឍន៍
- ។ល។

៧.១២. វដ្តនៃទ្រព្យសកម្មព័ត៌មាន

គោលបំណង: គ្រប់គ្រងទ្រព្យសកម្មព័ត៌មាន របស់អង្គភាព ដើម្បីប្រាកដថាការប្រើប្រាស់ទ្រព្យសកម្មព័ត៌មានផ្តល់នូវតម្លៃដ៏ប្រសើរ ភាពអាចដំណើរការ (ស្របតាមគោលបំណង) និងថែរក្សាការពារដោយការទទួលខុសត្រូវ។ សុវត្ថិភាពព័ត៌មានចាំបាច់ត្រូវបានពិចារណានៅគ្រប់ដំណាក់កាលនៃវដ្តទ្រព្យសម្បត្តិព័ត៌មានដូចជាការធ្វើផែនការ ការតាក់តែង ការទិញ ការចាត់ចំណាត់ថ្នាក់ ការអនុវត្ត ការថែរក្សាការពារ និងការជម្រះ។ ខាងក្រោមនេះជាចំណុចគួរពិចារណា÷

- កំណត់ និងកត់ត្រាទ្រព្យសកម្មព័ត៌មានទាំងអស់ (បញ្ជីរសារពើភ័ណ្ឌទ្រព្យសកម្មព័ត៌មាន) ដូចជាអត្តសញ្ញាណ/យថាប្រភេទច្បាស់លាស់ តម្លៃធៀប ទីតាំង សុវត្ថិភាព/ចំណាត់ថ្នាក់ហានិភ័យ ម្ចាស់ និងអ្នកថែទាំ
- គ្រប់គ្រងវដ្តទ្រព្យសកម្មចាប់ពីការធ្វើលទ្ធកម្មរហូតដល់ការជម្រះ
- ពិនិត្យឡើងវិញជាប្រចាំលើទ្រព្យសម្បត្តិដែលមាន ដើម្បីកំណត់វិធីធ្វើឱ្យកាន់តែមានប្រសិទ្ធភាពស្របតាមតម្រូវការធុរកិច្ច
- គ្រប់គ្រងអាជ្ញាប័ណ្ណកម្មវិធីដើម្បីរក្សាបានចំនួនអាជ្ញាប័ណ្ណសម្រាប់គាំទ្រតម្រូវការធុរកិច្ច
- ។ល។

៧.១៣. ការគ្រប់គ្រងប្រតិបត្តិការប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

គោលបំណង: សម្របសម្រួល និងអនុវត្តសកម្មភាព និងនីតិវិធីប្រតិបត្តិចាំបាច់ សម្រាប់ដំណើរការសេវាកម្មបច្ចេកវិទ្យាព័ត៌មានទាំងប្រភពខាងក្នុងនិងខាងក្រៅ ដូចជាការអនុវត្តនីតិវិធីប្រតិបត្តិស្តង់ដារបានកំណត់ និងសកម្មភាព

តាមដាននានា ការផ្គត់ផ្គង់ផលិតផល និងសេវាកម្មប្រតិបត្តិការបច្ចេកវិទ្យាព័ត៌មានតាមការគ្រោងទុក។ ខាងក្រោមនេះជាចំណុចគួរពិចារណា÷

- រក្សាទុក និងអនុវត្តនីតិវិធីប្រតិបត្តិ ព្រមទាំងអនុវត្តកិច្ចការប្រកបដោយភាពជឿជាក់ និងសង្គតិភាព
- គ្រប់គ្រងការផ្តល់សេវាកម្មបច្ចេកវិទ្យាព័ត៌មានពីប្រភពខាងក្រៅ ដើម្បីធានាភាពជឿជាក់បាន និងការពារព័ត៌មាន
- ត្រួតពិនិត្យហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និងព្រឹត្តិការណ៍ពាក់ព័ន្ធ (ឧ.កំណត់ហេតុ គន្លងសវនកម្ម...)
- គ្រប់គ្រងវិធានការដើម្បីទប់ស្កាត់ផលប៉ះពាល់ដែលបណ្តាលមកពីបរិស្ថានជុំវិញ (ឧ.ដំឡើងឧបករណ៍ដើម្បីតាមដាន និងត្រួតពិនិត្យបរិស្ថាន)
- គ្រប់គ្រងគ្រឿងបរិក្ខារ ឧបករណ៍ទំនាក់ទំនង រួមទាំងថាមពលអគ្គិសនី (ឧ.ឧបករណ៍ផ្គុកថាមពលអគ្គិសនីម៉ាស៊ីនភ្លើង) ស្របតាមគោលការណ៍ណែនាំ តម្រូវការបច្ចេកទេស ធុរកិច្ច លក្ខណៈបច្ចេកទេសអ្នកផ្គត់ផ្គង់ គោលការណ៍សុវត្ថិភាព និងសុខភាពជាដើម។

៧.១៤. ការគ្រប់គ្រងលើសំណើសុំសេវាកម្ម

គោលបំណង: ឆ្លើយតបទាន់ពេលវេលា និងមានប្រសិទ្ធភាពចំពោះសំណូមពរអ្នកប្រើប្រាស់ និងផ្តល់ការដោះស្រាយរាល់ការស្នើសុំគ្រប់ប្រភេទដូចជា ការផ្តល់សេវាកម្មឡើងវិញជាធម្មតា ការស៊ើបអង្កេត ការវិនិច្ឆ័យ ការបញ្ជូនបន្ត ការដោះស្រាយ និងការបំពេញតាមសំណើរបស់អ្នកប្រើប្រាស់ ព្រមទាំងមានការកត់ត្រាត្រឹមត្រូវ។ ខាងក្រោមនេះជាចំណុចគួរពិចារណា÷

- កំណត់ចំណាត់ថ្នាក់សំណើសេវាកម្មទៅតាមប្រភេទ
- កត់ត្រា ចាត់ថ្នាក់ និងផ្តល់អាទិភាពដល់សំណើ
- ផ្ទៀងផ្ទាត់ អនុម័ត និងបំពេញតាមការស្នើសុំសេវាកម្ម
- ស៊ើបអង្កេត វិនិច្ឆ័យ និងបែងចែកឧប្បត្តិហេតុ (កំណត់អត្តសញ្ញាណ កត់ត្រាឧប្បត្តិហេតុ កំណត់មូលហេតុ និងរកដំណោះស្រាយសមស្រប)
- ដោះស្រាយ និងសង្គ្រោះពីឧប្បត្តិហេតុ (ចងក្រងជាឯកសារនូវការអនុវត្ត និងតេស្តលើដំណោះស្រាយ)
- ធ្វើការស្តារសេវាកម្មបច្ចេកវិទ្យាព័ត៌មានឡើងវិញ
- បិទសំណើសុំសេវាកម្ម (ផ្ទៀងផ្ទាត់ភាពពេញចិត្តនៃការដោះស្រាយឧប្បត្តិហេតុ/ឬការបំពេញតាមសំណើ និងបិទបញ្ចប់)
- តាមដានស្ថានភាព និងរៀបចំរបាយការណ៍ (តាមដាន វិភាគ និងរាយការណ៍ជាទៀងទាត់នូវសំណើដែលបានបំពេញ)
- ។ល។

៧.១៥. ការគ្រប់គ្រងឧប្បត្តិហេតុ

គោលបំណង: ឆ្លើយតបទាន់ពេលវេលា និងមានប្រសិទ្ធភាពចំពោះឧប្បត្តិហេតុប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានដូចជា ការប្រើប្រាស់ទ្រព្យសកម្មព័ត៌មាន ដោយមិនត្រឹមត្រូវ ការបង្ហាញព័ត៌មាន ឬព្រឹត្តិការណ៍ដែលគំរាមកំហែងដល់ដំណើរការធុរកិច្ច។

ជាទូទៅប្រភេទឧប្បត្តិហេតុអាចមានដូចជា ការដាច់ឬយឺតនៃសេវាកម្មបណ្តាលមកពីបញ្ហាសមត្ថភាពផ្នែករឹងនិងផ្នែកទន់ ការចូលប្រើប្រព័ន្ធដោយគ្មានការអនុញ្ញាត ការលួចអត្តសញ្ញាណ ការបែកធ្លាយ ឬការបាត់បង់ទិន្នន័យ កម្មវិធីដែលមានគ្រោះថ្នាក់ ការចម្លងទុកមិនសម្រេច ការវាយប្រហារលើប្រព័ន្ធ និងបញ្ហាសុចរិតភាពទិន្នន័យ។ ខាងក្រោមនេះជាចំណុចគួរពិចារណា÷

- បង្កើត និងអនុវត្តដំណើរការការពារ ស្វែងរក វិភាគ និងឆ្លើយតបទៅនឹងឧប្បត្តិហេតុបច្ចេកវិទ្យាព័ត៌មាន
- បង្កើតដំណើរការបញ្ជូនបន្ត និងទំនាក់ទំនងទៅតាមកម្រិតនៃការទទួលខុសត្រូវ
- រៀបចំផែនការឆ្លើយតប និងកត់ត្រាឧប្បត្តិហេតុប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន
- ចាត់ថ្នាក់ឧប្បត្តិហេតុប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានតាមកម្រិតធ្ងន់ធ្ងរផ្អែកលើផលប៉ះពាល់ធុរកិច្ច និងភាពបន្ទាន់
- រៀបចំក្រុមការងារ និងបណ្តុះបណ្តាល ដើម្បីអាចឆ្លើយតបទៅនឹងឧប្បត្តិហេតុប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន
- ធ្វើតេស្ត និងកែលម្អផែនការឆ្លើយតបទៅនឹងឧប្បត្តិហេតុប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន
- ។ល។

៧.១៦. ការគ្រប់គ្រងនិរន្តរភាពបច្ចេកវិទ្យាព័ត៌មាន

គោលបំណង: បង្កើត និងថែរក្សាផែនការនិរន្តរភាពបច្ចេកវិទ្យាព័ត៌មានដើម្បីឱ្យអង្គភាពអាចឆ្លើយតបទៅនឹងឧប្បត្តិហេតុ ឬគ្រោះមហន្តរាយ និងដោះស្រាយបានឆាប់រហ័សចំពោះការរំខាន ក៍ដូចជាដើម្បីឱ្យមាននិរន្តរភាពដំណើរការប្រតិបត្តិការធុរកិច្ច និងសេវាកម្មបច្ចេកវិទ្យាព័ត៌មានសំខាន់ៗ ព្រមទាំងរក្សាភាពអាចប្រើប្រាស់បាននៃធនធាន និងទ្រព្យសកម្មព័ត៌មាន ក្នុងកម្រិតអាចទទួលយកបាន។ ខាងក្រោមនេះជាចំណុចគួរពិចារណា÷

- រៀបចំគោលនយោបាយនិរន្តរភាពធុរកិច្ច
- បង្កើត និងអនុវត្តសាកល្បងផែនការនិរន្តរភាពធុរកិច្ច និងផែនការស្តារពីគ្រោះមហន្តរាយ
- ត្រួតពិនិត្យឡើងវិញ និងកែលម្អផែនការនិរន្តរភាពធុរកិច្ច ដើម្បីធានាបាននូវភាពសមស្រប ភាពគ្រប់គ្រាន់និងប្រសិទ្ធភាព
- បណ្តុះបណ្តាលអំពីនីតិវិធី ភារកិច្ច និងការទទួលខុសត្រូវដើម្បីឆ្លើយតបទៅនឹងគ្រោះមហន្តរាយ
- រៀបចំការគ្រប់គ្រងលើការចម្លងទុក

- ពិនិត្យឡើងវិញលើផែនការនិរន្តរភាពធុរកិច្ច និងផែនការស្តារពីគ្រោះមហន្តរាយបន្ទាប់ពីផែនការនោះត្រូវបានយកទៅអនុវត្តនៅពេលមានការរំខាន
- ។ល។

៧.១៧. គ្រប់គ្រងសុវត្ថិភាពសេវាកម្ម

គោលបំណង: កាត់បន្ថយផលប៉ះពាល់ពីភាពងាយរងគ្រោះ និងឧប្បត្តិហេតុសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន។ ការពារព័ត៌មានរបស់អង្គភាពក្នុងកម្រិតហានិភ័យដែលអាចទទួលយកបាន ស្របតាមគោលនយោបាយសុវត្ថិភាពបច្ចេក-វិទ្យាព័ត៌មាន។ ខាងក្រោមនេះជាចំណុចគួរពិចារណា÷

- អនុវត្ត និងថែរក្សាវិធានការបង្ការ ស្វែងរក និងកែតម្រូវ នៅទូទាំងអង្គភាព ដើម្បីការពារប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានដូចជាធ្វើបច្ចុប្បន្នភាពកម្មវិធីសុវត្ថិភាពប្រព័ន្ធប្រតិបត្តិការ កម្មវិធីកំចាត់មេរោគ ឬកម្មវិធីអាក្រក់ផ្សេងៗ
- គ្រប់គ្រងសុវត្ថិភាពបណ្តាញ និងការតភ្ជាប់
- គ្រប់គ្រងសុវត្ថិភាពឧបករណ៍ប្រើប្រាស់ចុងក្រោយ (ឧ.កុំព្យូទ័រ ម៉ាស៊ីនមេ ទូរស័ព្ទ និងឧបករណ៍បណ្តាញឬផ្នែកទន់) ដើម្បីធានាសុវត្ថិភាពព័ត៌មានដែលបានដំណើរការ រក្សាទុក ឬបញ្ជូនស្របតាមការកំណត់ក្នុងគោលនយោបាយសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន
- គ្រប់គ្រងអត្តសញ្ញាណអ្នកប្រើប្រាស់ និងការគ្រប់គ្រងការចូលប្រើប្រាស់
- គ្រប់គ្រងការចូលប្រើប្រាស់រូបវន្តលើទ្រព្យសកម្មព័ត៌មាន
- គ្រប់គ្រងភាពងាយរងគ្រោះ និងត្រួតពិនិត្យហេដ្ឋារចនាសម្ព័ន្ធពាក់ព័ន្ធសុវត្ថិភាព ដើម្បីធានាថាឧបករណ៍បច្ចេកវិទ្យា និងការស្វែងរក ត្រូវបានដាក់បញ្ចូលក្នុងការគ្រប់គ្រង និងតាមដានឧប្បត្តិហេតុ
- ។ល។

៨. ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ: កម្មវិធីស្រេចនីមួយៗ ត្រូវមានប្រព័ន្ធត្រួតពិនិត្យដែលរឹងមាំ និងគ្រប់គ្រាន់ ដើម្បីធានាថា÷

- រាល់ទិន្នន័យបានបញ្ចូលទាំងអស់គឺពេញលេញ សុក្រឹតភាព និងបានអនុញ្ញាតត្រឹមត្រូវ
- រាល់ទិន្នន័យបានដំណើរការតាមការរំពឹងទុក
- ទិន្នន័យដែលបានរក្សាទុកទាំងអស់ គឺត្រឹមត្រូវ និងសុក្រឹតភាព
- ធាតុចេញទាំងអស់ គឺត្រឹមត្រូវ និងពេញលេញ

- កំណត់ត្រាត្រូវបានរក្សាទុកដើម្បីតាមដានដំណើរការទិន្នន័យ ចាប់ពីការបញ្ចូល ការរក្សាទុក និងលទ្ធផលចុងក្រោយ
- ។ល។

ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេចត្រូវមាននៅតាមផ្នែកដូចខាងក្រោម÷

៨.១. ប្រព័ន្ធត្រួតពិនិត្យលើធាតុចូល

គោលបំណង: ដើម្បីធានាភាពពេញលេញ សុក្រឹតភាព និងការបានអនុញ្ញាតត្រឹមត្រូវនៃទិន្នន័យដែលបានបញ្ចូលក្នុងកម្មវិធីស្រេច។ ប្រព័ន្ធត្រួតពិនិត្យលើធាតុចូលរួមមាន÷

- ប្រព័ន្ធត្រួតពិនិត្យលើការចូលប្រើ:
  - ការអនុញ្ញាត: រាល់ការបង្កើតគណនី ពាក្យសម្ងាត់អ្នកប្រើប្រាស់ ការអនុញ្ញាត ការបែងចែកតួនាទី ឬការកំណត់សិទ្ធិ ត្រូវអនុលោមតាមគោលនយោបាយ និងនីតិវិធីរបស់អង្គភាព
  - ការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវ: គួរប្រើគណនីចូលប្រើប្រាស់ ពាក្យសម្ងាត់ លេខកូដផ្ទៀងផ្ទាត់ ហត្ថលេខាឌីជីថល ក្រយៅដៃ ...
- ភាពពេញលេញនៃការបញ្ចូលទិន្នន័យ: គួរមានការឆែកលើភាពសមហេតុផល និងកម្រិតកំណត់នៃតម្លៃ ហិរញ្ញវត្ថុ លើទម្រង់ និងប្រឡងចាំបាច់ លើលំដាប់ លើចន្លោះ លើចំនួនតួលេខ និងផ្ទៀងផ្ទាត់...
- ដំណើរការបញ្ចូលទិន្នន័យមិនទាន់រួចរាល់: គួរមានការត្រួតពិនិត្យលើប្រតិបត្តិការដែលមិនទាន់បញ្ចប់រួចរាល់
- ប្រព័ន្ធត្រួតពិនិត្យលើការអនុញ្ញាតដោយស្វ័យប្រវត្តិ អនុម័ត និងការបំពាន
- ប្រព័ន្ធត្រួតពិនិត្យលើការបែងចែកមុខងារដោយស្វ័យប្រវត្តិ និងសិទ្ធិចូលប្រើប្រាស់
- ។ល។

៨.២. ប្រព័ន្ធត្រួតពិនិត្យលើដំណើរការ

គោលបំណង: ដើម្បីធានាថាដំណើរការត្រូវបានបញ្ចប់ត្រឹមត្រូវ និងមានការអនុញ្ញាត។

ប្រព័ន្ធត្រួតពិនិត្យលើដំណើរការរួមមាន÷

- ការទាញទិន្នន័យ ការច្រោះ និងការទាញរបាយការណ៍
- តុល្យភាពរវាងសន្ធានកម្ម: ផ្ទៀងផ្ទាត់ដោយស្វ័យប្រវត្តិលើភាពដូចគ្នានៃទិន្នន័យប្រព័ន្ធដើមជាមួយប្រព័ន្ធគោលដៅ ករណីទិន្នន័យមិនដូចគ្នាគួរអាចទាញជារបាយការណ៍ដើម្បីត្រួតពិនិត្យបន្ថែម
- ការត្រួតពិនិត្យលើការស្ទួន: ផ្ទៀងផ្ទាត់ដោយស្វ័យប្រវត្តិលើភាពស្ទួនគ្នានៃប្រតិបត្តិការដែលបានកត់ត្រា
- ។ល។

៨.៣. ប្រព័ន្ធត្រួតពិនិត្យលើធាតុចេញ

គោលបំណង: ដើម្បីធានាថាធាតុចេញអាចទាញពីប្រព័ន្ធតាមតម្រូវការ ទាន់ពេលវេលា ត្រឹមត្រូវ អាចផ្ទៀងផ្ទាត់បានជាមួយទិន្នន័យដែលបានបញ្ចូល រក្សាការសម្ងាត់ ហើយរាល់កំហុស និងបញ្ហាត្រូវបានកត់ត្រាដោយប្រព័ន្ធព្រមទាំងមានការស៊ើបអង្កេត និងវិធានការដោះស្រាយត្រឹមត្រូវ។

៨.៤. ប្រព័ន្ធត្រួតពិនិត្យលើសុចរិតភាព

គោលបំណង: ដើម្បីធានាថាទិន្នន័យមេ និងទិន្នន័យនៃប្រតិបត្តិការកំពុងដំណើរការមានសង្គតិភាព និងសុចរិតភាព ហើយនៅមុនរាល់ការកែប្រែ ឬផ្លាស់ប្តូរត្រូវមានការអនុញ្ញាតត្រឹមត្រូវ។

៨.៥. ការគ្រប់គ្រងលើគន្លងសវនកម្ម

គោលបំណង: ដើម្បីអាចតាមដានខ្សែដំណើរការរបស់ប្រតិបត្តិការចាប់ពីដើមដំបូងដល់លទ្ធផលចុងក្រោយ ព្រមទាំងអាចផ្ទៀងផ្ទាត់ជាមួយអត្តសញ្ញាណប្រតិបត្តិការ និងព្រឹត្តិការណ៍។ ការគ្រប់គ្រងលើគន្លងសវនកម្មត្រូវពិចារណាចំណុចខាងក្រោម÷

- ត្រូវមានការតាមដានដោយស្វ័យប្រវត្តិលើការផ្លាស់ប្តូរ និងការបំពានដំណើរការទិន្នន័យ ដោយរំលេចអត្តសញ្ញាណអ្នកធ្វើការផ្លាស់ប្តូរ ឬបំពាន
- ត្រូវមានការគ្រប់គ្រងលើសុវត្ថិភាពគន្លងសវនកម្ម
- ។ល។

ផ្នែកទាំងអស់ខាងលើនេះ នឹងត្រូវមានការត្រួតពិនិត្យដោយសវនកម្មផ្ទៃក្នុងដើម្បីផ្តល់ការធានាដល់ថ្នាក់ដឹកនាំថាប្រព័ន្ធត្រួតពិនិត្យត្រូវបានតាក់តែងឡើង និងដំណើរការប្រកបដោយប្រសិទ្ធភាព ដោយផ្តល់នូវសក្តានុពលក្នុងការធ្វើឱ្យប្រសើរឡើងនូវប្រព័ន្ធគ្រប់គ្រងផ្ទៃក្នុងដែលមានស្រាប់ ក្នុងបំណងជំរុញអត្ថប្រយោជន៍នៃប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានឱ្យបានពេញលេញ។

៩. ប្រព័ន្ធត្រួតពិនិត្យដំណើរការធុរកិច្ចដោយឡែក

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ: រាល់ដំណើរការធុរកិច្ចទាំងអស់ដែលប្រតិបត្តិដោយ បបព ត្រូវមានប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងឱ្យបានគ្រប់គ្រាន់។

ដំណើរការធុរកិច្ច និងតម្រូវការប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងគន្លឹះមានដូចខាងក្រោម÷

៩.១. វដ្តសំណើចំណាយដល់ការទូទាត់

ដំណើរការនៃការស្នើសុំចំណាយរហូតដល់ការទូទាត់ រួមបញ្ចូលនូវសកម្មភាពទាក់ទងនឹងការស្នើសុំ ការធានាចំណាយ ការបញ្ជាទិញ ការទទួលទំនិញ ឬសេវាកម្ម និងការទូទាត់លើទំនិញ ឬសេវាកម្មជាមួយអ្នកផ្គត់ផ្គង់។ សកម្មភាពទាំងនេះរួមមាន÷

- ការកត់ត្រាឯកសារមេអំពីទំនិញ និងអ្នកផ្គត់ផ្គង់
- ដំណើរការស្នើសុំ ធានាចំណាយ និងបញ្ជាទិញ
- ដំណើរការទទួលទំនិញ ឬសេវាកម្ម និងផ្ទៀងផ្ទាត់
- ការកត់ត្រាវិក្កយបត្រ និងការផ្គូផ្គង
- ដំណើរការទូទាត់ និងចេញលិខិតប្រកាសឥណទាន
- ការធ្វើបច្ចុប្បន្នភាពសៀវភៅធំ និងសៀវភៅធំរង។

ប្រព័ន្ធត្រួតពិនិត្យដែលត្រូវយកចិត្តទុកដាក់នៅក្នុងផ្នែកនេះមាន÷

ទីត្រួតពិនិត្យគន្លឹះ	ប្រព័ន្ធត្រួតពិនិត្យរៀបតម្រូវ
ចម្ងងការទិញ	វិធីសាស្ត្រផ្ទៀងផ្ទាត់: -លិខិតបញ្ជាទិញ និងវិក្កយបត្រ -លិខិតបញ្ជាទិញ ទំនិញដែលបានទទួល និងវិក្កយបត្រ -លិខិតបញ្ជាទិញ ទំនិញដែលបានទទួល ត្រួតពិនិត្យជាក់ស្តែង និងវិក្កយបត្រ
ការកត់ត្រាវិក្កយបត្រ	ការព្រមានអំពីលេខវិក្កយបត្រស្ទួន
ការផ្គូផ្គងវិក្កយបត្រ	ចំនួនទឹកប្រាក់លម្អៀងក្នុងកម្រិតសមស្របដែលអាចអនុញ្ញាតឱ្យទូទាត់បាន
ដំណើរការទូទាត់	ដំណើរការទូទាត់ត្រូវមានការអនុម័ត និងកម្រិតកំណត់ទឹកប្រាក់

៩.២. វដ្តនៃការផ្គត់ផ្គង់ដល់ការទទួលសាច់ប្រាក់

វដ្តនៃការផ្គត់ផ្គង់រហូតដល់ការទទួលសាច់ប្រាក់ រួមបញ្ចូលនូវសកម្មភាពដែលទាក់ទងទៅនឹងការលក់ ការផ្គត់ផ្គង់ និងការចេញវិក្កយបត្រនៃការផ្តល់សេវាកម្មរបស់រដ្ឋាភិបាល។ សកម្មភាពទាំងនេះរួមមាន÷

- ការធ្វើបច្ចុប្បន្នភាពសៀវភៅធំ និងសៀវភៅធំរង
- ការកត់ត្រាឯកសារមេអំពីអតិថិជន
- ការស្នូរតម្លៃ ការប៉ាន់តម្លៃ ការកំណត់តម្លៃ និងការគ្រប់គ្រងកិច្ចសន្យា
- ដំណើរការបញ្ជាលក់ និងការគ្រប់គ្រងឥណទាន
- ដំណើរការផ្គត់ផ្គង់ទំនិញ ឬសេវាកម្ម
- ការប្រគល់ទំនិញត្រលប់មកវិញ
- ដំណើរការចេញវិក្កយបត្រ និងការបង់ប្រាក់។

ប្រព័ន្ធត្រួតពិនិត្យដែលត្រូវយកចិត្តទុកដាក់នៅក្នុងផ្នែកនេះរួមមាន: ការគ្រប់គ្រងលើការធ្វើបច្ចុប្បន្នភាពឯកសារមេអំពីអតិថិជន ការឆែកភាពស្ទួន តម្លៃសមស្រប ការអនុញ្ញាតកត់ត្រាទំហំលម្អៀងក្នុងវិក្កយបត្រ ការឆែកវិក្កយបត្រស្ទួន

អាយុកាលបំណុល កម្រិតកំណត់ឥណទាន ដំណើរការបញ្ចូលទិន្នន័យទៅក្នុងទិន្នានុប្បវត្តិ ការផ្ទៀងផ្ទាត់ចម្លងការ ការទទួលស្គាល់ចំណូល និងការបែងចែកតាមគណនី។

១០. ប្រព័ន្ធត្រួតពិនិត្យដោយដៃសម្រាប់គោលដៅស្វ័យប្រវត្តិកម្ម

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ: ដំណើរការស្វ័យប្រវត្តិកម្មនៃប្រព័ន្ធត្រួតពិនិត្យដោយដៃត្រូវបញ្ចូលក្នុងផែនការ និងគ្រប់គ្រងច្បាស់លាស់ ដើម្បីកាត់បន្ថយការចំណាយនិងពេលវេលាការងាររបស់មន្ត្រី ព្រមទាំងបង្កើនប្រសិទ្ធភាពប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។

ការជំរុញរចនាសម្ព័ន្ធ និងការអនុវត្តសាកល្បងពាក់ព័ន្ធដំណើរការស្វ័យប្រវត្តិកម្មនៃប្រព័ន្ធត្រួតពិនិត្យ គឺជាដំណើរការសន្សឹមៗ និងទាមទារពេលវេលា ដើម្បីផ្តល់ភាពជឿជាក់ទៅលើប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិ ។

ស្វ័យប្រវត្តិកម្មប្រព័ន្ធត្រួតពិនិត្យត្រូវរៀបចំក្នុងករណី÷

- បបព ដែលមានប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិសម្រាប់ជំនួស
- ប្រព័ន្ធត្រួតពិនិត្យកំពុងដំណើរការនៅផ្នែកមានហានិភ័យ ដែលប៉ះពាល់ខ្លាំងលើប្រតិបត្តិការ និង/ឬរបាយការណ៍ហិរញ្ញវត្ថុ
- ប្រព័ន្ធត្រួតពិនិត្យបច្ចុប្បន្នទាមទារចំណាយខ្ពស់ និង/ឬពេលវេលាច្រើនសម្រាប់ប្រតិបត្តិការ
- ដំណើរការអនុវត្តបច្ចុប្បន្នងាយនឹងមានកំហុស និង/ឬខូចខាត
- នីតិវិធីបច្ចុប្បន្នមានលក្ខណៈដដែលៗ និងត្រូវការការវិនិច្ឆ័យតិចតួចពីមនុស្ស

នៅពេលប្រព័ន្ធត្រួតពិនិត្យស្វ័យប្រវត្តិពុំទាន់ដំណើរការប្រកបដោយប្រសិទ្ធភាពពេញលេញ និងពិនិត្យដោយសវនកម្មផ្ទៃក្នុង ប្រព័ន្ធត្រួតពិនិត្យដោយដៃនៅតែអនុញ្ញាតឱ្យបន្តអនុវត្តដដែល។

១១. ការតាមដានលើប្រព័ន្ធត្រួតពិនិត្យ

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យរបស់ បបព គឺជាកម្មវត្ថុនៃការពិនិត្យតាមដានបន្ត។

ការតាមដាន គឺជាដំណើរការនៃការវាយតម្លៃលើការតាក់តែង និងការប្រតិបត្តិនៃប្រព័ន្ធត្រួតពិនិត្យក្នុងពេលវេលាសមស្រប និងមានវិធានការតាមការចាំបាច់។ ការតាមដាននេះត្រូវអនុវត្តដោយមន្ត្រីទទួលបន្ទុកលើគ្រប់សកម្មភាពនៅក្នុងអង្គភាព និងពេលខ្លះជាមួយភាគីកិច្ចសន្យាខាងក្រៅផងដែរ។ ការតាមដានអាចអនុវត្តបានតាមពីររបៀប÷

- សកម្មភាពជាប្រចាំ: សំដៅដល់សកម្មភាពតាមដានប្រសិទ្ធភាពនៃប្រព័ន្ធត្រួតពិនិត្យនៃប្រតិបត្តិការជាធម្មតា ដូចជាសកម្មភាពត្រួតពិនិត្យ និងគ្រប់គ្រងជាទៀងទាត់របស់ថ្នាក់ដឹកនាំ ការប្រៀបធៀប ការផ្សះផ្គង និងសកម្មភាពជាប្រចាំផ្សេងៗទៀត (ឧ.ការប្រៀបធៀបទិន្នន័យដែលបានកត់ត្រាដោយប្រព័ន្ធ និងជាក់ស្តែងនៅខាងក្រៅ)

- ការវាយតម្លៃដោយឡែក: សំដៅដល់ការវាយតម្លៃលើប្រព័ន្ធត្រួតពិនិត្យដោយថ្នាក់ដឹកនាំ និង/ឬដោយសវនកម្មផ្ទៃក្នុង។ ប្រព័ន្ធត្រួតពិនិត្យទាក់ទងនឹងហានិភ័យកម្រិតខ្ពស់និងសំខាន់ ទាមទារនូវការតាមដានវាយតម្លៃឱ្យបានញឹកញាប់។

រាល់សកម្មភាពតាមដានលើប្រសិទ្ធភាពប្រព័ន្ធត្រួតពិនិត្យនៃប្រតិបត្តិការប្រចាំថ្ងៃ ត្រូវបញ្ចូលជារចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងរបស់ បបព។

សន្ទានុក្រម

ការអនុញ្ញាត (Authorisation)	ការផ្តល់សិទ្ធិចំពោះអត្តសញ្ញាណដែលបានកំណត់ដើម្បីផ្ទៀងផ្ទាត់លើការចូលទៅប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។
ការផ្ទៀងផ្ទាត់អត្តសញ្ញាណ (Authentication)	ការបញ្ជាក់អត្តសញ្ញាណអ្នកប្រើប្រាស់មុនពេលចូលទៅប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។
ម៉ូដែលអាជែល (Agile Model)	វិធីចាត់ចែងគំរោងអភិវឌ្ឍន៍ប្រព័ន្ធតាមរយៈការបំបែកជាដំណាក់កាលច្រើន ទន់ភ្លន់ និងលឿនជាងម៉ូដែលតាមដំណាក់។
កម្មវិធីស្រេច (Application)	សំណុំនៃកម្មវិធី ទិន្នន័យ និងនីតិវិធីដែលរួមបញ្ចូលគ្នាបង្កើតជាប្រព័ន្ធព័ត៌មានដែលត្រូវបានតាក់តែងឡើងដើម្បីគ្រប់គ្រងមុខងាររដ្ឋបាល ឬធុរកិច្ចជាក់លាក់ (ឧ. គណនេយ្យ ការទូទាត់ ការកត់ត្រាបញ្ជីសារពើភណ្ឌ)។
គន្លងសវនកម្ម (Audit Trail)	ព័ត៌មានសម្រាប់តាមដានសកម្មភាពដែលចូល និងប៉ះពាល់ដល់ទិន្នន័យក្នុងប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។ គន្លងសវនកម្មអាចរួមបញ្ចូល ឈ្មោះអ្នកកែចម្លងការ និងពេលវេលាកែជាដើម។
ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច (Application Controls)	នីតិវិធីត្រួតពិនិត្យផ្ទៃក្នុងលើប្រព័ន្ធកម្មវិធីស្រេចជាក់លាក់ ដើម្បីធានាថារាល់ចម្លងការទាំងអស់ត្រូវបានអនុញ្ញាត និងកត់ត្រា ហើយត្រូវបានដំណើរការពេញលេញត្រឹមត្រូវ និងទាន់ពេលវេលា ដោយផលិតចេញនូវលទ្ធផលតាមការកំណត់។
បន្ទាត់មូលដ្ឋាន (Baseline)	មូលដ្ឋាន ឬចំណុចគោលសម្រាប់ប្រៀបធៀប ដើម្បីធ្វើការវាយតម្លៃ ឧ.ប្រព័ន្ធសុវត្ថិភាពជាមូលដ្ឋាន។
ផែនការនិរន្តរភាពធុរកិច្ច (Business Continuity Planning)	ដំណើរការដែលពាក់ព័ន្ធនឹងការបង្កើតប្រព័ន្ធការពារ និងការស្តារឡើងវិញពីការគំរាមកំហែងដែលអាចកើតមានចំពោះអង្គភាព។
សុវត្ថិភាព (Security)	ការរារាំងចំពោះការចូលដំណើរការ និងការផ្លាស់ប្តូរដោយគ្មានការអនុញ្ញាត ព្រមទាំងការបាត់បង់ភាពប្រើប្រាស់បាននៃព័ត៌មាន និងប្រព័ន្ធ។
សកម្មភាពកែតម្រូវ (Corrective Action)	សកម្មភាពដើម្បីលប់បំបាត់ឫសគល់នៃភាពមិនអនុលោម ឬស្ថានភាពមិនសមស្របផ្សេងៗដែលបានរកឃើញ។

គ្រីបតូក្រាហ្វិក (Cryptographic)	បច្ចេកទេសសម្រាប់រក្សាសុវត្ថិភាពគមនាគមន៍ព័ត៌មានដោយបំប្លែងព័ត៌មានទៅជាទម្រង់សុវត្ថិភាព។
ការសម្ងាត់ (Confidentiality)	ការបង្ការព័ត៌មានពីការចូលប្រើដោយគ្មានការអនុញ្ញាត។
ការរៀបតម្រូវ (Configuration)	ការរៀបចំជាផ្នែក ឬតាមសមាសធាតុនៅក្នុងទម្រង់ជាក់លាក់មួយ។
ផែនការស្តារគ្រោះមហន្តរាយ (Disaster Recovery Plan)	ផែនការសម្រាប់ស្តារសេវាកម្មព័ត៌មានវិទ្យាសំខាន់ៗក្នុងករណីមានគ្រោះមហន្តរាយប៉ះពាល់ដល់ហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មានវិទ្យា។ ផែនការស្តារពីគ្រោះមហន្តរាយគឺជាផ្នែកមួយនៃផែនការនិរន្តរភាពធុរកិច្ច។
ឃ្លាំងទិន្នន័យ (Data Warehouses)	ប្រព័ន្ធគ្រប់គ្រងទិន្នន័យដែលត្រូវបានតាក់តែងឡើងដើម្បីគាំទ្រសកម្មភាពធុរកិច្ចវៃឆ្លាត (BI) ជាពិសេសសម្រាប់រាយការណ៍ និងវិភាគទិន្នន័យ។
បណ្ណសារទិន្នន័យ (Data Archives)	ការផ្ទេរទិន្នន័យដែលមិនសូវប្រើប្រាស់ទៅឧបករណ៍ផ្ទុកទិន្នន័យរយៈពេលវែង។
ទិន្នន័យ (Data)	លេខ តួអក្សរ រូបភាព ឬកំណត់ត្រាតាមវិធីសាស្ត្រផ្សេងៗ ក្នុងទម្រង់ដែលអាចវាយតម្លៃបានដោយមនុស្ស ឬអាចបញ្ចូលក្នុងកុំព្យូទ័រ។
ការវាយប្រហារលើប្រព័ន្ធ (Denial of Service Attack)	ការវាយប្រហារដែលធ្វើគាំងម៉ាស៊ីន ឬបណ្តាញ និងធ្វើឱ្យអ្នកប្រើប្រាស់មិនអាចចូលបាន។
ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (IT Controls)	នីតិវិធី ឬគោលនយោបាយដែលផ្តល់ការធានាសមស្របថា បច្ចេកវិទ្យាព័ត៌មានប្រើប្រាស់ដោយអង្គភាពប្រព្រឹត្តទៅតាមការរំពឹងទុក ទិន្នន័យជឿទុកចិត្តបាន ហើយអនុលោម តាមច្បាប់និងបទប្បញ្ញត្តិជាធរមាន។ ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានចែកជាប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅនិងប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច។
សវនកម្មបច្ចេកវិទ្យាព័ត៌មាន (IT Audit)	ដំណើរការមានលក្ខណៈជាប្រព័ន្ធ ឯករាជ្យ និងចងក្រងឯកសារ ដើម្បីប្រមូល និងវាយតម្លៃភស្តុតាង ក្នុងគោលបំណងបញ្ជាក់អំពីកម្រិតសមស្របជាមួយលក្ខណៈវិនិច្ឆ័យនៃសវនកម្មបច្ចេកវិទ្យាព័ត៌មាន។

ទ្រព្យសកម្មព័ត៌មាន (Information Asset)	ទ្រព្យសកម្មព័ត៌មានគឺជាទិន្នន័យ ឬចំណេះដឹងទាំងឡាយដែលមានតម្លៃចំពោះស្ថាប័ន។ ទ្រព្យសកម្មមិនត្រឹមតែទំនិញប្រើប្រាស់ ឬផ្នែករឹង ប៉ុន្ណែ្ណមបញ្ចូលទាំងផ្នែកទន់ ព័ត៌មាន មនុស្ស និងកេរ្តិ៍ឈ្មោះ។
ប្រព័ន្ធព័ត៌មាន (Information System)	ការរួមបញ្ចូលគ្នានៃយុទ្ធសាស្ត្រ ការគ្រប់គ្រង និងសកម្មភាពប្រតិបត្តិការ រួមទាំងដំណើរការដែលពាក់ព័ន្ធនឹងការប្រមូល កិច្ចដំណើរការ ការរក្សាទុក ការចែកចាយ និងការប្រើប្រាស់ព័ត៌មាននិងបច្ចេកវិទ្យាពាក់ព័ន្ធ។
បច្ចេកវិទ្យាព័ត៌មាន (Information Technology)	ផ្នែករឹង ផ្នែកទន់ គមនាគមន៍ និងបរិធានផ្សេងទៀតដែលប្រើសម្រាប់បញ្ចូល រក្សាទុក ដំណើរការ បញ្ជូន និងបញ្ចេញទិន្នន័យក្នុងទម្រង់ណាមួយ។
ឧប្បត្តិហេតុបច្ចេកវិទ្យាព័ត៌មាន (IT Incident)	ព្រឹត្តិការណ៍ដែលរំខាន ឬកាត់បន្ថយគុណភាពសេវាកម្មបច្ចេកវិទ្យាព័ត៌មាន។
ការគ្រប់គ្រងអត្តសញ្ញាណអ្នកប្រើប្រាស់និងការគ្រប់គ្រងការចូលប្រើប្រាស់ (Identity and Access management)	ជាក្របខ័ណ្ឌនៃដំណើរការធុរកិច្ច គោលនយោបាយ និងបច្ចេកវិទ្យាដែលសម្របសម្រួលការគ្រប់គ្រងអត្តសញ្ញាណអេឡិចត្រូនិក ឬឌីជីថល។
ហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (IT Infrastructure)	ប្រព័ន្ធសម្ភារៈ ឧបករណ៍ និងសេវាកម្មផ្សេងៗសម្រាប់ដំណើរការរបស់អង្គភាពដូចជាបណ្តាញ ម៉ាស៊ីនបម្រើ ម៉ាស៊ីនភ្ជៀវ ម៉ាស៊ីនបោះពុម្ព ជាដើម។
ធាតុចូល (Input)	ទិន្នន័យដែលបញ្ចូលក្នុងកុំព្យូទ័រសម្រាប់ដំណើរការ ឬដំណើរការបញ្ចូលទិន្នន័យទៅក្នុងប្រព័ន្ធកុំព្យូទ័រ។
ការសម្រាល (Mitigate)	ការកាត់បន្ថយលទ្ធភាព ឬផលវិបាកនៃការគំរាមកំហែងដោយប្រព័ន្ធត្រួតពិនិត្យ។
កម្មវិធីអាក្រក់ (Malicious Software)	ប្រភេទកម្មវិធីដែលមានបំណងបង្កគ្រោះថ្នាក់ ឬលួចព័ត៌មានអ្នកប្រើប្រាស់។
ការផ្តត់ផ្តង់ពីក្រៅ (Outsource)	ការទទួលបានទំនិញ ឬសេវាកម្មតាមកិច្ចសន្យាពីអ្នកផ្តត់ផ្តង់ខាងក្រៅ។
ការបំពាន (Override)	ការលុប ឬការផ្លាស់ប្តូរព័ត៌មានដោយគ្មានការអនុញ្ញាត និងការរំលោភលើសិទ្ធិអំណាចព្រមទាំងគោលការណ៍បានកំណត់។

ធាតុចេញ (Output)	ទិន្នន័យបញ្ចេញពីប្រព័ន្ធកុំព្យូទ័រតាមរយៈឧបករណ៍បញ្ចេញទិន្នន័យ ឬព័ត៌មានផ្សេងៗ។
ហ្វីស៊ីង (Phishing)	ប្រភេទនៃការវាយប្រហារដោយបន្លំតាមមធ្យោបាយបច្ចេកវិទ្យាព័ត៌មានក្នុងគោលបំណងទទួលបានព័ត៌មានផ្ទាល់ខ្លួនអ្នកប្រើប្រាស់។
ដំណើរការ (Processing)	ការអនុវត្តន៍វប្រតិបត្តិការដែលកំណត់ទុកជាមុនតាមលំដាប់បន្តគ្នាលើទិន្នន័យបញ្ចូលដើម្បីបញ្ចេញជាទិន្នន័យ ឬព័ត៌មាន។
តម្លៃធៀប (Relative Value)	តម្លៃនៃទ្រព្យសកម្មដែលកំណត់តាមមធ្យោបាយធៀបជាមួយតម្លៃនៃទ្រព្យសកម្មស្រដៀងគ្នា។
ការដោះស្រាយហានិភ័យ (Risk Treatment)	ដំណើរការជ្រើសរើស និងអនុវត្តវិធានការដើម្បីឆ្លើយតបទៅលើហានិភ័យ រួមមានការបញ្ឈៀស ការកាត់បន្ថយ ការផ្ទេរចេញ ឬការរក្សាទុក។
កម្រិតនៃហានិភ័យទទួលយក (Risk appetite levels)	កម្រិតនៃហានិភ័យដែលអង្គភាពទទួលយកដើម្បីសម្រេចគោលបំណងរបស់ខ្លួនមុនចេញវិធានការលើហានិភ័យ។
ការកាក់ទុក (Retention)	ការបន្តរក្សាទុកទិន្នន័យរបស់អង្គភាពតាមការកំណត់ ឬដោយហេតុផលធុរកិច្ច។
ការគ្រប់គ្រងហានិភ័យ (Risk Management)	ការអនុវត្តជាប្រព័ន្ធនូវគោលការណ៍គ្រប់គ្រង នីតិវិធី និងការអនុវត្តផ្សេងៗ ទៅលើការវិភាគ វាយតម្លៃ និងគ្រប់គ្រងហានិភ័យ។
ហានិភ័យ (Risk)	ឱកាសដែលព្រឹត្តិការណ៍ ឬសកម្មភាព (រួមទាំងការមិនមានសកម្មភាព) នាំឱ្យមានលទ្ធផលមិនគាប់បំណង ដូចជាផលប៉ះពាល់អវិជ្ជមានលើការសម្រេចបាននូវគោលបំណងធុរកិច្ច ឬកំហុសឆ្គងក្នុងរបាយការណ៍ហិរញ្ញវត្ថុ។
ការវិភាគហានិភ័យ (Risk Analysis)	ការប្រើប្រាស់ព័ត៌មានជាប្រព័ន្ធដើម្បីកំណត់ និងវាយតម្លៃហានិភ័យ។
ការវាយតម្លៃហានិភ័យ (Risk Assessment)	ការវាយតម្លៃពេញលេញលើហានិភ័យ រួមទាំងផលប៉ះពាល់។
តេស្តស្ត្រេស (Stress Test)	ការធ្វើតេស្តជាមួយកំណើនព្រមគ្នានៃអ្នកប្រើប្រាស់ ឬសេវាកម្ម នៅក្នុងកម្មវិធីស្រេចដើម្បីកំណត់ចំនួនអតិបរមាដែលកម្មវិធីស្រេចនៅអាចដំណើរការបាន។

ឯកសារមេ (Standing data/ Master files)	ឯកសារផ្តុំកន្លែវព័ត៌មាន ដូចជា ឈ្មោះ និងអាសយដ្ឋានរបស់អ្នកផ្គត់ផ្គង់/អតិថិជន ដែលមិនផ្លាស់ប្តូរញឹកញាប់ និងត្រូវបានប្រើប្រាស់អំឡុងពេលដំណើរការ។
កម្រិត/ទំហំអាចទទួលយក Tolerance Levels/Amount	កម្រិតបំរែបំរួល ឬទំហំដែលអ្នកគ្រប់គ្រងមានឆន្ទៈកំណត់ ឬទទួលយកដើម្បីសម្រេចគោលបំណងរបស់ខ្លួន។
ការគំរាមកំហែង (Threats)	ដំណើរការដែលជំរុញលទ្ធភាពឱ្យកើតឡើងនៅព្រឹត្តិការណ៍អវិជ្ជមាន ដូចជាសកម្មភាពបំពានផ្សេងៗលើផ្នែកដែលទន់ខ្សោយ។
ភាពងាយរងគ្រោះ (Vulnerabilities)	ភាពទន់ខ្សោយនៅក្នុងហេដ្ឋារចនាសម្ព័ន្ធ បណ្តាញ ឬកម្មវិធីស្រេច ដែលបង្កបញ្ហាប្រឈមនឹងការគំរាមកំហែង។
ម៉ូដែលតាមដំណាក់ (Waterfall Model)	ការបំបែកសកម្មភាពក្នុងគំរោងអភិវឌ្ឍន៍ប្រព័ន្ធជាដំណាក់ៗ ដែលដំណាក់នីមួយៗអាស្រ័យនឹងលទ្ធផលនៃដំណាក់មុនៗស្របតាមចរិតនៃមុខការ។