ក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ

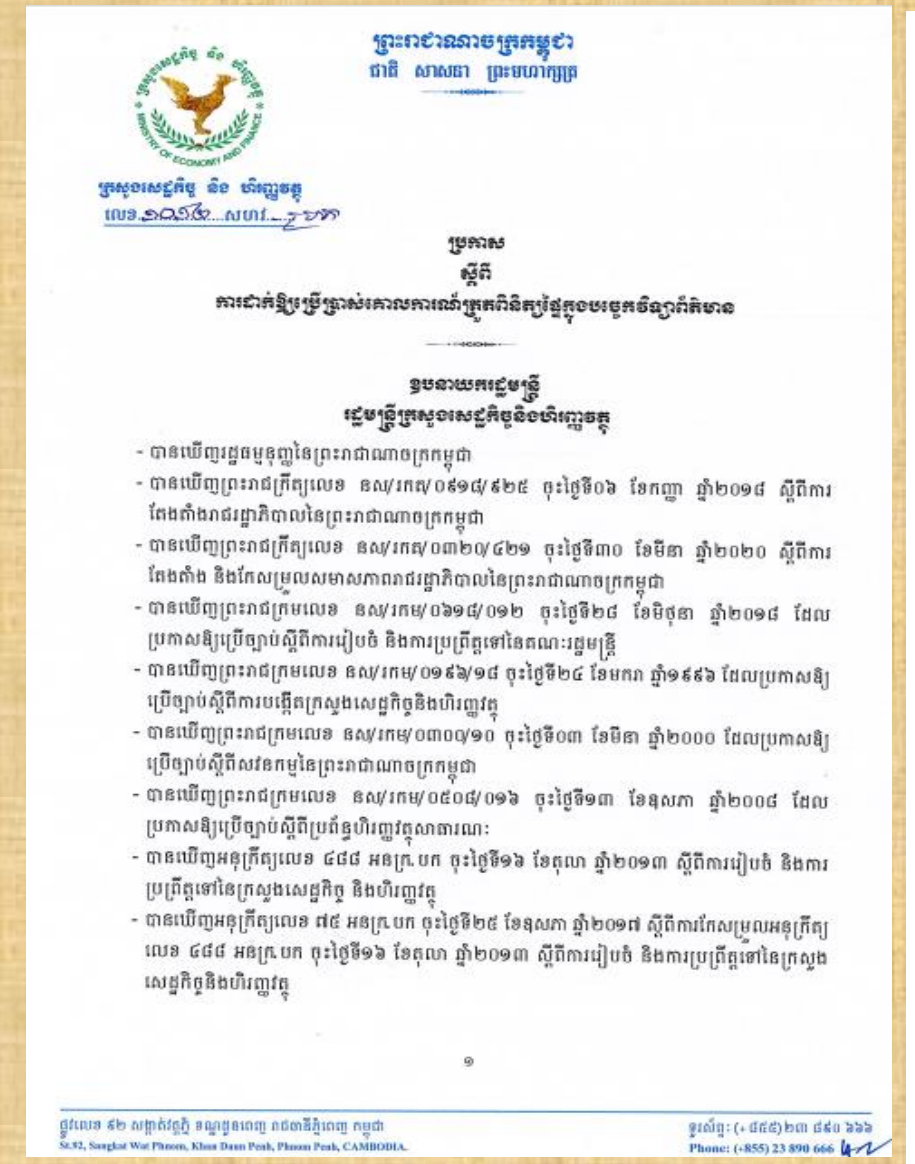
បទបង្ហាញ

ស្តីពី

“គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកទិទ្យាព័ត៌មាន ”

សណ្ឋាគារភ្នំពេញ, ថ្ងៃទី២៣ ខែមិថុនា ឆ្នាំ២០២២

ប្រកាសស្តីពីការដាក់ឱ្យប្រើប្រាស់គោលការណ៍ត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន



ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ
លេខ ...សហវ...

ប្រកាស
ស្តីពី
ការដាក់ឱ្យប្រើប្រាស់គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

ឧបនាយករដ្ឋមន្ត្រី
រដ្ឋមន្ត្រីក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

- បានឃើញរដ្ឋធម្មនុញ្ញនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកស/០៩១៨/៩២៥ ចុះថ្ងៃទី០៦ ខែកញ្ញា ឆ្នាំ២០១៨ ស្តីពីការតែងតាំងរាជរដ្ឋាភិបាលនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកស/០៣២០/៨២១ 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 ៧៩ 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 សរណ ចុះថ្ងៃទី២៥ ខែវិច្ឆិកា ឆ្នាំ២០១១ ស្តីពីការបន្តពង្រឹងមុខងារសវនកម្មផ្ទៃក្នុងតាមបណ្តាក្រសួង ស្ថាប័ន និងសហគ្រាសសាធារណៈ
- យោងតាមតម្រូវការចាំបាច់របស់ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

សម្រេច

ប្រការ១.-

ត្រូវបានដាក់ឱ្យប្រើប្រាស់គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន ជាក្របខណ្ឌសម្រាប់រៀបចំ គ្រប់គ្រង និងត្រួតពិនិត្យលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មានតាមក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែលរបស់រាជរដ្ឋាភិបាល។

ប្រការ២.-

គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន ត្រូវភ្ជាប់ជានុបសម្ព័ន្ធនៃប្រកាសនេះ។

ប្រការ៣.-

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

ប្រការ៤.-

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

ថ្ងៃ...ខែ...ឆ្នាំឆ្លូវ ត្រីស័ក ព.ស. ២៥៦៥
រាជធានីភ្នំពេញ ថ្ងៃទី...ខែ...ឆ្នាំ២០២១

ឧបនាយករដ្ឋមន្ត្រី
រដ្ឋមន្ត្រីក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

អគ្គបណ្ឌិតសភាចារ្យ អូន ព័ន្ធមុនីរ័ត្ន

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

បច្ចុប្បន្នភាព

ប្រកាសលេខ១០១២ សហវ.ប្រក ចុះថ្ងៃទី៣១ ខែធ្នូ ឆ្នាំ២០២១ ស្តីពី "**ការដាក់ឱ្យប្រើប្រាស់គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន**" (ជំនាន់ទី២) គឺត្រូវបានធ្វើបច្ចុប្បន្នភាពឡើងវិញលើប្រកាសលេខ ១៤៣៦ សហវ.ប្រក ចុះថ្ងៃទី០៨ ខែធ្នូ ឆ្នាំ២០១៦ ស្តីពី "**ការដាក់ឱ្យប្រើប្រាស់ឯកសារស្តីពីការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន**" (ជំនាន់ទី១) ដោយមានការកែសម្រួលខ្លឹមសារមួយចំនួនឱ្យស្របតាមបរិបទនៃការងារបច្ចុប្បន្ន និងស្របតាមឧត្តមានុវត្តន៍ ដែលជំនាន់ទី២នេះ មានភាពខុសគ្នា រវាងជំនាន់ទី១ ៦ចំណុច ដូចខាងក្រោម÷

- ចំណងជើងឯកសារ កែប្រែពី "ការគ្រប់គ្រងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន" ទៅជា "គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន"
- និយមន័យ និងគោលបំណងនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង " រួមបញ្ចូលនិយមន័យ និងគោលបំណងក្នុងផ្នែកតែមួយ និងបន្ថែម៣ចំណុច ក្នុងជំនាន់ទី២នេះ"

បច្ចុប្បន្នភាព (ត)

- តួនាទី និងភារកិច្ចរបស់សវនកម្មផ្ទៃក្នុង ក្នុងការអនុវត្តប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ត្រូវបានដកចេញ ដោយសារតួនាទីសវនកម្មបានរំលេចនៅចំណុច១ រួចហើយ
- កែសម្រួលរចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន និងនិយមន័យ
- ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅ "កែសម្រួលប្រព័ន្ធត្រួតពិនិត្យ និងបន្ថែមថ្មី ដោយពន្យល់ពីគោលបំណង និងចំណុចចំណុចគួរយកចិត្តទុកដាក់"
- ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច "កែសម្រួលប្រព័ន្ធត្រួតពិនិត្យ និងបន្ថែមនិយមន័យ គោលបំណង និងចំណុចគួរយកចិត្តទុកដាក់"

មាតិកា

ផ្នែកទី ១: ទិដ្ឋភាពទូទៅនៃគោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

១.១. និយមន័យ និងគោលបំណង

និយមន័យ÷ ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង គឺជាដំណើរការអនុវត្តដោយថ្នាក់ដឹកនាំ និងបុគ្គលិកផ្សេងទៀតដែលត្រូវបានរៀបចំឡើង ដើម្បីធានាដល់ការសម្រេចបាននូវគោលដៅដូចខាងក្រោម÷

- របាយការណ៍ហិរញ្ញវត្ថុដែលអាចជឿទុកចិត្តបាន
- ប្រសិទ្ធភាព និងប្រសិទ្ធផលនៃប្រតិបត្តិការ
- អនុលោមភាពជាមួយច្បាប់ និងបទប្បញ្ញត្តិ
- ការពារសុវត្ថិភាពទ្រព្យសម្បត្តិ

(ប្រភព: ផ្អែកលើនិយមន័យនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង របស់ COSO)

១.១. និយមន័យ និងគោលបំណង (ត)

គោលបំណង÷ ប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងរបស់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ត្រូវរៀបចំឡើងដើម្បីជួយដល់ថ្នាក់ដឹកនាំសម្រេចបាននូវគោលបំណង ដូចខាងក្រោម:

- **ធានាបូរណភាពនៃបរិស្ថានប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរសើប និងសំខាន់÷**
  - **ការអនុញ្ញាត** - ធានាថាចម្លងការទាំងអស់ត្រូវបានទទួលការឯកភាពពីមន្ត្រីទទួលខុសត្រូវ ស្របតាមសិទ្ធិសម្រេចជាទូទៅ ឬដោយឡែកមុនពេលដែលចម្លងការត្រូវបានកត់ត្រា។
  - **សុពលភាព** - មានតែប្រតិបត្តិការដែលបានអនុញ្ញាតហើយដែលកើតឡើងពិតប្រាកដ និងពាក់ព័ន្ធនឹងអង្គភាពប៉ុណ្ណោះត្រូវបានកត់ត្រា។
  - **ភាពពេញលេញ** - រាល់ប្រតិបត្តិការដែលកើតឡើងត្រូវបានបញ្ចូល និងទទួលយកសម្រាប់ដំណើរការនៅក្នុងប្រព័ន្ធតែមួយលើក។

១.១. និយមន័យ និងគោលបំណង (ត)

- **សុក្រឹតភាព** - ប្រតិបត្តិការត្រូវបានកត់ត្រានូវចំនួន និងក្នុងគណនីត្រឹមត្រូវជាមួយពេលសមស្រប។

- **ការកំណត់អត្តសញ្ញាណ និងការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវ:** ធានាបាននូវភាពសមស្របលើការគ្រប់គ្រង ការកំណត់អត្តសញ្ញាណ និងផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវនៃអ្នកប្រើប្រាស់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។

- **ប្រសិទ្ធភាព និងប្រសិទ្ធផលនៃប្រតិបត្តិការ:** ធានាបាននូវប្រសិទ្ធភាព និងប្រសិទ្ធផលនៃប្រតិបត្តិការដែលគាំទ្រដោយប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។

- **លទ្ធភាពប្រើប្រាស់នៃសេវាកម្មបច្ចេកវិទ្យាព័ត៌មាន:** ធានាលទ្ធភាពដែលអាចប្រើប្រាស់បានរបស់ព័ត៌មាន នៅពេលដែលមានតម្រូវការពីម្ចាស់ដំណើរការធុរកិច្ចក្នុងពេលបច្ចុប្បន្ន និងទៅអនាគត។

១.១. និយមន័យ និងគោលបំណង (ត)

- **ការឆ្លើយតបឧប្បត្តិហេតុ:** ធានាថាឧប្បត្តិហេតុទាំងអស់គ្រប់គ្រងបានត្រឹមត្រូវ និងកំហុសដែលបានរកឃើញនៅគ្រប់ដំណាក់កាលនៃដំណើរការត្រូវបានកែតម្រូវទាន់ពេល និងរាយការណ៍ទៅថ្នាក់គ្រប់គ្រងសមស្រប។
- **ប្រូវណភាព និងភាពជឿជាក់នៃប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន:** ធានាបាននូវប្រសិទ្ធភាពនៃការអនុវត្តនីតិវិធីគ្រប់គ្រងការផ្លាស់ប្តូរ។
- **ដំណើរការ និងសេវាកម្មប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានផ្តល់ពីខាងក្រៅ:**ធានាថាដំណើរការ និងសេវាកម្មប្រព័ន្ធ បច្ចេកវិទ្យាព័ត៌បានកំណត់ច្បាស់នូវកិច្ចព្រមព្រៀងកម្រិតសេវាកម្ម (SLA) និងលក្ខខ័ណ្ឌនៃកិច្ចសន្យាដើម្បីធានាថាទ្រព្យសម្បត្តិអង្គភាពត្រូវបានការពារត្រឹមត្រូវ ហើយបំពេញតាមគោលដៅ និងគោលបំណងធុរកិច្ច។

១.២.ការទទួលខុសត្រូវលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

- ថ្នាក់ដឹកនាំ រួមទាំងមន្ត្រីទាំងអស់របស់ក្រសួង ស្ថាប័ន និងអង្គភាពសាធារណៈប្រហាក់ប្រហែល ជាអ្នកទទួលខុសត្រូវលើ÷
  - ការតាក់តែង
  - ការអនុវត្តលើប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងស្របតាមបទប្បញ្ញត្តិពាក់ព័ន្ធ និង;
  - ការថែរក្សារចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

- សវនកម្មផ្ទៃក្នុងមានតួនាទី÷
  - ពិនិត្យតាមដានការត្រួតពិនិត្យផ្ទៃក្នុង
  - ផ្តល់ការអះអាងជូនថ្នាក់ដឹកនាំអំពីគុណភាពនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង និងប្រសិទ្ធភាពនៃការអនុវត្ត។

១.៣. បច្ចុប្បន្នភាពគោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

អគ្គនាយកដ្ឋានសវនកម្មផ្ទៃក្នុង (អសក) នៃក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ (កសហវ) ត្រូវពិនិត្យឡើងវិញជារៀងរាល់ឆ្នាំនូវ “គោលការណ៍ត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន” និងធ្វើការកែតម្រូវតាមការចាំបាច់។

ផ្នែកទី ២: គោលការណ៍ និងស្តង់ដារប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

២.១. ស្តង់ដារនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង

- ក្របខ័ណ្ឌសវនកម្មកំណត់ដោយគណៈកម្មាធិការនៃអង្គការគាំទ្ររបស់ស្ថងការទ្រីដវេ (COSO) ត្រូវបានយកមកប្រើប្រាស់ដើម្បីវាយតម្លៃលើភាពគ្រប់គ្រាន់នៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង។ COSO ផ្តោតលើផ្នែកចំនួនប្រាំសម្រាប់សម្រេចគោលបំណងប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង រួមមាន÷
  - **បរិស្ថានត្រួតពិនិត្យ:** គឺជាសកម្មភាព គោលនយោបាយ និងនីតិវិធីដែលឆ្លុះបញ្ចាំងអំពីឥរិយាបថទូទៅរបស់អ្នកគ្រប់គ្រងជាន់ខ្ពស់ចំពោះសារសំខាន់នៃការគ្រប់គ្រងផ្ទៃក្នុងចំពោះអង្គភាព។
  - **ការវាយតម្លៃហានិភ័យ:** ជាដំណើរការនៃការកំណត់ហានិភ័យ និងហានិភ័យត្រូវបានគ្រប់គ្រងដើម្បីសំរេចគោលដៅរបស់អង្គភាព។
  - **សកម្មភាពត្រួតពិនិត្យ:** ជាគោលនយោបាយ និងនីតិវិធីដែលធានា ការណែនាំ និងទិសដៅរបស់អ្នកគ្រប់គ្រងត្រូវបានអនុវត្តក្នុងការឆ្លើយតបនិងអត្តសញ្ញាណហានិភ័យនានាដែលបានរកឃើញ ដើម្បីសំរេចគោលដៅរបស់អង្គភាព។

២.១. ស្តង់ដារនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង (ត)

- **ព័ត៌មាន និងគមនាគមន៍:** ព័ត៌មាន គឺចាំបាច់គ្រប់កម្រិតរបស់អង្គភាព ក្នុងប្រតិបត្តិការប្រចាំថ្ងៃ រួមមាន ព័ត៌មានប្រតិបត្តិការ និង ហិរញ្ញវត្ថុ (ព័ត៌មានល្អ ជាព័ត៌មាន មានប្រភពច្បាស់លាស់ និងទាន់ពេលវេលា) ។ គមនាគមន៍ ឋានុក្រមនៃលំហូរព័ត៌មានត្រូវបានកំណត់ ដើម្បីឆ្លើយតបនិងតម្រូវការប្រើប្រាស់និងការទទួលខុសត្រូវ របស់អ្នកគ្រប់គ្រងគ្រប់កម្រិត។
- **ការតាមដាន:** ជាការវាយតម្លៃជាប្រចាំនិងវាយតម្លៃក្នុងកំឡុងពេលណាមួយអំពីគុណភាពនៃការអនុវត្តការ គ្រប់គ្រងផ្ទៃក្នុង ដើម្បីកំណត់ថាតើការគ្រប់គ្រងផ្ទៃក្នុង បានប្រតិបត្តិការដូចបំណង និងកែតម្រូវនៅពេលចាំបាច់ដែរឬទេ។

២.១. ស្តង់ដារនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង (ត)

- ក្របខ័ណ្ឌ COSO មិនអាចប្រើប្រាស់សម្រាប់ធ្វើសវនកម្មប្រព័ន្ធព័តិមានបានពេញលេញទេ គឺត្រូវប្រើប្រាស់ក្របខ័ណ្ឌ “គោលបំណងប្រព័ន្ធត្រួតពិនិត្យព័តិមាន និងបច្ចេកវិទ្យាពាក់ព័ន្ធ” (Control Objectives for Information and Related Technology-COBIT) នៃសមាគមសវនកម្ម និងត្រួតពិនិត្យប្រព័ន្ធបច្ចេកវិទ្យាព័តិមាន (ISACA)។
- នៅក្នុងការអនុវត្ត COBIT សម្រាប់ធ្វើសវនកម្មប្រព័ន្ធព័តិមាន ពិសេសការវាយតម្លៃលើភាពគ្រប់គ្រាន់នៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងនៃប្រព័ន្ធបច្ចេកវិទ្យាព័តិមាន ត្រូវគោរពគោលបំណងរបស់ COSO ខាងលើ។

២.២. ការវាយតម្លៃហានិភ័យប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ៖ ការវាយតម្លៃហានិភ័យត្រូវអនុវត្តជាប្រចាំ ហើយប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងត្រូវ តាក់តែង ដើម្បីកាត់បន្ថយហានិភ័យដែលបានកត់សម្គាល់ឃើញ។

“**ហានិភ័យ**” គឺជាស្ថានភាពដែលព្រឹត្តិការណ៍ ឬសកម្មភាព (រួមទាំងដំណើរគ្មានសកម្មភាព) បានផ្តល់ផលប៉ះពាល់ទៅលើការសម្រេចគោលបំណងធុរកិច្ច ឬកំហុសឆ្គងនៅក្នុងរបាយការណ៍ហិរញ្ញវត្ថុ។ កម្រិតហានិភ័យអាចវាស់វែងដោយ ផ្អែកលើផលប៉ះពាល់ និងឱកាសដែលអាចកើតឡើង។

ហានិភ័យដែលទាក់ទងនឹងដំណើរការប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ត្រូវបានកំណត់ បន្ទាប់មកប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងត្រូវតាក់តែងឡើងដោយចំណុចចាប់ផ្តើមសំខាន់ គឺវាយតម្លៃរចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យដែលមានស្រាប់ ដើម្បីកែតម្រូវក្នុងករណីមិនឆ្លើយតបក្នុងបរិស្ថានស្ងួយប្រវត្តិ។

២.៣. អត្ថប្រយោជន៍នៃស្វ័យប្រវត្តិកម្មប្រព័ន្ធត្រួតពិនិត្យ

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ជំរុញការផ្លាស់ប្តូរជាបណ្តើរៗពីរចនាសម្ព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងដោយដៃទៅជាប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងស្វ័យប្រវត្តិ។

ផលប្រយោជន៍នៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងស្វ័យប្រវត្តិ មាន÷

- កាត់បន្ថយលទ្ធភាពអាចកើតឡើងនូវកំហុស និងការកេងបន្លំដែលបង្កដោយមនុស្ស
- ចំណាយពេលតិចជាងក្នុងការងារ ឬការគ្រប់គ្រងដែលបំពេញដោយដៃ
- បង្កើនវិសាលភាពនិងគុណភាពនៃការធ្វើតេស្តសវនកម្មតាមរយៈការទាញយកនិងការបម្លែងកំណត់ត្រា និងទិន្នន័យអេឡិចត្រូនិក
- បង្កើនប្រសិទ្ធភាពសវនកម្មតាមរយៈការជំនួសការធ្វើតេស្តសវនកម្មដោយដៃ ដែលយឺតយ៉ាវនិងងាយកើតមានកំហុស ដោយកម្មវិធីស្រេច។

២.៤. ប្រភេទនៃប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងបច្ចេកវិទ្យាព័ត៌មាន

ប្រព័ន្ធត្រួតពិនិត្យស្ថិយប្រវត្តិ គួរអនុវត្តនៅតាមទីកន្លែងដែលអាចធ្វើបាន។ ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទៅតាមគោលបំណងត្រួតពិនិត្យអាចចែកជាបីប្រភេទ÷

- ការពារ
- ស្វែងរក
- កែតម្រូវ

ទន្ទឹមនេះ ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានក៏អាចចែកជាបីប្រភេទតាមមធ្យោបាយជាក់ឱ្យប្រើប្រាស់÷

- រដ្ឋបាល
- បច្ចេកទេស/ប្រព័ន្ធ
- រូបវន្ត

២.៥. ប្រព័ន្ធត្រួតពិនិត្យអប្បបរមាស្តង់ដារ

ប្រព័ន្ធត្រួតពិនិត្យមិនគ្រប់គ្រាន់អាចកត់សំគាល់ឃើញតាមរយៈការគាក់តែង ឬការអនុវត្តជាក់ស្តែងរបស់ប្រព័ន្ធដែលមិនមានប្រសិទ្ធភាព។

ជាទូទៅ:

- ប្រព័ន្ធត្រួតពិនិត្យខ្លាំង = ពហុប្រព័ន្ធត្រួតពិនិត្យការពារ + ពហុប្រព័ន្ធត្រួតពិនិត្យស្វែងរក + ពហុប្រព័ន្ធត្រួតពិនិត្យកែតម្រូវ
- ប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា = ប្រព័ន្ធត្រួតពិនិត្យការពារមួយ + ប្រព័ន្ធត្រួតពិនិត្យស្វែងរកមួយ + ប្រព័ន្ធត្រួត
- ពិនិត្យកែតម្រូវមួយ + ប្រសិទ្ធភាពប្រតិបត្តិការនៃប្រព័ន្ធត្រួតពិនិត្យនីមួយៗនេះ
- ប្រព័ន្ធត្រួតពិនិត្យខ្សោយ = តិចជាងកម្រិតប្រព័ន្ធត្រួតពិនិត្យអប្បបរមា + ប្រតិបត្តិការប្រព័ន្ធត្រួតពិនិត្យមានចំណុចសង្ស័យ ឬអសង្គតិភាព។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន

ជាទូទៅរចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុងពេញលេញសម្រាប់ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន មានលក្ខណៈដូចខាងក្រោម÷

- **ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅ:** ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅ អនុវត្តគ្រប់សមាសធាតុប្រព័ន្ធបច្ចេកវិទ្យា ដំណើរការ និងទិន្នន័យទាំងអស់របស់ស្ថាប័ន ឬបរិស្ថានប្រព័ន្ធ។
- **ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច:** ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច សំដៅដល់កម្មវិធីកុំព្យូទ័រជាក់លាក់ ដែលរួមបញ្ចូលទាំងការគ្រប់គ្រងលើការបញ្ចូលប្រតិបត្តិការ ការដំណើរការ លទ្ធផល និងទិន្នន័យមេ។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ក. ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅ

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ

ប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មានទូទៅដែលគ្រប់គ្រាន់ ត្រូវដាក់ឱ្យអនុវត្តដើម្បីគាំទ្រដល់ហេដ្ឋារចនាសម្ព័ន្ធ និងប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេចនៃ បបព ។

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

បបព ត្រូវគាំទ្រដោយប្រព័ន្ធត្រួតពិនិត្យនៅតាមផ្នែកនានា ដូចខាងក្រោម÷

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១. ស្តង់ដារបច្ចេកវិទ្យាព័ត៌មាន គោលនយោបាយ និងគោលការណ៍ណែនាំ

គោលបំណង: ដើម្បីផ្តល់ទិសដៅការគ្រប់គ្រង និងគាំទ្រប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានស្របតាមតម្រូវការធុរកិច្ច ច្បាប់ និងបទប្បញ្ញត្តិពាក់ព័ន្ធ។

ស្តង់ដារបច្ចេកវិទ្យាព័ត៌មាន គោលនយោបាយ និងគោលការណ៍ណែនាំទាំងនេះ គួរតែជាក្របខ័ណ្ឌដែលអាចជួយគាំទ្រដល់ប្រតិបត្តិការប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។

ក្របខ័ណ្ឌនេះត្រូវមានការត្រួតពិនិត្យជាប្រចាំឆ្នាំដោយគិតគូរពីការផ្លាស់ប្តូរផែនការធុរកិច្ចរបស់អង្គភាព និងបរិស្ថានបច្ចេកវិទ្យាព័ត៌មាន។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

២. រចនាសម្ព័ន្ធរបស់ស្ថាប័ន

គោលបំណង: បង្កើតក្របខ័ណ្ឌគ្រប់គ្រងដើម្បីផ្តួចផ្តើម និងត្រួតពិនិត្យការអនុវត្ត និងប្រតិបត្តិការប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និងសុវត្ថិភាពព័ត៌មាននៅក្នុងអង្គភាព។

ចំណុចគួរពិចារណាអនុវត្ត÷

- កំណត់ និងរៀបចំរចនាសម្ព័ន្ធស្ថាប័ន
- បង្កើតតួនាទី និងការទទួលខុសត្រូវ
- កំណត់ព័ត៌មាន (ទិន្នន័យ) និងម្ចាស់ប្រព័ន្ធ ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

៣.ការគ្រប់គ្រងធនធានបច្ចេកវិទ្យាព័ត៌មាន (មនុស្ស ជំនាញ និងសមត្ថភាព)

គោលបំណង:ដើម្បីកំណត់បាននូវ÷

- ជំនាញ និងសមត្ថភាពដែលត្រូវការដើម្បីសម្រេចបាននូវគោលបំណងពាក់ព័ន្ធ
- បុគ្គលិក និងអ្នកម៉ៅការត្រូវមានសមត្ថភាព ជំនាញ និងបទពិសោធន៍ដើម្បីបំពេញតួនាទី និងការទទួលខុសត្រូវរបស់ខ្លួន
- ទីប្រឹក្សា និងបុគ្គលិកកិច្ចសន្យា យល់ដឹង និងគោរពតាមគោលនយោបាយរបស់អង្គភាព និងបំពេញតាមតម្រូវការកិច្ចសន្យាដែលបានព្រមព្រៀង។ ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

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

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

៤. ការគ្រប់គ្រងអ្នកផ្គត់ផ្គង់ និងកិច្ចព្រមព្រៀងសេវាកម្ម

គោលបំណង: ផលិតផល និងសេវាកម្មប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានផ្តល់ជូនដោយអ្នកផ្គត់ផ្គង់គ្រប់ប្រភេទដល់អង្គភាព÷

- ត្រូវបំពេញតាមតម្រូវការរបស់អង្គភាព
- កាត់បន្ថយហានិភ័យដែលអ្នកផ្គត់ផ្គង់មិនអាចអនុវត្ត ឬមិនគោរពតាមកិច្ចសន្យា
- ព្រមទាំងធានាតម្លៃប្រកួតប្រជែង។ ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

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

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

៥.ការគ្រប់គ្រងហានិភ័យ

គោលបំណង:ដើម្បីកំណត់អត្តសញ្ញាណ វាយតម្លៃ កាត់បន្ថយហានិភ័យប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានជាប្រចាំក្នុងកម្រិតទទួលយកបានដែលកំណត់ដោយអ្នកគ្រប់គ្រងអង្គភាព។

ចំណុចគួរពិចារណាអនុវត្ត÷

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

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

៦.ប្រព័ន្ធគ្រប់គ្រងសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន (បគសប)

គោលបំណង: គឺដើម្បីអាចកំណត់បាននូវ÷

- កំណត់ដំណើរការ និងត្រួតពិនិត្យប្រព័ន្ធគ្រប់គ្រងសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន។
- រក្សាផលប៉ះពាល់ និងការកើតឡើងនៃឧប្បត្តិហេតុសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មានក្នុងកម្រិតនៃហានិភ័យអាចទទួលបានដោយអង្គភាព។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

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

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

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

៧. សុវត្ថិភាពទិន្នន័យ

គោលបំណង: ធានាបាននូវ÷

- សុចរិតភាពការចម្លងទុក និងភាពស៊ីសង្វាក់គ្នានៃទិន្នន័យទាំងអស់ដែលត្រូវបានរក្សាទុកជាទម្រង់អេឡិចត្រូនិក ដូចជាមូលដ្ឋានទិន្នន័យ ឃ្លាំងទិន្នន័យ បណ្ណសារទិន្នន័យ
- សម្រេចបាន និងទ្រទ្រង់ការគ្រប់គ្រងប្រកបដោយប្រសិទ្ធភាពលើការរៀបចំទ្រព្យសម្បត្តិទិន្នន័យ តាមវដ្តទិន្នន័យ ចាប់តាំងពីការបង្កើតរហូតដល់ការចែកចាយ ការថែរក្សា និងការរក្សាទុកបណ្ណសារ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

- រៀបចំយុទ្ធសាស្ត្រគ្រប់គ្រងទិន្នន័យ/ចំណាត់ថ្នាក់ទិន្នន័យ តួនាទី និងការទទួលខុសត្រូវរបស់អង្គភាព
- គ្រប់គ្រងលើការចម្លងទុកទិន្នន័យ និងរៀបចំការស្តារឡើងវិញ
- កំណត់ការរក្សាទុកបណ្ណសារ ការកាក់ទុក ការគ្រប់គ្រងឧបករណ៍ចម្លងទុក ការជម្រះ និងការបញ្ជូនទិន្នន័យ
- ប្រព័ន្ធត្រួតពិនិត្យរឹងមាំលើការពារការផ្លាស់ប្តូរកូដរបស់កម្មវិធីស្រេច និងទិន្នន័យប្រតិបត្តិការផលិតកម្ម ដោយគ្មានការអនុញ្ញាត (ឧ.ការត្រួតពិនិត្យសុចរិតភាព គ្រីបតូក្រាហ្វិច...)។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

៨.ការទិញ ការអភិវឌ្ឍ និងការថែរក្សាប្រព័ន្ធ

គោលបំណង: ការអភិវឌ្ឍគម្រោង និងការគ្រប់គ្រងសេវាកម្មដ៏រឹងមាំ គឺចាំបាច់សម្រាប់ការគាំទ្រដល់÷

- ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន
- សេវាកម្ម និងប្រតិបត្តិការ
- ការគ្រប់គ្រងការផ្លាស់ប្តូរ
- ឧប្បត្តិហេតុក៏ដូចជាធានាស្ថិរភាពបរិស្ថានប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន។

២.៦.វចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

វដ្តនៃការអភិវឌ្ឍប្រព័ន្ធ រួមមាន÷

- ការសិក្សាសមិទ្ធិលទ្ធភាព
- តម្រូវការ
- ការជ្រើសរើសប្រព័ន្ធ ការទិញ និងការតាក់តែង
- ការរៀបតម្រូវ/ការអភិវឌ្ឍ
- ការធ្វើតេស្តចុងក្រោយ និងការដាក់អនុវត្ត
- ការពិនិត្យឡើងវិញក្រោយការដាក់អនុវត្ត

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

៩.ការគ្រប់គ្រងលទ្ធភាពប្រើប្រាស់បាន និងសមត្ថភាព

គោលបំណង:

- ធ្វើឱ្យមានតុល្យភាពនៃតម្រូវការលើភាពអាចប្រើប្រាស់បាន ដំណើរការ និងសមត្ថភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន នាពេលបច្ចុប្បន្ន និងអនាគត ប្រកបដោយភាពសមនឹងតម្លៃ
- រក្សានូវភាពអាចប្រើប្រាស់បាននៃសេវាកម្មការគ្រប់គ្រងធនធានប្រកបដោយប្រសិទ្ធភាព និងការធ្វើឱ្យប្រសើរឡើងនូវដំណើរការប្រព័ន្ធ។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

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

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១០. ការគ្រប់គ្រងលើការផ្លាស់ប្តូរប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

គោលបំណង: រាល់ការផ្លាស់ប្តូរជាធម្មតា និងបន្ទាន់នៃដំណើរការធុរកិច្ច កម្មវិធីស្រេច និងហេដ្ឋារចនាសម្ព័ន្ធមានការគ្រប់គ្រង និងប្រព័ន្ធត្រួតពិនិត្យត្រឹមត្រូវ ដើម្បីផ្តល់នូវភាពរហ័ស និងអាចជឿទុកចិត្តបាន។

ចំណុចគួរពិចារណាអនុវត្ត÷

- គោលនយោបាយ និងនីតិវិធីគ្រប់គ្រងការផ្លាស់ប្តូរ
- វាយតម្លៃផលប៉ះពាល់នៃការផ្លាស់ប្តូរ ការផ្តល់អាទិភាព និងការអនុញ្ញាតលើការផ្លាស់ប្តូរ
- ធ្វើតេស្តសាកល្បងរាល់ការផ្លាស់ប្តូរ មុនពេលដាក់អនុវត្ត និងមានផែនការត្រលប់ក្រោយ
- គ្រប់គ្រងលើការផ្លាស់ប្តូរបន្ទាន់ ដើម្បីកាត់បន្ថយឧប្បត្តិហេតុ បន្ទាប់មកវាយតម្លៃ និងអនុម័តរាល់ការផ្លាស់ប្តូរដែលបានអនុវត្តរួច ។ល។

២.៦.វចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១១. ការយល់ដឹង និងការបណ្តុះបណ្តាលដល់អ្នកប្រើប្រាស់

គោលបំណង: បុគ្គលិកទាំងអស់របស់អង្គភាព និងអ្នកពាក់ព័ន្ធទទួលបាននូវ÷

- ការអប់រំ និងការបណ្តុះបណ្តាលគ្រប់គ្រាន់សមស្របជាប្រចាំលើគោលនយោបាយ និងនីតិវិធីពាក់ព័ន្ធនឹងមុខងារភារកិច្ចរបស់ខ្លួន
- ស្វែងយល់លើសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ការគំរាមកំហែង ភាពងាយរងគ្រោះ ឬក្របខ័ណ្ឌសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់អង្គភាព។ ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

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

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១២. វដ្តនៃទ្រព្យសកម្មព័ត៌មាន

គោលបំណង: គ្រប់គ្រងទ្រព្យសកម្មព័ត៌មាន របស់អង្គភាព ដើម្បីប្រាកដថាការប្រើប្រាស់ទ្រព្យសកម្មព័ត៌មានផ្តល់នូវ÷

- តម្លៃដ៏ប្រសើរ
- ភាពអាចដំណើរការ (ស្របតាមគោលបំណង)
- ថែរក្សាការពារដោយការទទួលខុសត្រូវ។

សុវត្ថិភាពព័ត៌មានចាំបាច់ត្រូវបានពិចារណានៅគ្រប់ដំណាក់កាលនៃវដ្តទ្រព្យសម្បត្តិព័ត៌មានដូចជាការធ្វើផែនការ ការគាក់តែងការទិញ ការចាត់ចំណាត់ថ្នាក់ ការអនុវត្ត ការថែរក្សាការពារ និងការជម្រះ។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

- កំណត់ និងកត់ត្រាទ្រព្យសកម្មព័ត៌មានទាំងអស់ (បញ្ជីរសារពើភ័ណ្ឌទ្រព្យសកម្មព័ត៌មាន) ដូចជាអត្តសញ្ញាណ /យថាប្រភេទ ច្បាស់លាស់ តម្លៃធៀប ទីតាំង សុវត្ថិភាព/ចំណាត់ថ្នាក់ហានិភ័យ ម្ចាស់ និងអ្នកថែទាំ
- គ្រប់គ្រងវដ្តទ្រព្យសកម្មចាប់ពីការធ្វើលទ្ធកម្មរហូតដល់ការជម្រះ
- ពិនិត្យឡើងវិញជាប្រចាំលើទ្រព្យសម្បត្តិដែលមានដើម្បីកំណត់វិធីធ្វើឱ្យកាន់តែមានប្រសិទ្ធភាពស្របតាមតម្រូវការធុរកិច្ច
- គ្រប់គ្រងអាជ្ញាប័ណ្ណកម្មវិធីដើម្បីរក្សាបានចំនួនអាជ្ញាប័ណ្ណសម្រាប់គាំទ្រតម្រូវការធុរកិច្ច ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១៣. ការគ្រប់គ្រងប្រតិបត្តិការប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន

គោលបំណង: សម្របសម្រួល និងអនុវត្តនីតិវិធីប្រតិបត្តិការស្តង់ដារបានកំណត់ និងសកម្មភាពតាមដាននានា ការផ្តត់ផ្តង់ផលិតផល និងសេវាកម្មប្រតិបត្តិការបច្ចេកវិទ្យាព័ត៌មានតាមការគ្រោងទុក។

ចំណុចគួរពិចារណាអនុវត្ត÷

- រៀបចំនីតិវិធីប្រតិបត្តិការសម្រាប់អង្គភាព
- អនុវត្តកិច្ចការស្របតាមនីតិវិធីប្រកបដោយសង្គតិភាព
- គ្រប់គ្រងការផ្តល់សេវាកម្មបច្ចេកវិទ្យាព័ត៌មានពីប្រភពខាងក្រៅ ដើម្បីធានាភាពជឿជាក់បាន និងការពារព័ត៌មាន
- ត្រួតពិនិត្យហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និងព្រឹត្តិការណ៍ពាក់ព័ន្ធ (ឧ. កំណត់ហេតុ គន្លងសវនកម្ម...)
- គ្រប់គ្រងវិធានការដើម្បីទប់ស្កាត់ផលប៉ះពាល់ដែលបណ្តាលមកពីបរិស្ថានជុំវិញ (ឧ. ឧបករណ៍ដើម្បីតាមដាន និងត្រួតពិនិត្យ...) ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១៤.ការគ្រប់គ្រងលើសំណើសុំសេវាកម្ម

គោលបំណង: ឆ្លើយតបទាន់ពេលវេលា និងមានប្រសិទ្ធភាពចំពោះសំណូមពរអ្នកប្រើប្រាស់ និងផ្តល់ការដោះស្រាយរាល់ការស្នើសុំគ្រប់ប្រភេទតាមរយៈ÷

- ការផ្តល់សេវាកម្មឡើងវិញជាធម្មតា
- ការស៊ើបអង្កេត
- ការវិនិច្ឆ័យ
- ការបញ្ជូនបន្ត
- ការដោះស្រាយ
- ការបំពេញតាមសំណើរបស់អ្នកប្រើប្រាស់ ព្រមទាំងមានការកត់ត្រាត្រឹមត្រូវ។ ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

- គោលការណ៍ណែនាំ ឬនិតិធីក្នុងការស្នើសុំ
- កំណត់ចំណាត់ថ្នាក់សំណើសេវាកម្មទៅតាមប្រភេទ
- ផ្ទៀងផ្ទាត់ អនុម័ត និងបំពេញតាមការស្នើសុំសេវាកម្មទៅតាមអាទិភាព
- បិទសំណើសុំសេវាកម្ម (ផ្ទៀងផ្ទាត់ភាពពេញចិត្តលើការបំពេញតាមសំណើ និងបិទបញ្ចប់)
- កត់ត្រារាល់ការស្នើសុំ ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១៥.ការគ្រប់គ្រងឧប្បត្តិហេតុ

គោលបំណង: ឆ្លើយតបទាន់ពេលវេលា និងមានប្រសិទ្ធភាពចំពោះឧប្បត្តិហេតុប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានដូចជា÷

- ការប្រើប្រាស់ទ្រព្យសកម្មព័ត៌មាន ដោយមិនត្រឹមត្រូវ
- ការបង្ហាញព័ត៌មាន ឬព្រឹត្តិការណ៍ដែលគំរាមកំហែងដល់ដំណើរការធុរកិច្ច។

ជាទូទៅប្រភេទឧប្បត្តិហេតុអាចមានដូចជា ÷

- ផ្នែករឹងនិង ផ្នែកទន់
- សុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

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

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១៦.ការគ្រប់គ្រងនិរន្តរភាពបច្ចេកវិទ្យាព័ត៌មាន

គោលបំណង: បង្កើត និងថែរក្សាផែនការនិរន្តរភាពបច្ចេកវិទ្យាព័ត៌មានដើម្បីឱ្យអង្គភាពអាចឆ្លើយតបទៅនឹងឧប្បត្តិហេតុ ឬគ្រោះមហន្តរាយ និងដោះស្រាយបានឆាប់រហ័សចំពោះការរំខាន ក៍ដូចជាដើម្បីឱ្យមាននិរន្តរភាពដំណើរការប្រតិបត្តិការធុរកិច្ច និងសេវាកម្មបច្ចេកវិទ្យាព័ត៌មានសំខាន់ៗ។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ចំណុចគួរពិចារណាអនុវត្ត÷

- រៀបចំគោលនយោបាយនិរន្តរភាពធុរកិច្ច
- បង្កើត និងអនុវត្តសាកល្បងផែនការនិរន្តរភាពធុរកិច្ច និងផែនការស្តារពីគ្រោះមហន្តរាយ
- ត្រួតពិនិត្យឡើងវិញ និងកែលម្អផែនការនិរន្តរភាពធុរកិច្ច ដើម្បីធានាបាននូវភាពសមស្រប ភាពគ្រប់គ្រាន់ និងប្រសិទ្ធភាព
- បណ្តុះបណ្តាលអំពីនីតិវិធី ភារកិច្ច និងការទទួលខុសត្រូវដើម្បីឆ្លើយតបទៅនឹងគ្រោះមហន្តរាយ
- រៀបចំការគ្រប់គ្រងលើការចម្លងទុក
- ពិនិត្យឡើងវិញលើផែនការនិរន្តរភាពធុរកិច្ច និងផែនការស្តារពីគ្រោះមហន្តរាយ ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១៧.គ្រប់គ្រងសុវត្ថិភាពសេវាកម្ម

គោលបំណង: កាត់បន្ថយផលប៉ះពាល់ពីភាពងាយរងគ្រោះ និងឧប្បត្តិហេតុសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន។

ចំណុចគួរពិចារណាអនុវត្ត÷

- គោលនយោបាយសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន
- គ្រប់គ្រងសុវត្ថិភាពបណ្តាញ និងការតភ្ជាប់
- គ្រប់គ្រងអត្តសញ្ញាណអ្នកប្រើប្រាស់ និងការគ្រប់គ្រងការចូលប្រើប្រាស់
- ធ្វើបច្ចុប្បន្នភាពកម្មវិធីសុវត្ថិភាពប្រព័ន្ធប្រតិបត្តិការ កម្មវិធីកំចាត់មេរោគ ឬកម្មវិធីអាក្រក់ផ្សេងៗ
- គ្រប់គ្រងភាពងាយរងគ្រោះ និងត្រួតពិនិត្យហេដ្ឋារចនាសម្ព័ន្ធពាក់ព័ន្ធសុវត្ថិភាព
- គ្រប់គ្រងការចូលប្រើប្រាស់រួបរួនលើទ្រព្យសកម្មព័ត៌មាន ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ខ. ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេច

គោលការណ៍ប្រព័ន្ធត្រួតពិនិត្យ: កម្មវិធីស្រេចនីមួយៗ ត្រូវមានប្រព័ន្ធត្រួតពិនិត្យដែលរឹងមាំ និងគ្រប់គ្រាន់ ដើម្បីធានាថា÷

- រាល់ទិន្នន័យបានបញ្ចូលទាំងអស់គឺពេញលេញ សុក្រឹតភាព និងបានអនុញ្ញាតត្រឹមត្រូវ
- រាល់ទិន្នន័យបានដំណើរការតាមការរំពឹងទុក
- ទិន្នន័យដែលបានរក្សាទុកទាំងអស់ គឺត្រឹមត្រូវ និងពេញលេញ
- ធាតុចេញទាំងអស់ គឺត្រឹមត្រូវ និងពេញលេញ
- កំណត់ត្រាត្រូវបានរក្សាទុកដើម្បីតាមដានដំណើរការទិន្នន័យ ចាប់ពីការបញ្ចូល ការរក្សាទុក និងលទ្ធផលចុងក្រោយ ។ល។

ប្រព័ន្ធត្រួតពិនិត្យកម្មវិធីស្រេចត្រូវមាននៅតាមផ្នែកដូចខាងក្រោម÷

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

១. ប្រព័ន្ធត្រួតពិនិត្យលើធាតុចូល

គោលបំណង: ដើម្បីធានាបាននូវ÷

- ភាពពេញលេញ
- សុក្រឹតភាព
- ការបានអនុញ្ញាតត្រឹមត្រូវនៃទិន្នន័យដែលបានបញ្ចូលក្នុងកម្មវិធីស្រេច។

២.៦.វចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

ប្រព័ន្ធត្រួតពិនិត្យលើធាតុចូលរួមមាន÷

- **ប្រព័ន្ធត្រួតពិនិត្យលើការចូលប្រើ:**
  - ការអនុញ្ញាត: រាល់ការបង្កើតគណនី ពាក្យសម្ងាត់អ្នកប្រើប្រាស់ ការអនុញ្ញាត ការបែងចែកតួនាទី ឬការកំណត់សិទ្ធិ ត្រូវអនុលោមតាមគោលនយោបាយ និងនីតិវិធីរបស់អង្គភាព
  - ការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវ: គួរប្រើគណនីចូលប្រើប្រាស់ ពាក្យសម្ងាត់ លេខកូដផ្ទៀងផ្ទាត់ ហត្ថលេខាឌីជីថល ក្រយៅដៃ ...
- **ភាពពេញលេញនៃការបញ្ចូលទិន្នន័យ:** គួរមានការឆែកលើភាពសមហេតុផល និងកម្រិតកំណត់នៃតម្លៃហិរញ្ញវត្ថុ លើទម្រង់ និងប្រឡង់ចាំបាច់ លើលំដាប់ លើចន្លោះ លើចំនួនតួលេខ និងផ្ទៀងផ្ទាត់...
- **ដំណើរការបញ្ចូលទិន្នន័យមិនទាន់រួចរាល់:** គួរមានការត្រួតពិនិត្យលើប្រតិបត្តិការដែលមិនទាន់បញ្ចប់រួចរាល់ ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

២.ប្រព័ន្ធត្រួតពិនិត្យលើដំណើរការ

គោលបំណង: ដើម្បីធានាថា÷

- ដំណើរការប្រតិបត្តិការគឺមានភាពសុក្រិត និងពេញលេញ
- ប្រតិបត្តិការត្រូវបានកត់ត្រាទៅគណនីត្រឹមត្រូវ និងទាន់ពេលវេលាកំណត់
- ប្រតិបត្តិការគឺមានតែមួយ (គ្មានការស្ទួនគ្នា) ។ល។

ប្រព័ន្ធត្រួតពិនិត្យលើដំណើរការរួមមាន÷

- **តុល្យភាពរវាងសន្ធានកម្ម:** ផ្ទៀងផ្ទាត់ដោយស្វ័យប្រវត្តិលើភាពដូចគ្នានៃទិន្នន័យប្រព័ន្ធដើមជាមួយប្រព័ន្ធគោលដៅ ករណីទិន្នន័យមិនដូចគ្នាគួរអោចទាញជារបាយការណ៍ដើម្បីត្រួតពិនិត្យបន្ថែម
- **ការត្រួតពិនិត្យលើការស្ទួន:** ផ្ទៀងផ្ទាត់ដោយស្វ័យប្រវត្តិលើភាពស្ទួនគ្នានៃប្រតិបត្តិការដែលបានកត់ត្រា ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

៣.ប្រព័ន្ធត្រួតពិនិត្យលើធាតុចេញ

គោលបំណង: ដើម្បីធានាថាធាតុចេញអាចទាញពីប្រព័ន្ធតាមតម្រូវការ ទាន់ពេលវេលា ត្រឹមត្រូវ អាចផ្ទៀងផ្ទាត់បានជាមួយទិន្នន័យដែលបានបញ្ចូល រក្សាការសម្ងាត់ ហើយរាល់កំហុស និងបញ្ហាត្រូវបានកត់ត្រាដោយប្រព័ន្ធព្រមទាំងមានការស៊ើបអង្កេត និងវិធានការដោះស្រាយត្រឹមត្រូវ។

ប្រព័ន្ធត្រួតពិនិត្យលើធាតុចេញរួមមាន÷

- **Output error handling:** រាល់បញ្ហា ឬកំហុសត្រូវបានកត់ត្រាដោយប្រព័ន្ធ និងអាចទាញយកមកពិនិត្យឡើងវិញដោយអ្នកទទួលខុសត្រូវ
- **Distribution of reports:** មានតែអ្នកប្រើប្រាស់ដែលមានការអនុញ្ញាតអាចចូលទាញយក ឬមើលរបាយការណ៍
- **Accuracy and Completeness of output:** ផ្ទៀងផ្ទាត់របាយការណ៍មានតុល្យភាព និងសមស្រប, ពិនិត្យលើកាលវិភាគអំពីការផលិត ភាពញឹកញាប់ ការចែកចាយនៃធាតុចេញទាំងអស់ និងពិនិត្យលើធាតុចេញ។ល។

២.៦.រចនាសម្ព័ន្ធប្រព័ន្ធត្រួតពិនិត្យបច្ចេកវិទ្យាព័ត៌មាន (ត)

៤.ប្រព័ន្ធត្រួតពិនិត្យលើសុចរិតភាព

គោលបំណង: ដើម្បីធានាថាទិន្នន័យមេ និងទិន្នន័យនៃប្រតិបត្តិការកំពុងដំណើរការមានសង្គតិភាព និងសុចរិតភាព ហើយនៅមុនរាល់ការកែប្រែ ឬផ្លាស់ប្តូរ ត្រូវមានការអនុញ្ញាតត្រឹមត្រូវ។

៥. ការគ្រប់គ្រងលើគន្លងសវនកម្ម

គោលបំណង: ដើម្បីអាចតាមដានន្ទវដំណើរការរបស់ប្រតិបត្តិការចាប់ពីដើមដំបូងដល់លទ្ធផលចុងក្រោយ ព្រមទាំងអាចផ្ទៀងផ្ទាត់ជាមួយអត្តសញ្ញាណប្រតិបត្តិការ និងព្រឹត្តិការណ៍។

ប្រព័ន្ធត្រួតពិនិត្យរួមមាន÷

- ត្រូវមានការតាមដានដោយស្វ័យប្រវត្តិលើការផ្លាស់ប្តូរ និងការបំពានដំណើរការទិន្នន័យ ដោយរំលេចអត្តសញ្ញាណអ្នកធ្វើការផ្លាស់ប្តូរ ឬបំពាន
- ត្រូវមានការគ្រប់គ្រងលើសុវត្ថិភាពគន្លងសវនកម្ម ។ល។

៣. ការតាមដានលើប្រព័ន្ធត្រួតពិនិត្យ

គោលការណ៍ត្រួតពិនិត្យ: ប្រព័ន្ធត្រួតពិនិត្យរបស់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន គឺជាកម្មវត្ថុនៃការពិនិត្យតាមដានបន្ត។

ការតាមដាន គឺជាដំណើរការនៃការវាយតម្លៃលើការតាក់តែង និងការប្រតិបត្តិនៃប្រព័ន្ធត្រួតពិនិត្យក្នុងពេលវេលាសមស្រប និងមានវិធានការតាមការចាំបាច់។ ការតាមដាននេះត្រូវអនុវត្តដោយមន្ត្រីទទួលបន្ទុកលើគ្រប់សកម្មភាពនៅក្នុងអង្គភាព និងពេលខ្លះជាមួយភាគីកិច្ចសន្យាខាងក្រៅផងដែរ។

៣. ការតាមដានលើប្រព័ន្ធត្រួតពិនិត្យ (ត)

ការតាមដានអាចអនុវត្តបានតាមពីររបៀប÷

- **សកម្មភាពជាប្រចាំ:** សំដៅដល់សកម្មភាពតាមដានប្រសិទ្ធភាពនៃប្រព័ន្ធត្រួតពិនិត្យនៃប្រតិបត្តិការជាធម្មតា ដូចជាសកម្មភាពត្រួតពិនិត្យ និងគ្រប់គ្រងជាទៀងទាត់របស់ថ្នាក់ដឹកនាំ ការប្រៀបធៀប ការផ្គងផ្គង និងសកម្មភាពជាប្រចាំផ្សេងៗទៀត (ខ. ការប្រៀបធៀបទិន្នន័យដែលបានកត់ត្រាដោយប្រព័ន្ធ និងជាក់ស្តែងនៅខាងក្រៅ)
- **ការវាយតម្លៃដោយឡែក:** សំដៅដល់ការវាយតម្លៃលើប្រព័ន្ធត្រួតពិនិត្យដោយថ្នាក់ដឹកនាំ និង/ឬដោយសវនកម្មផ្ទៃក្នុង។ ប្រព័ន្ធត្រួតពិនិត្យទាក់ទងនឹងហានិភ័យកម្រិតខ្ពស់និងសំខាន់ ទាមទារនូវការតាមដានវាយតម្លៃឱ្យបានញឹកញាប់។

សូមអរគុណ !