ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ធនាគារជាតិ នៃ កម្ពុជា

លេខ..ធ៧..០៨...០៨៩...ជ.ក.

លិខិតចូល
ថ្ងៃទី...ខែ...ឆ្នាំ20..

ប្រកាស
ស្តីពី
ការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម

ទេសាភិបាល ធនាគារជាតិនៃកម្ពុជា

- បានឃើញរដ្ឋធម្មនុញ្ញនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រមលេខ នស/រកម/០១៩៦/ ២៧ ចុះថ្ងៃទី២៦ ខែមករា ឆ្នាំ១៩៩៦ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃធនាគារជាតិនៃកម្ពុជា
- បានឃើញព្រះរាជក្រមលេខ នស/រកម/១១៩៩/ ១៣ ចុះថ្ងៃទី១៨ ខែវិច្ឆកា ឆ្នាំ១៩៩៩ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ
- បានឃើញព្រះរាជក្រម នស/រកម/០៦០៧/០១៤ ចុះថ្ងៃទី២៤ ខែមិថុនា ឆ្នាំ២០០៧ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីការប្រឆាំងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកត/០៥០៨/៥២៦ ចុះថ្ងៃទី១៣ ខែឧសភា ឆ្នាំ២០០៨ ស្តីពីការតែងតាំង **ឯកឧត្តម ជា ចាន់តូ** ជាអគ្គទេសាភិបាលនៃធនាគារជាតិនៃកម្ពុជា មានឋានៈស្មើទេសរដ្ឋមន្ត្រី
- យោងតាមសំណើរបស់អគ្គនាយកដ្ឋាន
- យោងតាមស្មារតីនៃអង្គប្រជុំថ្នាក់ដឹកនាំធនាគារជាតិនៃកម្ពុជា ថ្ងៃទី២៧ ខែឧសភា ឆ្នាំ២០០៨

ស ម្រេ ច

ប្រការ ១.- ដែនកំណត់

សម្រាប់គោលបំណងនៃប្រកាសនេះ ពាក្យថា "គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ" គឺសំដៅចំពោះ គ្រឹះស្ថាន និង វិជ្ជាជីវៈដូចខាងក្រោម ដែលស្ថិតក្រោមការគ្រប់គ្រងរបស់ធនាគារជាតិនៃកម្ពុជា ហើយត្រូវបានហៅថា "បុគ្គលរាយការណ៍ " នៅក្នុងច្បាប់ស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ÷

ក) ធនាគារ រួមទាំងសាខាធនាគារបរទេស

ខ) គ្រឹះស្ថានមីក្រូហិរញ្ញវត្ថុ

គ) សហករណ៍ឥណទាន

ឃ) ក្រុមហ៊ុនភតិសន្យា

ង) បញ្ជូរប្តូរប្រាក់/អ្នកប្តូរប្រាក់

ច) សេវាផ្ទេរប្រាក់

ឆ) ឈ្មួញលោហធាតុ និងត្បូងថ្មមានតម្លៃ

ជ) គ្រឹះស្ថាន ឬវិជ្ជាជីវៈដទៃទៀតដែលកំណត់ដោយអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ត្រូវស្ថិតនៅក្នុងដែនអនុវត្ត នៃច្បាប់ស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម និង ក្រោមការគ្រប់គ្រងរបស់ធនាគារជាតិនៃកម្ពុជា ។

ប្រការ ២.- គោលការណ៍ទទួលស្គាល់អតិថិជន

គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបង្កើតគោលការណ៍ និងនីតិវិធីទទួលស្គាល់អតិថិជន ហើយត្រូវមានវិធានការសមស្រប រួមមាន សាវតារហានិភ័យនៅក្នុងគោលការណ៍ និងនីតិវិធីផ្ទៃក្នុងរបស់ខ្លួនដើម្បីកំណត់ហានិភ័យផ្សេងៗ ដែលបានបង្កើតឡើងដោយប្រភេទនៃអតិថិជននីមួយៗ ឬអតិថិជនជារូបវន្តបុគ្គលនីមួយៗ ។

ប្រការ ៣.- ការកំណត់សាវតារហានិភ័យ

៣.១ ក្នុងការកំណត់សាវតារហានិភ័យតាមប្រភេទអតិថិជននីមួយៗ ឬតាមអតិថិជនជារូបវន្តបុគ្គលនីមួយៗ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ យ៉ាងហោចណាស់ ត្រូវយកចិត្តទុកដាក់ទៅលើកត្តាមួយចំនួន ដូចខាងក្រោម ÷

- ប្រភពដើមរបស់អតិថិជន និងទីតាំងអាជីវកម្ម
- សាវតារ និងបុគ្គលិកលក្ខណៈពិសេសរបស់អតិថិជន
- លក្ខណៈអាជីវកម្មរបស់អតិថិជន
- រចនាសម្ព័ន្ធកម្មសិទ្ធិសម្រាប់អតិថិជនជាក្រុមហ៊ុន និង
- ព័តិមានផ្សេងៗ ដែលអាចបញ្ជាក់ថា អតិថិជនមានហានិភ័យខ្ពស់ ។

៣.២ បន្ទាប់ពីទទួលស្គាល់អតិថិជនជាលើកដំបូង គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវតាមដានសកម្មភាពគណនីអតិថិជនជាប្រចាំ ដើម្បីធានាថាសកម្មភាពគណនីនេះស្របទៅនឹងសាវតារអតិថិជន ។ ក្នុងករណីមានភាពមិនស្របគ្នា គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវវាយតម្លៃឡើងវិញថា ជាអតិថិជនមានហានិភ័យខ្ពស់ ។

ប្រការ ៤.- ការហាមឃាត់គណនីអនាមិក និងគណនីបតិជ្ញកម្ម

គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវធានាថា ការបើកគណនីត្រូវតែមានឈ្មោះម្ចាស់គណនី និងត្រូវរក្សាទុកឈ្មោះម្ចាស់គណនីគ្រប់ពេលទាំងអស់ ។ លើសពីនេះ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ត្រូវសំគាល់អត្តសញ្ញាណអតិថិជនដូចមានចែងនៅក្នុងប្រការ ៦ និង ៧ នៃប្រកាសនេះ ហើយត្រូវធានាថា គ្មានអតិថិជនណាម្នាក់ត្រូវបានអនុញ្ញាតឱ្យបើក ឬ ធ្វើប្រតិបត្តិការគណនីណាមួយដែលមានឈ្មោះប្រឌិត មិនត្រឹមត្រូវ ឬក្លែងក្លាយ ។

ប្រការ ៥.- ការយកចិត្តទុកដាក់ស្គាល់អតិថិជន

៥.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជន និង ទាមទារឱ្យមានភស្តុតាងគ្រប់គ្រាន់ ព្រមទាំងកត់ត្រាទុកឱ្យបានត្រឹមត្រូវនូវអត្តសញ្ញាណ និងលក្ខណៈគតិយុត្តរបស់បុគ្គលដែលស្នើសុំធ្វើប្រតិបត្តិការ ។ ភស្តុតាងទាំងនេះ ត្រូវតែជាឯកសារដែលអាចជឿជាក់បាន ។

៥.២ ការយកចិត្តទុកដាក់ស្គាល់អតិថិជនត្រូវធ្វើឡើង នៅពេលដែល÷

- បង្កើតទំនាក់ទំនងអាជីវកម្មជាមួយអតិថិជន ដូចជា ការបើកគណនី ការផ្តល់សេវាប្រអប់សុវត្ថិភាព ឬ ការចុះកិច្ចសន្យាអាជីវកម្មផ្សេងទៀត
- អនុវត្តប្រតិបត្តិការដែលកើតឡើងតែមួយដង ឬម្តងម្កាលដែលមានទឹកប្រាក់លើសពី ១០.០០០ ដុល្លារអាមេរិក (៤០ លានរៀល ឬសមមូលនឹងរូបិយប័ណ្ណផ្សេងទៀត) ឬការផ្ទេរតាមប្រព័ន្ធអេឡិចត្រូនិកដែលមានទឹកប្រាក់លើសពី ១.០០០ ដុល្លារអាមេរិក (៤ លានរៀល ឬសមមូលនឹងរូបិយប័ណ្ណផ្សេងទៀត)
- គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុសង្ស័យថា ជាការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ឬ
- គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុសង្ស័យពីភាពត្រឹមត្រូវ ឬភាពគ្រប់គ្រាន់នៃព័ត៌មានដែលបានទទួលកន្លងមក ។

៥.៣ ក្នុងការអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជន គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ យ៉ាងហោចណាស់ត្រូវ÷

- សំគាល់អត្តសញ្ញាណ និង ផ្ទៀងផ្ទាត់បុគ្គលដែលអនុវត្តប្រតិបត្តិការដោយប្រើប្រាស់ប្រភពឯកសារ ទិន្នន័យ ឬ ព័ត៌មានដែលឯករាជ្យ និងអាចជឿជាក់បានយោងតាមប្រការ ៦ ឬ ៧ នៃ ប្រកាសនេះ
- កំណត់ថា អតិថិជនកំពុងធ្វើប្រតិបត្តិការជំនួសបុគ្គល ឬអត្តគាហកណាមួយ
- ស្វែងយល់ពីអត្តគាហក និងរចនាសម្ព័ន្ធត្រួតពិនិត្យរបស់អតិថិជន ។ អត្តគាហកត្រូវបានផ្តល់ និយមន័យនៅក្នុងប្រការ ៨ នៃប្រកាសនេះ
- ប្រមូលព័ត៌មានស្តីពីគោលបំណង និងលក្ខណៈនៃទំនាក់ទំនងអាជីវកម្ម និង

- អនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជន និងពិនិត្យពិច័យជាបន្តបន្ទាប់ដើម្បីធានាថា ព័ត៌មានដែលបាន ទទួល ត្រូវបានធ្វើបច្ចុប្បន្នកម្ម និងសមស្របជាមួយចំណេះដឹងរបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ អំពី អាជីវកម្ម និងសាវតារហានិភ័យរបស់អតិថិជន និងប្រសិនបើចាំបាច់ ត្រូវដឹងពីប្រភពមូលនិធិ ។

៥.៤ ការបដិសេធរបស់អតិថិជនក្នុងការផ្តល់ព័ត៌មាន និងមិនសហការក្នុងដំណើរការយកចិត្តទុកដាក់ស្គាល់ អតិថិជនរបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ អាចចាត់ទុកជាការសង្ស័យ ។

៥.៥ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុមិនត្រូវបើកគណនី ផ្តើមទំនាក់ទំនងអាជីវកម្ម ឬធ្វើប្រតិបត្តិការ ឬ ក្នុងករណីដែលទំនាក់ទំនងអាជីវកម្មមានស្រាប់ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបញ្ឈប់ទំនាក់ទំនងទាំងនោះ ប្រសិនបើ អតិថិជនមិនអនុវត្តតាមការតម្រូវនៃការយកចិត្តទុកដាក់ស្គាល់អតិថិជន ។ ស្ថានការណ៍បែបនេះ ត្រូវកត់ត្រាក្នុង របាយការណ៍ប្រតិបត្តិការសង្ស័យដែលត្រូវផ្ញើជូនអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ។

ប្រការ ៦._ អតិថិជនជាឯកត្តបុគ្គល

៦.១ ក្នុងការបង្កើតទំនាក់ទំនងអាជីវកម្មជាមួយអតិថិជនជាឯកត្តបុគ្គល គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវ ប្រមូលព័ត៌មាន ដូចជា ឈ្មោះ ថ្ងៃខែឆ្នាំកំណើត លេខអត្តសញ្ញាណប័ណ្ណ លេខលិខិតឆ្លងដែន លេខយោងឯកសារ បញ្ជាក់ពីអត្តសញ្ញាណ អាជីវកម្ម/មុខរបរ សញ្ជាតិ និង អាសយដ្ឋាន ។

៦.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវតម្រូវឱ្យឯកត្តបុគ្គលផ្តល់ឯកសារដើម និងថតចម្លងទុកនូវឯកសារ មួយ ឬ ច្រើនជាង ដូចខាងក្រោម ÷

- អត្តសញ្ញាណប័ណ្ណ
- លិខិតឆ្លងដែន ឬ
- ឯកសារបញ្ជាក់ពីអត្តសញ្ញាណប្រហាក់ប្រហែលផ្សេងៗទៀត ដែលមានភ្ជាប់មកជាមួយនូវរូបថតរបស់ អតិថិជន ដែលចេញផ្សាយដោយអាជ្ញាធរមានសមត្ថកិច្ច ។

ប្រការ ៧._ អតិថិជនជាក្រុមហ៊ុន

៧.១ ក្នុងការបង្កើតទំនាក់ទំនងជាមួយអតិថិជនជាក្រុមហ៊ុន គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវតម្រូវឱ្យ ក្រុមហ៊ុន/ អាជីវកម្ម ផ្តល់ឯកសារដើម និងថតចំលងទុកនូវឯកសារដូចខាងក្រោម÷

- អនុស្សារណៈ លក្ខន្តិកៈ វិញ្ញាបនប័ត្រក្រុមហ៊ុន ភាពជាដៃគូ
- ឯកសារអត្តសញ្ញាណ របស់នាយក ភាគទុនិក ដៃគូ
- សេចក្តីសម្រេចចិត្ត របស់ក្រុមប្រឹក្សាភិបាល ឬ នាយក
- លិខិតផ្ទេរសិទ្ធិដល់បុគ្គលណាម្នាក់ជាតំណាងឱ្យក្រុមហ៊ុន/អាជីវកម្ម

• សិទ្ធិអំណាច ឬ ការអនុញ្ញាតឱ្យធ្វើអាជីវកម្ម ។

៧.២ លើសពីនេះ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវស្រាវជ្រាវ ឬ សាកសួរពីប្រវត្តិរបស់ក្រុមហ៊ុន/អាជីវកម្ម ដើម្បីធានាថាក្រុមហ៊ុនមិនទាន់ត្រូវបាន ឬមិនស្ថិតនៅក្នុងដំណើរការជំរះបញ្ជី ឬមានបញ្ហាលំបាកអ្វីឡើយ ។

៧.៣ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវផ្ទៀងផ្ទាត់អត្តសញ្ញាណនៃគ្រប់ហត្ថលេខីលើគណនី ដោយយោងទៅតាមការយកចិត្តទុកដាក់ស្គាល់អតិថិជនជាឯកត្តបុគ្គល ។ ពេលផ្លាស់ប្តូរហត្ថលេខី ត្រូវយកចិត្តទុកដាក់ ដើម្បីធានាថា ហត្ថលេខាបច្ចុប្បន្នទាំងអស់ត្រូវបានផ្ទៀងផ្ទាត់ហើយ ។

៧.៤ ដើម្បីផ្ទៀងផ្ទាត់ព័ត៌មានដែលទទួលបាន គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវពិនិត្យមើលការចុះបញ្ជីរបស់ក្រុមហ៊ុន/អាជីវកម្ម ដើម្បីបញ្ជាក់ភាពត្រឹមត្រូវនៃព័ត៌មាន ដែលទទួលបានអំពីអត្តសញ្ញាណរបស់ក្រុមហ៊ុន/អាជីវកម្ម និងអភិបាល ម្ចាស់ភាគទុនិក និងនាយកនៃក្រុមហ៊ុននោះ ។

៧.៥ នៅពេលដែលអតិថិជន ឬម្ចាស់គ្រប់គ្រងភាគទុនិកជាសាជីវកម្មដែលមានកាតព្វកិច្ចបើកចំហព័ត៌មាននៅក្នុងទីផ្សារភាគហ៊ុនដែលបានទទួលស្គាល់ នោះអត្តសញ្ញាណរបស់ភាគទុនិកនៃសាជីវកម្ម ពុំចាំបាច់ត្រូវស្វែងរក ឬផ្ទៀងផ្ទាត់ឡើយ ។

៧.៦ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុក៏ត្រូវដឹងពីរចនាសម្ព័ន្ធកម្មសិទ្ធិរបស់អតិថិជនជាក្រុមហ៊ុន និងកំណត់ប្រភពទុនរបស់ក្រុមហ៊ុន/អាជីវកម្ម ។ ប្រការនេះនឹងជួយឱ្យគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុរកឃើញការសង្ស័យណាមួយ ដែលទាក់ទងនឹងការផ្លាស់ប្តូររចនាសម្ព័ន្ធ ឬភាពជាម្ចាស់កម្មសិទ្ធិរបស់ក្រុមហ៊ុន ឬ ការផ្លាស់ប្តូរសារៈតារអតិថិជន និងសកម្មភាពតាមរយៈគណនីរបស់ក្រុមហ៊ុន/អាជីវកម្ម ។

ប្រការ ៨.- អត្តគាហក

គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជនឱ្យបានហ្មត់ចត់ ដូចបានអនុវត្តចំពោះអតិថិជនជាឯកត្តបុគ្គល នៅពេលសង្ស័យថា មានប្រតិបត្តិការមួយត្រូវបានធ្វើឡើងក្នុងនាមអត្តគាហក ហើយមិនមែនធ្វើឡើងសម្រាប់អតិថិជនដែលកំពុងធ្វើប្រតិបត្តិការនោះ ។ អត្តគាហកជាបុគ្គលដែលបានកាន់កាប់ផ្តាច់មុខ ឬត្រួតពិនិត្យអតិថិជនណាម្នាក់ ឬជាបុគ្គលត្រូវបានធ្វើប្រតិបត្តិការជំនួស ។ អត្តគាហកក៏រាប់បញ្ចូលនូវបុគ្គលដែលកាន់កាប់ផ្តាច់មុខលើនីតិបុគ្គល ឬការរៀបចំចាត់ចែងណាមួយផងដែរ ។

ប្រការ ៩.- អង្គការក្រៅរដ្ឋាភិបាល និង មូលនិធិ

៩.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវតម្រូវឱ្យអង្គការក្រៅរដ្ឋាភិបាល ឬ មូលនិធិ ដែលមានទំនាក់ទំនងអាជីវកម្ម ផ្តល់ឯកសារបង្កើតស្ថាប័ន ឬឯកសារប្រហាក់ប្រហែលគ្នាផ្សេងទៀត ដើម្បីធានាថា អង្គការក្រៅរដ្ឋាភិបាល និងមូលនិធិ នោះត្រូវបានបង្កើត និងចុះបញ្ជីបានត្រឹមត្រូវ ។

៩.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវផ្ទៀងផ្ទាត់អត្តសញ្ញាណនៃគ្រប់ហត្ថលេខីលើគណនី ដោយយោងទៅតាមការយកចិត្តទុកដាក់ស្គាល់អតិថិជនជាឯកត្តបុគ្គល ។ ពេលផ្លាស់ប្តូរហត្ថលេខី ត្រូវយកចិត្តទុកដាក់ ដើម្បីធានាថា ហត្ថលេខាបច្ចុប្បន្នទាំងអស់ត្រូវបានផ្ទៀងផ្ទាត់ហើយ ។

៩.៣ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវស្វែងយល់អំពីការត្រួតពិនិត្យ និងការសម្រេចចិត្តរបស់អង្គការក្រៅរដ្ឋាភិបាល/មូលនិធិ និងការប្រើប្រាស់ប្រភពមូលនិធិ ។

ប្រការ ១០.- គណនីអាណត្តិព្យាបាល និង គណនីតំណាង

១០.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវកំណត់ថាតើ អតិថិជនកំពុងតំណាងឱ្យបុគ្គលផ្សេងទៀតដែលជាអ្នកទទួល អាណត្តិព្យាបាល អ្នកតំណាង ឬ ភ្នាក់ងារ ។

១០.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវចាត់វិធានការសមស្របដើម្បីឱ្យដឹងពីភាពជាម្ចាស់កម្មសិទ្ធិ រចនាសម្ព័ន្ធគ្រប់គ្រង និងទំនាក់ទំនង ក្នុងចំណោមភាគីពាក់ព័ន្ធផ្សេងៗ ក្នុងការកាន់កាប់គណនីអាណត្តិព្យាបាល ឬគណនីតំណាង និងត្រូវប្រមូលភស្តុតាងឱ្យបានគ្រប់គ្រាន់ស្តីពីអត្តសញ្ញាណរបស់អ្នកទូទាត់ អ្នកទទួលអាណត្តិព្យាបាល ឬអ្នកតំណាង ហត្ថលេខីដែលទទួលបានការអនុញ្ញាត អ្នកគ្រប់គ្រង និងអត្ថគាហក ។

១០.៣ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវធានាថា តម្រូវការយកចិត្តទុកដាក់ស្គាល់អតិថិជនត្រូវបានបំពេញសម្រាប់អត្ថគាហក នៅពេលបង្កើតគណនីអាណត្តិព្យាបាល ឬគណនីតំណាង ។

១០.៤ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវតម្រូវឱ្យមានការធានាជាលាយល័ក្ខណ៍អក្សរពីអ្នកទទួលអាណត្តិព្យាបាល ឬអ្នកតំណាងថា ភស្តុតាងស្តីពីអត្តសញ្ញាណរបស់អត្ថគាហកត្រូវបានប្រមូលកត់ត្រា និងរក្សាទុក ហើយអ្នកទទួលអាណត្តិព្យាបាល ឬអ្នកតំណាងនោះពេញចិត្តនឹងប្រភពមូលនិធិ ។ លើសពីនេះ ព័ត៌មានស្តីពីអត្តសញ្ញាណទាំងនេះចាំបាច់ត្រូវផ្តល់ឱ្យជាបន្ទាន់ តាមការស្នើសុំរបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ។

ប្រការ ១១.- គណនីអតិថិជន

គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវដឹងអំពីប្រតិបត្តិការគណនីអតិថិជន តាមរយៈមេធាវី និងគណនេយ្យករ ដែលបណ្តាលឱ្យមានការបារម្ភ ហើយត្រូវរាយការណ៍ពីប្រតិបត្តិការទាំងឡាយដល់អង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ប្រសិនបើមានការសង្ស័យណាមួយកើតឡើង ។

ប្រការ ១២.- ក្រុមហ៊ុនសំបក (Shell Company)

គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុមិនត្រូវបើកគណនី ឬធ្វើអាជីវកម្មជាមួយក្រុមហ៊ុនដែលមិនធ្វើសកម្មភាពអាជីវកម្ម ឬពុំមានរូបភាពអាជីវកម្មនៅក្នុងប្រទេស ប៉ុន្តែប្រតិបត្តិការហិរញ្ញវត្ថុអាចត្រូវបានធ្វើឡើងតាមរយៈក្រុមហ៊ុន ដែលជានីតិបុគ្គលទាំងនោះ ។

ប្រការ ១៣._ ការពឹងផ្អែកលើអន្តរការី ឬតតិយភាគីសម្រាប់ការយកចិត្តទុកដាក់ស្គាល់អតិថិជន ដើម្បីផ្តើមអាជីវកម្ម

១៣.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវប្រុងប្រយ័ត្ននិងធានាថា ខ្លួនមិនងាយពេញចិត្ត និងមិនពឹងផ្អែកទាំងស្រុងលើការយកចិត្តទុកដាក់ស្គាល់អតិថិជនដែលធ្វើឡើងដោយអន្តរការី ឬតតិយភាគី ។ ការយកចិត្តទុកដាក់ស្គាល់អតិថិជនត្រូវតែជាការទទួលខុសត្រូវចុងក្រោយរបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ។

១៣.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ត្រូវពេញចិត្តថា អន្តរការី÷

- អនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជន ដោយការសំគាល់អត្តសញ្ញាណ និងផ្ទៀងផ្ទាត់ថា ប្រភពឯកសារ ទិន្នន័យ ឬព័ត៌មានមានភាពឯករាជ្យ និងអាចជឿជាក់បាន
- សំគាល់អត្តសញ្ញាណអត្ថគាហក ហើយចំពោះអតិថិជនជាក្រុមហ៊ុនត្រូវយល់ពីភាគទុនិក និងការគ្រប់គ្រង
- យល់ពីគោលបំណង និងលក្ខណៈអាជីវកម្ម
- មានប្រព័ន្ធសម្រាប់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុដែលអាចទទួលបានឯកសារ អត្តសញ្ញាណ ទិន្នន័យ ដោយពុំមានការពន្យារពេល
- អនុញ្ញាតឱ្យគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រួតពិនិត្យជាប្រចាំសារឡើងវិញ ដើម្បីផ្ទៀងផ្ទាត់ការយកចិត្តទុកដាក់ស្គាល់អតិថិជន និង
- ត្រូវបានធ្វើបញ្ញត្តិកម្ម និងត្រួតពិនិត្យយ៉ាងត្រឹមត្រូវដោយអាជ្ញាធរពាក់ព័ន្ធអំពីការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម ។

ប្រការ ១៤._ អតិថិជនមិនជួបផ្ទាល់

១៤.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវយកចិត្តទុកដាក់ជាពិសេសក្នុងការបង្កើត និងទំនាក់ទំនងអាជីវកម្មមិនជួបផ្ទាល់ ហើយអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជនតាមរយៈអន្តរកម្មជួបផ្ទាល់ ឬ តាមរយៈអន្តរការី ដូចដែលបានតម្រូវដោយប្រការ ១៣នៃប្រកាសនេះ មុននឹងបង្កើតទំនាក់ទំនងបែបនេះជាមួយអតិថិជនរបស់ខ្លួន ។

១៤.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុក៏ត្រូវបានតម្រូវឱ្យអនុវត្តយន្តការតាមដាន និងរាយការណ៍ ដើម្បីសំគាល់អត្តសញ្ញាណជាសក្តានុពលនៃសកម្មភាពសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ។

ប្រការ ១៥ ._ធនាគារទំនាក់ទំនង

១៥.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវចាត់វិធានការចាំបាច់ដើម្បីធានាថា គ្រឹះស្ថានមិនទទួលរងនូវការគំរាមកំហែងពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម តាមរយៈគណនីទំនាក់ទំនងជាមួយគ្រឹះស្ថានធនាគារ និងហិរញ្ញវត្ថុផ្សេងទៀត ។

១៥.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុដែលមានទំនាក់ទំនងបែបនេះត្រូវប្រមូល និងវាយតម្លៃព័ត៌មានស្តីពីគ្រឹះស្ថានធនាគារ និង ហិរញ្ញវត្ថុទំនាក់ទំនងទាំងនោះ យ៉ាងហោចណាស់ដូចជា ÷

- ក្រុមប្រឹក្សាភិបាល និងគណៈគ្រប់គ្រង
- ផលិតផល និងសកម្មភាពអាជីវកម្ម
- ច្បាប់ បទប្បញ្ញត្តិ និងការត្រួតពិនិត្យដែលពាក់ព័ន្ធ
- ការត្រួតពិនិត្យ និងវិធានការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម
- របាយការណ៍ប្រចាំឆ្នាំ ។

១៥.៣ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបង្កើត ឬ បន្តទំនាក់ទំនងសកម្មភាពធនាគារទៅវិញទៅមកជាមួយគ្រឹះស្ថានធនាគារ និង ហិរញ្ញវត្ថុទំនាក់ទំនងបាន លុះត្រាតែខ្លួនបានពេញចិត្តលើការវាយតម្លៃព័ត៌មានដែលប្រមូលបាន ។

១៥.៤ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវចងក្រងឯកសារទទួលខុសត្រូវរបស់ភាគីពាក់ព័ន្ធនីមួយៗ ដែលទាក់ទងនឹងសកម្មភាពធនាគារទំនាក់ទំនង ។

១៥.៥ គណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវសម្រេច និងអនុម័តបង្កើត ឬបន្តទំនាក់ទំនងជាមួយធនាគារទំនាក់ទំនង ។

១៥.៦ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវធានាថា ទំនាក់ទំនងជាមួយធនាគារទំនាក់ទំនងមិនត្រូវបានធ្វើឡើង ជាមួយគ្រឹះស្ថានធនាគារ និង ហិរញ្ញវត្ថុទំនាក់ទំនងដែលពុំមានរូបរាង ហើយមិនមែនជាសម្ព័ន្ធរបស់ក្រុមហិរញ្ញវត្ថុដែលមានការគ្រប់គ្រងតាមច្បាប់ ។

១៥.៧ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវពង្រឹងការយកចិត្តទុកដាក់ស្គាល់អាជីវករជាមួយ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុទំនាក់ទំនងដែលអនុញ្ញាតឱ្យមានការប្រើប្រាស់ដោយផ្ទាល់នៃគណនីទំនាក់ទំនងអតិថិជនរបស់ខ្លួន ដើម្បីធ្វើប្រតិបត្តិការអាជីវកម្មជំនួសអតិថិជន ដូចជាការទូទាត់សងតាមគណនី ។ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជនសម្រាប់អតិថិជនបែបនេះដូចដែលបានតម្រូវចំពោះអន្តរការិយកម្មផ្តើមអាជីវកម្ម ។

១៥.៨ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវយកចិត្តទុកដាក់ជាពិសេសចំពោះទំនាក់ទំនងជាមួយគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុទំនាក់ទំនងពីប្រទេសទាំងឡាយ ដែលពុំមានការអនុវត្តគ្រប់គ្រាន់តាមវិធានការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្មដែលបានទទួលយកជាអន្តរជាតិ ។ ការយកចិត្តទុកដាក់ស្គាល់អតិថិជនដែលបានពង្រឹងរួចហើយ គឺជាតម្រូវការចាំបាច់ដើម្បីវាយតម្លៃហានិភ័យនៃការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ។

ប្រការ ១៦.-ការផ្ទេរប្រាក់/ការផ្ទេរតាមប្រព័ន្ធអេឡិចត្រូនិក

១៦.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុដែលអនុវត្ត ឬចូលរួមប្រតិបត្តិការផ្ទេរប្រាក់ចេញ/ការផ្ទេរចេញតាមប្រព័ន្ធអេឡិចត្រូនិកត្រូវមានព័ត៌មានចាំបាច់ស្តីពីអ្នកផ្តើមប្រតិបត្តិការ ឈ្មោះ អាសយដ្ឋាន លេខគណនី លេខអត្តសញ្ញាណ ឬ លេខយោងអតិថិជន និងសេចក្តីលំអិតនៃប្រតិបត្តិការ ។

១៦.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុដែលជួយសម្រួល ឬធ្វើសកម្មភាពជាអន្តរការីចំពោះប្រតិបត្តិការផ្ទេរប្រាក់/ការផ្ទេរតាមប្រព័ន្ធអេឡិចត្រូនិកត្រូវធានាថា ព័ត៌មានស្តីពីអ្នកផ្តើមប្រតិបត្តិការនៅតែត្រូវបានរក្សាទុកជាមួយសារផ្ទេរប្រាក់/សារផ្ទេរតាមអេឡិចត្រូនិកនោះ ។

១៦.៣ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ដែលទទួលប្រតិបត្តិការផ្ទេរប្រាក់/ការផ្ទេរចូលតាមប្រព័ន្ធអេឡិចត្រូនិក ដោយទទួលព័ត៌មានពុំគ្រប់គ្រាន់ស្តីពីអ្នកផ្តើមប្រតិបត្តិការត្រូវពង្រឹងការយកចិត្តទុកដាក់ស្គាល់អតិថិជន ហើយអាចចាត់ទុកប្រតិបត្តិការនេះជាប្រតិបត្តិការសង្ស័យ ។

១៦.៤ ប្រតិបត្តិការផ្ទេរប្រាក់/ការផ្ទេរតាមប្រព័ន្ធអេឡិចត្រូនិកដែលមានទឹកប្រាក់តិចជាង ១.០០០ ដុល្លារអាមេរិក (៤ លានរៀល) ឬសមមូលនឹងរូបិយប័ណ្ណផ្សេងទៀត មិនចាំបាច់មានព័ត៌មានដូចដែលបានតម្រូវខាងលើនោះទេ ។

១៦.៥ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវពិនិត្យជាពិសេសចំពោះអតិថិជនដែលមានហានិភ័យខ្ពស់ ដោយយកចិត្តទុកដាក់លើកត្តាមួយចំនួនដូចជា ឈ្មោះអត្ថគាហក ទិសដៅ និងចំនួនប្រាក់ដែលត្រូវផ្ទេរ ។ លើសពីនេះប្រសិនបើការផ្ទេរប្រាក់/ការផ្ទេរតាមប្រព័ន្ធអេឡិចត្រូនិកនេះ មិនស៊ីគ្នានឹងសកម្មភាព/អាជីវកម្មធម្មតារបស់អតិថិជន គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ត្រូវទាមទារឱ្យអតិថិជនពន្យល់បន្ថែមពីលក្ខណៈនៃប្រតិបត្តិការផ្ទេរប្រាក់/ការផ្ទេរតាមប្រព័ន្ធអេឡិចត្រូនិក ។

ប្រការ ១៧.- បុគ្គលពាក់ព័ន្ធនយោបាយ

១៧.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវពិនិត្យមើលអតិថិជនថ្មីៗនិងបច្ចុប្បន្ន បន្ថែមលើការអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជនដើម្បីឱ្យដឹងថា អតិថិជនជាបុគ្គលពាក់ព័ន្ធ ឬពុំពាក់ព័ន្ធនយោបាយ ដូចមានចែងនៅក្នុងមាត្រា៣ នៃច្បាប់ស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ។ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវប្រមូលព័ត៌មានឱ្យបានគ្រប់គ្រាន់ពីអតិថិជននោះ និងត្រូវស្វែងរកព័ត៌មានដែលមានជាសាធារណៈ ដើម្បីកំណត់កម្រិតហានិភ័យនៃការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ។

១៧.២ ខណៈដែលបុគ្គលពាក់ព័ន្ធនយោបាយត្រូវបានសំគាល់អត្តសញ្ញាណ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវចាត់វិធានការសមស្របដើម្បីកំណត់ពីប្រភពទ្រព្យសម្បត្តិ និងមូលនិធិរបស់បុគ្គលនោះ ។

១៧.៣ គណៈគ្រប់គ្រងជាន់ខ្ពស់របស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវសម្រេចចិត្តក្នុងការចូលរួម ឬបន្តទំនាក់ទំនងអាជីវកម្មជាមួយបុគ្គលពាក់ព័ន្ធនយោបាយ ។

១៧.៤ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ត្រូវបង្កើតសាវតារហានិភ័យនៃបុគ្គលពាក់ព័ន្ធនយោបាយម្នាក់ៗដោយផ្អែកលើព័ត៌មានដែលប្រមូលបានពីអតិថិជន និងការស្រាវជ្រាវឯករាជ្យ ព្រមទាំងយល់ពីលក្ខណៈនៃទំនាក់ទំនងអាជីវកម្ម និង សកម្មភាពប្រតិបត្តិការ ។ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវតាមដានជាប្រចាំនូវទំនាក់ទំនង និង

សកម្មភាពទប់ទល់ហានិភ័យ និងបញ្ហាដែលកើតឡើងពីដំណើរការត្រួតពិនិត្យ ត្រូវរាយការណ៍ទៅថ្នាក់គ្រប់គ្រងជាន់ខ្ពស់ និងអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ បើចាំបាច់ ។

ប្រការ ១៨.- ប្រតិបត្តិការធនាគារកម្មឯកជន (Private banking)

១៨.១ អាជីវកម្មធនាគារកម្មឯកជន ត្រូវបានផ្តល់ឱ្យអតិថិជនដែលមានមូលនិធិផ្ទាល់សុទ្ធខ្ពស់ និងបុគ្គលពិសេស ហើយឯកសិទ្ធិពិសេសសម្ងាត់ និងឯកជននៃប្រតិបត្តិការបែបនេះអាចផ្តល់លទ្ធភាពដល់ការបំភាន់ពីសំណាក់អ្នកសំអាតប្រាក់ និងអ្នកផ្តល់ហិរញ្ញប្បទានភេរវកម្ម ។

១៨.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវយកចិត្តទុកដាក់ជាពិសេសចំពោះអាជីវកម្មធនាគារកម្មឯកជន ។ នីតិវិធីផ្ទៀងផ្ទាត់និងសំគាល់អត្តសញ្ញាណត្រូវតែរឹតបន្តឹងជាងនីតិវិធីសំគាល់អត្តសញ្ញាណធម្មតា ជាពិសេស វិធានការផ្ទៀងផ្ទាត់បន្ថែមត្រូវអនុវត្តទាក់ទងនឹងអត្តសញ្ញាណ លក្ខណៈអាជីវកម្ម និងប្រភពមូលនិធិអតិថិជន ។

១៨.៣ អតិថិជនថ្មី និងអតិថិជនមានស្រាប់ទាំងអស់ដែលទទួលសេវាប្រតិបត្តិការធនាគារកម្មឯកជន ត្រូវតែមានការអនុមតិពីគណៈគ្រប់គ្រងជាន់ខ្ពស់ ពោលគឺមិនមែនពីអ្នកគ្រប់គ្រងផ្នែកទំនាក់ទំនងប្រតិបត្តិការធនាគារកម្មឯកជនដែលជាអ្នករៀបចំដំណើរការផង និង អនុម័តពាក្យសុំផងទេ ។

១៨.៤ មន្ត្រីប្រតិបត្តិ និងសវនករត្រូវតែបានអនុញ្ញាតឱ្យធ្វើសវនកម្មនិងពិនិត្យឡើងវិញលើប្រតិបត្តិការរបស់អតិថិជនជាធនាគារកម្ម ។

ប្រការ ១៩.- អាជីវករប្តូរប្រាក់

១៩.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវយកចិត្តទុកដាក់ជាពិសេស ដើម្បីធានាថាអាជីវករប្តូរប្រាក់ដែលមានគណនីនៅគ្រឹះស្ថាន បានទទួលអាជ្ញាប័ណ្ណ និងធ្វើប្រតិបត្តិការប្តូរប្រាក់ស្របច្បាប់ ។ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវធានាថា លក្ខណៈនិងបរិមាណនៃប្រតិបត្តិការនៅក្នុងគណនីអាជីវករប្តូរប្រាក់បានឆ្លុះបញ្ចាំងនូវលក្ខណៈនៃអាជីវកម្មរបស់អាជីវករទាំងនោះ ។

១៩.២ ប្រសិនបើ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុរកឃើញសកម្មភាពខុសគ្នាណាមួយនៅក្នុងគណនីរបស់អាជីវករប្តូរប្រាក់ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ត្រូវរាយការណ៍ប្រតិបត្តិការសង្ស័យនេះមកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ។

ប្រការ ២០.- អតិថិជនមានហានិភ័យខ្ពស់ផ្សេងទៀត

២០.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ត្រូវលើកកម្ពស់ការយកចិត្តទុកដាក់ស្គាល់អតិថិជនចំពោះអតិថិជនមានហានិភ័យខ្ពស់ផ្សេងទៀត រួមបញ្ចូលអតិថិជនដែលមានហានិភ័យខ្ពស់ ដូចមានចែងនៅក្នុងប្រការ ១៨ និង ១៩ នៃប្រកាសនេះ ដើម្បីធានាថា គ្រឹះស្ថានមិនត្រូវបានបំភាន់ដោយអ្នកសំអាតប្រាក់ និង អ្នកផ្តល់ហិរញ្ញប្បទានភេរវកម្ម ។

២០.២ ការលើកកម្ពស់ការយកចិត្តទុកដាក់ស្គាល់អតិថិជនបែបនេះ យ៉ាងហោចណាស់ ត្រូវមាន÷

- ព័ត៌មានលំអិតបន្ថែមទៀតពីអតិថិជន ជាពិសេស គោលបំណងនៃប្រតិបត្តិការ និងប្រភពនៃមូលនិធិ
- ការស្រាវជ្រាវឯករាជ្យ និងរកប្រភពព័ត៌មានបន្ថែមអំពីអតិថិជន និង
- ការអនុមតិពីគណៈគ្រប់គ្រងថ្នាក់ខ្ពស់ ។

ប្រការ ២១.- គណនីមានស្រាប់

២១.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវចាត់វិធានការចាំបាច់ ដើម្បីធានាថា កំណត់ត្រានៃអតិថិជនមានស្រាប់ នៅតែធ្វើបច្ចុប្បន្នកម្មនិងមានភាពពាក់ព័ន្ធ ។ លើសពីនេះ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវប្រមូលភស្តុតាងបន្ថែមស្តីពីអត្តសញ្ញាណអតិថិជនមានស្រាប់ ប្រសិនបើចាំបាច់ ដើម្បីធានាអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជនស្របតាមបទដ្ឋាន ដែលបានកំណត់ដោយប្រកាសនេះ ។

២១.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ត្រូវអនុវត្តការពិនិត្យឡើងវិញឱ្យបានទៀងទាត់លើកំណត់ត្រាមានស្រាប់របស់អតិថិជន ។ ការពិនិត្យឡើងវិញនេះ យ៉ាងហោចណាស់ ធ្វើឡើងនៅពេល÷

- ប្រតិបត្តិការសំខាន់ៗកើតឡើង
- មានការផ្លាស់ប្តូរសំខាន់ៗនៅក្នុងគណនីដែលមានសកម្មភាព
- មានការផ្លាស់ប្តូរបទដ្ឋាននៃការរៀបចំឯកសាររបស់អតិថិជនយ៉ាងច្រើន ឬ
- ព័ត៌មានដែលទទួលបានពីអតិថិជនពុំគ្រប់គ្រាន់ ។

២១.៣ ប្រសិនបើគ្មានព្រឹត្តិការណ៍ដូចខាងលើកើតឡើង គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុចាំបាច់ត្រូវពិចារណាដោយផ្អែកលើការវាយតម្លៃហានិភ័យ និងត្រូវប្រមូលព័ត៌មានបន្ថែមពីអតិថិជនមានស្រាប់ ដែលចាត់ទុកថាមានហានិភ័យខ្ពស់ឱ្យស្របតាមបទដ្ឋានបច្ចុប្បន្នរបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ។

ប្រការ ២២ .- ការរក្សាទុកឯកសារកត់ត្រា

២២.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវរក្សាទុកកំណត់ត្រា ឯកសារ និងឯកសារចម្លងទាំងអស់ ដែលទាក់ទងនឹងគ្រប់រូបភាពនៃប្រតិបត្តិការឱ្យបានយ៉ាងតិចរយៈពេល ៥ ឆ្នាំ នៅក្រោយពេលធ្វើប្រតិបត្តិការ ។ គ្រប់ទិន្នន័យអត្តសញ្ញាណ កំណត់ត្រា ឯកសារ លិខិតទំនាក់ទំនងអាជីវកម្ម និងឯកសារចម្លង ដែលទទួលបានក្នុងពេលអនុវត្តនីតិវិធីយកចិត្តទុកដាក់ស្គាល់អតិថិជន ត្រូវតែរក្សាទុកឱ្យបានយ៉ាងតិច ៥ ឆ្នាំ បន្ទាប់ពីបិទគណនី ឬ បន្ទាប់ពីបញ្ចប់ទំនាក់ទំនងអាជីវកម្មជាមួយអតិថិជន ។

២២.២ ករណីដែលកំណត់ត្រាជាកម្មវត្ថុនៃការស៊ើបអង្កេតជាបន្តបន្ទាប់ ឬ នៃរបាយការណ៍ប្រតិបត្តិការសង្ស័យ កំណត់ត្រានោះត្រូវរក្សាទុកឱ្យបានលើសពីរយៈពេលដែលបានកំណត់រហូតដល់អាជ្ញាធរដែលពាក់ព័ន្ធនឹងការស៊ើបអង្កេត បញ្ជាក់ថា ឯកសារទាំងនោះលែងមានសារប្រយោជន៍ ។

ប្រការ ២៣.- ដាននៃសវនកម្ម

២៣.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវធានាថា រាល់ឯកសារនិងកំណត់ត្រាដែលបានរក្សាទុក បង្កើតជាដាននៃសវនកម្មចំពោះប្រតិបត្តិការនីមួយៗ ដែលជួយភ្នាក់ងារត្រួតពិនិត្យនិងភ្នាក់ងារមានសមត្ថកិច្ច ដើម្បីតាមដានមូលនិធិ ។

២៣.២ កំណត់ត្រាដែលបានរក្សាទុកទាំងនោះ ត្រូវតែអាចជួយគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ឱ្យបង្កើតប្រវត្តិ និង លក្ខណៈ និង បង្កើតប្រតិបត្តិការនីមួយៗឡើងវិញបាន ។ កំណត់ត្រាទាំងនោះ យ៉ាងហោចណាស់ត្រូវមាន÷

- ប្រភពមូលនិធិ ដូចជាវិធីសាស្ត្រនៃការទទួល និង/ឬអ្នកផ្តើមប្រតិបត្តិការផ្ទេរប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិច
- អត្តសញ្ញាណបុគ្គលដែលធ្វើប្រតិបត្តិការ ប្រសិនបើមិនមែនជាម្ចាស់គណនី
- ប្រភេទប្រតិបត្តិការ និង
- ការណែនាំ និង ទិសដៅនៃការផ្ទេរមូលនិធិ ។

ប្រការ ២៤ .- ទម្រង់ឯកសារដែលរក្សាទុក

គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវរក្សាទុកឯកសារពាក់ព័ន្ធ ជាច្បាប់ដើម ឬ ថតចម្លង ឬ មីក្រូហ្វីល ឬ ក្នុងទម្រង់អេឡិចត្រូនិក តែត្រូវមានសុវត្ថិភាព និងអាចយកមកប្រើប្រាស់នៅពេលត្រូវការ ហើយត្រូវមានលក្ខណៈត្រឹមត្រូវ និងទាន់ពេលវេលា ។

ប្រការ ២៥.-ការតាមដានបន្ត

២៥.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជនជាបន្តចំពោះទំនាក់ទំនងជាមួយអតិថិជនទាំងអស់ ដោយប្រើប្រាស់វិធីសាស្ត្រផ្អែកតាមហានិភ័យ ។ វិធីសាស្ត្រនេះ ត្រូវធានាថាសារពើហានិភ័យរបស់អតិថិជន ត្រូវបានធ្វើបច្ចុប្បន្នកម្ម ។

២៥.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវយកចិត្តទុកដាក់ជាពិសេស និងបន្តអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជន សម្រាប់គ្រប់ប្រតិបត្តិការធំៗ មិនប្រក្រតី ស្មុគស្មាញ ឬគំរូនៃប្រតិបត្តិការមិនប្រក្រតីដើម្បីកំណត់ថាតើប្រតិបត្តិការទាំងនេះមាន ឬពុំមានគោលបំណងស្របច្បាប់ច្បាស់លាស់ ។

ប្រការ ២៦.- ការគ្រប់គ្រងប្រព័ន្ធព័ត៌មាន

គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបង្កើតប្រព័ន្ធគ្រប់គ្រងព័ត៌មានគ្រប់គ្រាន់មួយ ដើម្បីអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជនរបស់ខ្លួន សម្រាប់សំគាល់អត្តសញ្ញាណ និងរកឱ្យឃើញនូវប្រតិបត្តិការទាំងឡាយណាដែលខ្លួនសង្ស័យ ឬមានមូលដ្ឋានសមស្របដើម្បីសង្ស័យលើប្រតិបត្តិការ ដែលជាប់ពាក់ព័ន្ធនឹងផលដែលបានមកពីសកម្មភាពខុសច្បាប់ ឬអតិថិជនដែលជាប់ទាក់ទងនឹងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ។ ប្រព័ន្ធគ្រប់គ្រងព័ត៌មានត្រូវផ្តល់ឱ្យគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុនូវព័ត៌មាន ទៀងទាត់ទាន់ពេលវេលា ដើម្បីអាចរកសកម្មភាពសង្ស័យ ។

ប្រការ ២៧.- ការយកចិត្តទុកដាក់ពិសេស

គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវអនុវត្តការយកចិត្តទុកដាក់ស្គាល់អតិថិជនជាបន្តបន្ទាប់អាស្រ័យលើទំនាក់ទំនងអាជីវកម្ម និងប្រតិបត្តិការជាមួយឯកត្តបុគ្គល អាជីវកម្ម ក្រុមហ៊ុន និងគ្រឹះស្ថានហិរញ្ញវត្ថុ មកពីបណ្តាប្រទេសដែលមិនបានអនុវត្តពេញលេញតាមវិធានការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្មដែលទទួលស្គាល់ជាអន្តរជាតិ ។ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវសួរសំណួរបន្ថែមពីគោលបំណង និងប្រវត្តិប្រតិបត្តិការ និងទំនាក់ទំនងអាជីវកម្មបែបនេះ ឱ្យបានល់អិតជាលាយល័ក្ខណ៍អក្សរ និងបញ្ជូនដល់អាជ្ញាធរមានសមត្ថកិច្ច ។

ប្រការ ២៨.- របាយការណ៍ប្រតិបត្តិការសាច់ប្រាក់

២៨.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវរាយការណ៍មកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុនូវប្រតិបត្តិការសាច់ប្រាក់ ដែលស្មើ ឬលើសពី ៤០ លានរៀល ឬសមមូលនឹងរូបិយប័ណ្ណផ្សេងទៀត ។

២៨.២ ប្រតិបត្តិការសាច់ប្រាក់ត្រូវផ្តល់មកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ កំឡុងពេល ១៤ ថ្ងៃ ក្រោយកាលបរិច្ឆេទនៃប្រតិបត្តិការ ហើយត្រូវបំពេញក្នុងទម្រង់ "របាយការណ៍ប្រតិបត្តិការសាច់ប្រាក់" ដែលបានអនុម័តដោយអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ឬទម្រង់ដែលបានអនុម័តសម្រាប់ការរាយការណ៍តាមអេឡិចត្រូនិច ។ ច្បាប់ចម្លងនៃទម្រង់របាយការណ៍ប្រតិបត្តិការសាច់ប្រាក់ត្រូវបានភ្ជាប់មកជាមួយក្នុងឧបសម្ព័ន្ធទី ៤ ។

២៨.៣ ប្រតិបត្តិការសាច់ប្រាក់ ដែលអាចរាយការណ៍បាន រួមមាន ប្រតិបត្តិការសាច់ប្រាក់ច្រើនសន្ទឹកសន្ទាប់របស់អតិថិជនម្នាក់/គណនីមួយដែលមានចំនួនសរុបនៃប្រតិបត្តិការរួមគ្នាក្នុងមួយថ្ងៃលើសពី ៤០ លានរៀល ឬសមមូលនឹងរូបិយប័ណ្ណផ្សេងទៀត ។

ប្រការ ២៩.- របាយការណ៍ប្រតិបត្តិការសង្ស័យ

២៩.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបានតម្រូវឱ្យបង្កើតប្រព័ន្ធរាយការណ៍ និង បញ្ជូនរបាយការណ៍ពីប្រតិបត្តិការសង្ស័យភ្លាមៗមកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ នៅពេលនិយោជិតរបស់ខ្លួនសង្ស័យ ឬមានមូលដ្ឋានសមស្របសង្ស័យថា ប្រតិបត្តិការនោះជាប់ពាក់ព័ន្ធនឹងប្រាក់បានមកពីផលនៃបទល្មើស ឬ អតិថិជនជាប់ពាក់ព័ន្ធនឹង

ការសំអាតប្រាក់ ឬហិរញ្ញប្បទានភេរវកម្ម ។ ឧទាហរណ៍នៃប្រតិបត្តិការសង្ស័យត្រូវបានលើកឡើង ក្នុងតារាងឧបសម្ព័ន្ធទី ២ នៃប្រកាសនេះ ។ ឧទាហរណ៍ទាំងនេះមិនមែនសរុបជារួមទេ គឺគ្រាន់តែផ្តល់ជាវិធីសាស្ត្រមូលដ្ឋានអំពីការសំអាតប្រាក់ ឬហិរញ្ញប្បទានភេរវកម្ម ។ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបង្កើតសេចក្តីណែនាំផ្ទៃក្នុងផ្ទាល់ខ្លួនអំពីការរាយការណ៍ប្រតិបត្តិការសង្ស័យ ដោយផ្សារភ្ជាប់ជាមួយច្បាប់ស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម និង បញ្ញត្តិដែលបានចែងនៅក្នុងប្រកាសនេះ រួមទាំងមានតារាងផ្ទាល់ខ្លួនស្តីពីសូចនាករ ប្រតិបត្តិការសង្ស័យផងដែរ ។

២៩.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបញ្ជូនរបាយការណ៍ប្រតិបត្តិការសង្ស័យ នៅពេលដែលអតិថិជនថ្មី ឬអតិថិជនមានស្រាប់មិនបានបំពេញនូវកាតព្វកិច្ចយកចិត្តទុកដាក់ស្គាល់អតិថិជន ដោយគ្មានហេតុផលសមស្រប ដោយពុំគិតថាគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុទទួលយក បដិសេធ បន្ត ឬបញ្ចប់ទំនាក់ទំនងអាជីវកម្មជាមួយអតិថិជននោះ ។

ប្រការ ៣០.-យន្តការរាយការណ៍

៣០.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវតែងតាំងមន្ត្រីថ្នាក់គ្រប់គ្រងជាន់ខ្ពស់មួយរូប ធ្វើជាមន្ត្រីប្រតិបត្តិទទួលខុសត្រូវក្នុងការបញ្ជូនរបាយការណ៍ប្រតិបត្តិការសង្ស័យមកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ។ មន្ត្រីប្រតិបត្តិដែលទទួលបានការតែងតាំងត្រូវដើរតួនាទីជាអ្នកទំនាក់ទំនងតែម្នាក់គត់សម្រាប់អង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ។ គ្រឹះស្ថានធនាគារ និងហិរញ្ញវត្ថុត្រូវធានាថា រាល់របាយការណ៍ប្រតិបត្តិការសង្ស័យដែលបានធ្វើឡើងដោយនិយោជិត ត្រូវបានផ្តល់ឱ្យមន្ត្រីប្រតិបត្តិយ៉ាងសមស្រប ។

៣០.២ គ្រឹះស្ថានធនាគារ និង ហិរញ្ញវត្ថុត្រូវណែនាំនិយោជិតឱ្យរាយការណ៍ប្រតិបត្តិការសង្ស័យទៅមន្ត្រីប្រតិបត្តិ ទោះបីជាគេពុំដឹងច្បាស់ថាប្រតិបត្តិការនោះជាសកម្មភាពខុសច្បាប់ ឬ ពិតជាកើតឡើងក៏ដោយ ។

៣០.៣ នៅពេលទទួលបានរបាយការណ៍ប្រតិបត្តិការសង្ស័យ មន្ត្រីប្រតិបត្តិត្រូវវាយតម្លៃ និងកំណត់ភ្លាមៗ ពីមូលដ្ឋានសមហេតុផលក្នុងការសង្ស័យ និង ត្រូវបញ្ជូនរបាយការណ៍ប្រតិបត្តិការសង្ស័យនេះជាបន្ទាន់ មកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុក្នុងរយៈពេល ២៤ ម៉ោង ប្រសិនបើមន្ត្រីប្រតិបត្តិគិតថា គ្មានមូលហេតុសមហេតុផលទេនោះត្រូវកត់ត្រាតែមតិរបស់ខ្លួនប៉ុណ្ណោះ ។

៣០.៤ របាយការណ៍ប្រតិបត្តិការសង្ស័យ ដែលបញ្ជូនមកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុដោយមន្ត្រីប្រតិបត្តិត្រូវធ្វើជាលាយល័ក្ខណ៍អក្សរ ដូចមានក្នុងឧបសម្ព័ន្ធទី ៣ ហើយត្រូវប្រគល់ដោយសុវត្ថិភាពដោយផ្ទាល់ដៃ ឬតាមសំបុត្រដែលមានសុវត្ថិភាព និងតាមអេឡិចត្រូនិច ជាដើម ។

៣០.៥ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវធានាថា នៅពេលរៀបចំ និងបញ្ជូនរបាយការណ៍ប្រតិបត្តិការសង្ស័យនោះ ត្រូវរក្សាការសម្ងាត់ និងអាចដឹងព័ត៌មាននេះបានត្រឹមតែបុគ្គលិកដែលមានសិទ្ធិប៉ុណ្ណោះ ។

៣០.៦ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវផ្តល់សិទ្ធិឱ្យមន្ត្រីប្រតិបត្តិសហការ ជាមួយអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ក្នុងការផ្តល់ព័ត៌មាននិងឯកសារចាំបាច់បន្ថែមទៅតាមសំណើសុំ និងឆ្លើយតបរាល់ការសាកសួរដែលពាក់ព័ន្ធនឹងរបាយការណ៍ប្រតិបត្តិការសង្ស័យ ។

ប្រការ ៣១.- ការហាមឃាត់ការផ្តល់ព័ត៌មាន

៣១.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវធានាថា ប្រព័ន្ធរាយការណ៍ដែលបានបង្កើតសម្រាប់បញ្ជូនរបាយការណ៍ប្រតិបត្តិការសង្ស័យត្រូវបានដំណើរការជាសម្ងាត់ ។

៣១.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវធានាថា អតិថិជនដែលបានរាយការណ៍នេះ មិនត្រូវបានផ្តល់ព័ត៌មាន ឬមិនបានដឹងថាមានរបាយការណ៍ប្រតិបត្តិការនេះទេ ។ បុគ្គលិកទាំងអស់ត្រូវយល់ដឹងអំពីមាត្រាទី ១៥ នៃច្បាប់ស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្មដែលបានចែងអំពីការហាមឃាត់បុគ្គលណា ដែលបានដឹងអំពីប្រតិបត្តិការសង្ស័យ មិនត្រូវផ្តល់ព័ត៌មានឬរាយការណ៍ទាំងនោះទៅបុគ្គលផ្សេង ក្រៅពីអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ លើកលែងតែមានការអនុញ្ញាតផ្សេងពីនេះ ពីអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ។

ប្រការ ៣២.- បញ្ហាផ្សេងទៀត

៣២.១ គ្រឹះស្ថានធនាគារ និង ហិរញ្ញវត្ថុត្រូវរក្សាទុកឯកសាររបាយការណ៍ប្រតិបត្តិការសង្ស័យ ដែលនិយោជិតបានផ្ញើទៅមន្ត្រីប្រតិបត្តិ និងបានផ្ញើបន្តមកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ។

៣២.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវចាត់វិធានការសមហេតុផល ដើម្បីធ្វើយ៉ាងណាឱ្យមន្ត្រី និងនិយោជិតដែលពាក់ព័ន្ធនឹងការអនុវត្ត ឬសម្របសម្រួលប្រតិបត្តិការរបស់អតិថិជន យល់ដឹងពីនីតិវិធីរាយការណ៍ ។

ប្រការ ៣៣.- ការរកឃើញ និង ការរាយការណ៍ពីហិរញ្ញប្បទានភេរវកម្ម

៣៣.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវចាត់វិធានការចាំបាច់ ដើម្បីអនុវត្តឱ្យស្របតាមសេចក្តីសម្រេចរបស់ក្រុមប្រឹក្សាសន្តិសុខសហប្រជាជាតិ និង ច្បាប់ និងបទប្បញ្ញត្តិស្តីពីហិរញ្ញប្បទានភេរវកម្ម ។

៣៣.២ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវធានាថា ប្រព័ន្ធនិងយន្តការរាយការណ៍ប្រតិបត្តិការសង្ស័យ ត្រូវបានពង្រីកគ្របដណ្តប់លើការសង្ស័យពីហិរញ្ញប្បទានភេរវកម្ម ។

៣៣.៣ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវរក្សាមូលដ្ឋានទិន្នន័យដែលមានឈ្មោះ និង ព័ត៌មានលំអិតរបស់ភេរវករដែលមានក្នុងបញ្ជីរបស់អង្គការសហប្រជាជាតិ ហើយត្រូវយកចិត្តទុកដាក់ដល់ការបញ្ចូលគ្នារវាងមូលដ្ឋានទិន្នន័យរបស់ខ្លួន និងបញ្ជីឈ្មោះបុគ្គលដែលបានសំគាល់អត្តសញ្ញាណផ្សេងទៀត ។ ព័ត៌មាននៅក្នុងមូលដ្ឋានទិន្នន័យត្រូវធ្វើបច្ចុប្បន្នកម្ម និងមានទំនាក់ទំនងគ្នា ហើយផ្តល់លទ្ធភាពងាយស្រួលដល់និយោជិតក្នុងការប្រើប្រាស់សម្រាប់សំគាល់អត្តសញ្ញាណប្រតិបត្តិការសង្ស័យ និងការបង្កកគណនី/មូលនិធិ ។

៣៣.៤ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវពិនិត្យមើលឈ្មោះរបស់អតិថិជនថ្មី និង អតិថិជនមានស្រាប់ជាមួយនឹងឈ្មោះដែលមាននៅក្នុងមូលដ្ឋានទិន្នន័យ ។ ប្រសិនបើមានឈ្មោះដូចគ្នា គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវចាត់វិធានការសមស្របដើម្បីផ្ទៀងផ្ទាត់ និងបញ្ជាក់ពីអត្តសញ្ញាណរបស់អតិថិជននោះ ។ ប្រសិនបើ ឈ្មោះអតិថិជន និងឈ្មោះនៅក្នុងមូលដ្ឋានទិន្នន័យជាឈ្មោះតែមួយ ហើយជាមនុស្សតែម្នាក់ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបង្កកគណនីរបស់អតិថិជននោះ និងត្រូវជូនដំណឹងមកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុជាបន្ទាន់ ។ នៅពេលដែលមានការសង្ស័យថាប្រតិបត្តិការមួយពាក់ព័ន្ធនឹងភេរវករ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវរាយការណ៍ប្រតិបត្តិការសង្ស័យមកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ ។

ប្រការ ៣៤.- ការគ្រប់គ្រងហានិភ័យ

៣៤.១ ក្រុមប្រឹក្សាភិបាលរបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបង្កើតប្រព័ន្ធត្រួតពិនិត្យផ្ទៃក្នុង ឱ្យមានប្រសិទ្ធភាព ដើម្បីប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ដែលស្របតាមការតម្រូវនៃច្បាប់ និងបទប្បញ្ញត្តិ ។ គណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវទទួលខុសត្រូវឱ្យមានការត្រួតពិនិត្យផ្ទៃក្នុងយ៉ាងមានប្រសិទ្ធភាព ។

៣៤.២ ក្រុមប្រឹក្សាភិបាល និងគណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវដឹង និងយល់ពីវិធានការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម ដែលតម្រូវដោយច្បាប់ បញ្ញត្តិករ បទដ្ឋានតាមវិស័យនីមួយៗ និងការអនុវត្តដ៏ប្រសើរ ក៏ដូចជាសារសំខាន់នៃការបង្កើតឱ្យមានវិធានការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ដើម្បីទប់ស្កាត់ការរំលោភបំពានរបស់អ្នកសំអាតប្រាក់ និងអ្នកផ្តល់ហិរញ្ញប្បទានភេរវកម្មមកលើគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ។ ក្រុមប្រឹក្សាភិបាលត្រូវត្រួតពិនិត្យឱ្យបានល្អិតល្អន់លើវិធានការទូទៅប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ដែលត្រូវអនុវត្ត ដោយគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ។

៣៤.៣ ក្រុមប្រឹក្សាភិបាល និង គណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវដឹងពីហានិភ័យនៃការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម ពាក់ព័ន្ធនឹងរាល់សេវាកម្ម និងផលិតផលអាជីវកម្មរបស់ខ្លួន ។

៣៤.៤ ក្រុមប្រឹក្សាភិបាលត្រូវធានាថា គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ យ៉ាងតិចបំផុតត្រូវមានគោលការណ៍ស្តីពីនីតិវិធី និងការត្រួតពិនិត្យការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ។ គណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវជួយក្រុមប្រឹក្សាភិបាលក្នុងការបង្កើតគោលការណ៍ ហើយត្រូវធានាថា គោលការណ៍នេះស្របតាមហានិភ័យដែលពាក់ព័ន្ធនឹងលក្ខណៈអាជីវកម្ម ភាពស្មុគស្មាញ និងទំហំប្រតិបត្តិការ ដែលអនុវត្តដោយគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ។

៣៤.៥ ក្រុមប្រឹក្សាភិបាលត្រូវធានាថា គ្រឹះស្ថានមានការអនុវត្តនីតិវិធីសម្រាប់វិធានការប្រឆាំងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម រួមទាំងគោលការណ៍ទទួលស្គាល់អតិថិជន ការយកចិត្តទុកដាក់ស្គាល់អតិថិជន ការរក្សាទុកឯកសារ ការតាមដានជាប្រចាំ ការរាយការណ៍ប្រតិបត្តិការសង្ស័យ និងប្រឆាំងហិរញ្ញប្បទានភេរវកម្ម ។

៣៤.៦ ក្រុមប្រឹក្សាភិបាលត្រូវវាយតម្លៃការអនុវត្តរបស់គណៈគ្រប់គ្រងជាន់ខ្ពស់លើគោលការណ៍ប្រឆាំងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ដែលបានអនុម័តតាមរយៈរបាយការណ៍ប្រចាំគ្រា ។

៣៤.៧ ក្រុមប្រឹក្សាភិបាលត្រូវកំណត់សិទ្ធិ និងការទទួលខុសត្រូវក្នុងការអនុវត្តវិធានការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម ហើយត្រូវធានាថា មានការបែងចែកភារកិច្ចរវាងការអនុវត្តគោលការណ៍ និង នីតិវិធី និង ការត្រួតពិនិត្យ ។ ក្រុមប្រឹក្សាភិបាលត្រូវធានាឱ្យមាន÷

- ការតែងតាំងមន្ត្រីប្រតិបត្តិម្នាក់ ដើម្បីធានាថា គោលការណ៍ នីតិវិធី និង ការត្រួតពិនិត្យ ត្រូវបានអនុវត្ត និង
- ប្រសិទ្ធភាពនៃសវនកម្មផ្ទៃក្នុងលើការសិក្សា និងវាយតម្លៃការត្រួតពិនិត្យ ដើម្បីប្រឆាំងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ។

៣៤.៨ ក្រុមប្រឹក្សាភិបាលត្រូវពិនិត្យឡើងវិញ និងវាយតម្លៃគោលការណ៍និងនីតិវិធីស្តីពីវិធានការប្រឆាំងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្មដែលស្របនឹងការផ្លាស់ប្តូរ និងការរីកចម្រើននៃផលិតផល សេវាកម្ម និងប្រព័ន្ធបច្ចេកវិទ្យា ព្រមទាំងស្របនឹងនិន្នាការនៃបច្ចេកទេសសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ។ គណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវទទួលខុសត្រូវក្នុងការអនុវត្តភាពផ្លាស់ប្តូរចាំបាច់លើគោលការណ៍និងនីតិវិធី ដោយមានការអនុមតិពីក្រុមប្រឹក្សាភិបាល ដើម្បីធានាថា គោលការណ៍ថ្មីនេះមានភាពរឹងមាំ និងសមស្រប ។

៣៤.៩ ក្រុមប្រឹក្សាភិបាល និងគណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវផ្តល់ការបណ្តុះបណ្តាល និងការអប់រំឱ្យបានគ្រប់គ្រាន់ដល់និយោជិតរបស់ខ្លួនស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ។

ប្រការ ៣៥.- សុចរិតភាពបុគ្គលិក

គណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវធានាថា គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ បង្កើតប្រព័ន្ធវាយតម្លៃនិយោជិត ដែលបានអនុម័តដោយក្រុមប្រឹក្សាភិបាល ដើម្បីពិនិត្យឱ្យបានគ្រប់គ្រាន់ ថាសុចរិតភាពបុគ្គលិករបស់ខ្លួនទាំងថ្មី និងចាស់ មិនត្រូវបានរំលោភ ។ ប្រព័ន្ធវាយតម្លៃនិយោជិតនេះ យ៉ាងហោចណាស់ត្រូវពិនិត្យមើលព័ត៌មានរបស់បុគ្គល រួមមានលិខិតថ្កោលទោស ប្រវត្តិការងារ និងហិរញ្ញវត្ថុរបស់បុគ្គលិកថ្មី ដែលជាផ្នែកមួយនៃដំណើរការជ្រើសរើសបុគ្គលិក ។

ប្រការ ៣៦.- មន្ត្រីប្រតិបត្តិ

៣៦.១ គណៈគ្រប់គ្រងជាន់ខ្ពស់ ទទួលខុសត្រូវតែងតាំងមន្ត្រីប្រតិបត្តិជាថ្នាក់នាយកគ្រប់គ្រងជាន់ខ្ពស់ ដោយមានការយល់ព្រមពីក្រុមប្រឹក្សាភិបាល ។ គណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវធានាថា មន្ត្រីប្រតិបត្តិអនុវត្តការទទួលខុសត្រូវចំពោះការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្មប្រកបដោយប្រសិទ្ធភាព ។ មន្ត្រីប្រតិបត្តិដើរតួជាអ្នកទំនាក់ទំនងសម្រាប់វិធានការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ដែលគ្រឹះស្ថានធនាគារ និងហិរញ្ញវត្ថុបានបង្កើត រួមមានការបណ្តុះបណ្តាលនិយោជិត និង ការរាយការណ៍ពីប្រតិបត្តិការសង្ស័យ ។

៣៦.២ នៅពេលតែងតាំង ឬផ្លាស់ប្តូរមន្ត្រីប្រតិបត្តិ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ត្រូវរាយការណ៍មកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុអំពីព័ត៌មានលំអិតនៃមន្ត្រីប្រតិបត្តិនោះ រួមមាន ឈ្មោះ អាសយដ្ឋាន លេខទូរស័ព្ទ លេខទូរសារ អាសយដ្ឋានអ៊ីមែល និងប្រវត្តិពាក់ព័ន្ធផ្សេងៗទៀត ។

៣៦.៣ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវកំណត់ និងចងក្រងជាឯកសារឱ្យបានច្បាស់លាស់ពីតួនាទី និងការទទួលខុសត្រូវរបស់មន្ត្រីប្រតិបត្តិ ។ តួនាទី និងការទទួលខុសត្រូវរបស់មន្ត្រីប្រតិបត្តិក្នុងការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម យ៉ាងហោចណាស់ ត្រូវធានាថា ៖

- អនុវត្តតាមគោលការណ៍នៃវិធានការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម
- អនុវត្តប្រកបដោយប្រសិទ្ធភាពនូវនីតិវិធីសមស្របស្តីពីការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម ដែលរួមមានគោលការណ៍ទទួលស្គាល់អតិថិជន ការយកចិត្តទុកដាក់ស្គាល់អតិថិជន ការរក្សាកំណត់ត្រា ការតាមដានបន្ត ការរាយការណ៍ពីប្រតិបត្តិការសង្ស័យ និង ការប្រឆាំងហិរញ្ញប្បទានភេរវកម្ម
- វាយតម្លៃទៀងទាត់លើយន្តការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ដើម្បីធានាថា យន្តការនោះមានលក្ខណៈគ្រប់គ្រាន់ឆ្លើយតបតាមនិន្នាការប្រែប្រួល
- បណ្តាញទំនាក់ទំនងទៅវិញទៅមកពីនិយោជិតទៅមន្ត្រីត្រូវបានរក្សាឱ្យមានសុវត្ថិភាព ហើយព័ត៌មានទាំងអស់ត្រូវបានរក្សាជាការសម្ងាត់
- អនុវត្តស្របតាមតម្រូវការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម
- និយោជិតទាំងអស់ត្រូវដឹងពីវិធានការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម រួមមានគោលការណ៍ យន្តការត្រួតពិនិត្យ និងបណ្តាញរាយការណ៍ ដើម្បីធានាពីប្រសិទ្ធភាពនៃវិធានការទាំងនោះ
- សំគាល់អត្តសញ្ញាណហានិភ័យនៃការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្មដែលពាក់ព័ន្ធនឹងផលិតផល ឬសេវាកម្មថ្មី ឬ ដែលកើតឡើងពីការប្រែប្រួលនៃប្រតិបត្តិការរបស់គ្រឹះស្ថានធនាគារ និង ហិរញ្ញវត្ថុ រួមមានការណែនាំឱ្យប្រើប្រាស់បច្ចេកវិទ្យាថ្មី និងដំណើរការថ្មី ។

៣៦.៤ មន្ត្រីប្រតិបត្តិត្រូវមានចំណេះដឹង និង ជំនាញចាំបាច់ ដើម្បីអនុវត្តការទទួលខុសត្រូវប្រកបដោយប្រសិទ្ធភាព រួមមានចំណេះដឹងពីកាតព្វកិច្ចប្រឆាំងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ដែលតម្រូវដោយច្បាប់ និងបទប្បញ្ញត្តិ ការវិវឌ្ឍន៍ និងបច្ចេកទេសថ្មីៗនៃការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ។

ប្រការ ៣៧.- កម្មវិធីបង្កើនការយល់ដឹង និងការបណ្តុះបណ្តាលបុគ្គលិក

៣៧.១ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវមានកម្មវិធីបណ្តុះបណ្តាល និងបង្កើនការយល់ដឹងស្តីពីវិធានការ និងការអនុវត្តការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្មសម្រាប់និយោជិតរបស់ខ្លួន ។

AML-CFT Prakas

៣៧.២ គណៈគ្រប់គ្រងជាន់ខ្ពស់ត្រូវធានាឱ្យមានបណ្តាញទំនាក់ទំនងសមស្រប ដើម្បីផ្តល់ព័ត៌មានដល់បុគ្គលិកគ្រប់ថ្នាក់របស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុស្តីពីគោលការណ៍ និងនីតិវិធីប្រឆាំងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្ម ។

៣៧.៣ និយោជិតត្រូវដឹងពីគោលការណ៍ការត្រួតពិនិត្យ និង កាតព្វកិច្ចប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្មដែលបានបញ្ជាក់នៅក្នុងប្រកាស និង នៅក្នុងក្បួនខ្នាតត្រួតពិនិត្យផ្ទៃក្នុងស្តីពីការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្មរបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ។

៣៧.៤ ក្បួនត្រួតពិនិត្យផ្ទៃក្នុងនៃការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម ត្រូវមានយ៉ាងហោចណាស់ ៖

- ច្បាប់ស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម
- ~~ប្រកាសស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម~~
- អនុសាសន៍ ៤០ និង អនុសាសន៍ពិសេស៩ របស់ក្រុមការងារហិរញ្ញវត្ថុ
- ឯកសារយកចិត្តទុកដាក់ស្គាល់អតិថិជនរបស់គណៈកម្មការបាសែលស្តីពីការត្រួតពិនិត្យធនាគារ និង
- វិធានការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្មរបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុដែលបានបង្កើតឡើង ដើម្បីបំពេញតម្រូវការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ។

៣៧.៥ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ យ៉ាងហោចណាស់ត្រូវអនុវត្តតាមតម្រូវការបណ្តុះបណ្តាលដូចខាងក្រោម សម្រាប់និយោជិតនៅតាមផ្នែកផ្សេងៗ ក្នុងគ្រឹះស្ថានរបស់ខ្លួន ៖

- **និយោជិតថ្មី**

  ប្រវត្តិទូទៅនៃការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម តម្រូវការនិងកាតព្វកិច្ចសំគាល់អត្តសញ្ញាណ និង រាយការណ៍ប្រតិបត្តិការសង្ស័យជូនបុគ្គល ដែលទទួលបានការតែងតាំងត្រឹមត្រូវក្នុងគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ហើយត្រូវទទួលបានការណែនាំឱ្យយល់ដឹងពីអត្ថប្រយោជន៍នៃការមិនបង្ហាញព័ត៌មានប្រាប់អតិថិជន ។

- **និយោជិតជួរមុខ**

  និយោជិតដែលទាក់ទងផ្ទាល់ជាមួយអតិថិជន ជាអ្នកទំនាក់ទំនងដំបូងជាមួយអ្នកសំអាតប្រាក់ និង អ្នកផ្តល់ហិរញ្ញប្បទានភេរវកម្មដែលមានសក្តានុពល ត្រូវបណ្តុះបណ្តាលអំពីការសំគាល់អត្តសញ្ញាណប្រតិបត្តិការសង្ស័យ និង វិធានការចាំបាច់ត្រូវអនុវត្តនៅពេលដែលប្រតិបត្តិការមួយមានលក្ខណៈគួរឱ្យសង្ស័យ កត្តាដែលអាចនាំដល់ការសង្ស័យ ការរាយការណ៍ប្រតិបត្តិការដែលមានចំនួនសាច់ប្រាក់ច្រើន និង ការពង្រឹងការយកចិត្តទុកដាក់ស្គាល់អតិថិជន ។

- **និយោជិត - ការបើកគណនី/អតិថិជនថ្មី**

និយោជិតដែលទទួលខុសត្រូវបើកគណនី ឬទទួលអតិថិជនថ្មី យ៉ាងហោចណាស់ត្រូវទទួលការបណ្តុះបណ្តាលដូចគ្នានឹងនិយោជិតជួរមុខ ។ លើសពីនេះ និយោជិតគ្រប់រូបត្រូវទទួលបានការបណ្តុះបណ្តាលពីការសំគាល់អត្តសញ្ញាណ និងការផ្ទៀងផ្ទាត់អតិថិជន ការបើកគណនី ឬការបង្កើតទំនាក់ទំនងអាជីវកម្មជាមួយអតិថិជន ។

- **អ្នកត្រួតពិនិត្យ និង អ្នកគ្រប់គ្រង**

កម្រិតខ្ពស់បំផុតនៃការណែនាំ ដែលគ្របដណ្តប់គ្រប់ទិដ្ឋភាពនៃនីតិវិធីប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្មត្រូវបានផ្តល់ទៅឱ្យអ្នកត្រួតពិនិត្យ និងអ្នកគ្រប់គ្រង ដែលរួមមានការពិន័យចំពោះការមិនគោរពតាមការតម្រូវនៃការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម និង នីតិវិធីកំណត់ការប្រឆាំងហិរញ្ញប្បទានភេរវកម្ម ។

៣៧.៦ កម្មវិធីបង្កើនការយល់ដឹង និង ការបណ្តុះបណ្តាលទាំងនេះត្រូវធ្វើឡើងជាទៀងទាត់ ដោយផ្តល់វគ្គសិក្សាថ្មីៗ ដល់និយោជិត ។ និយោជិតថ្មីត្រូវបណ្តុះបណ្តាលក្នុងរយៈពេលបីខែមុនការចាប់ផ្តើមបំពេញការងារ ហើយចំពោះនិយោជិតជួរមុខ អ្នកត្រួតពិនិត្យ និងអ្នកគ្រប់គ្រងត្រូវផ្តល់វគ្គសិក្សាថ្មីៗប្រចាំឆ្នាំ ។

ប្រការ ៣៨.- សវនកម្មផ្ទៃក្នុង

៣៨.១ ក្រុមប្រឹក្សាភិបាលត្រូវធានាថា សវនករផ្ទៃក្នុងត្រួតពិនិត្យប្រសិទ្ធភាព និងការប្រតិបត្តិតាមតម្រូវការប្រឆាំងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្មដែលមានក្នុងច្បាប់ បទប្បញ្ញត្តិ និងប្រកាសនេះ ។

៣៨.២ ក្រុមប្រឹក្សាភិបាលត្រូវកំណត់ និង រៀបចំឯកសារឱ្យបានច្បាស់លាស់ពីតួនាទី និងការទទួលខុសត្រូវរបស់សវនករផ្ទៃក្នុង យ៉ាងហោចណាស់ត្រូវមាន ÷

- ការសាកល្បងប្រសិទ្ធភាពនៃគោលការណ៍ នីតិវិធី និងការត្រួតពិនិត្យលើវិធានការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម
- ការធានាប្រសិទ្ធភាពនៃយន្តការត្រួតពិនិត្យការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម រួមមានការតែងតាំងមន្ត្រីប្រតិបត្តិ កម្មវិធីបង្កើនការយល់ដឹង និងការបណ្តុះបណ្តាលបុគ្គលិក យន្តការពិនិត្យតាមដាននិយោជិត ក្បួនផ្ទៃក្នុងស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម និង
- ការធានាថា វិធានការបានបង្កើតស្របគ្នានឹងការរីកចម្រើន និងបំរែបំរួលបច្ចុប្បន្ននៃតម្រូវការប្រឆាំងការសំអាតប្រាក់ និងហិរញ្ញប្បទានភេរវកម្មដែលជាប់ពាក់ព័ន្ធ ។

៣៨.៣ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវជូនដំណឹងមកអង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុ និងធនាគារជាតិនៃកម្ពុជា ពីការតែងតាំង ឬការផ្លាស់ប្តូរសវនករផ្ទៃក្នុង និងពិធីសាស្ត្រនិងនីតិវិធី ដែលបានអនុវត្តដោយសវនករផ្ទៃក្នុង ។

៣៨.៤ សវនករផ្ទៃក្នុងត្រូវបញ្ជូនរបាយការណ៍ជាលាយល័ក្ខណ៍អក្សរ ពីការរកឃើញសវនកម្មទៅក្រុមប្រឹក្សាភិបាលឱ្យបានទៀងទាត់ ។ របាយការណ៍សវនកម្មប្រចាំឆ្នាំត្រូវបានប្រើប្រាស់ ដើម្បីគូសបញ្ជាក់ពីភាពមិនគ្រប់គ្រាន់នៃវិធានការ និងប្រព័ន្ធត្រួតពិនិត្យការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម នៅក្នុងគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ហើយក្រុមប្រឹក្សាភិបាលត្រូវចាត់វិធានការចាំបាច់ក្នុងការកែតម្រូវស្ថានការណ៍នេះ ។ គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុត្រូវបញ្ជូនការរកឃើញ និងរបាយការណ៍សវនកម្មបែបនេះមកធនាគារជាតិនៃកម្ពុជា ឱ្យបានទៀងទាត់ក្រោយពីបានអនុម័តដោយក្រុមប្រឹក្សាភិបាល ។

ប្រការ ៣៩.-

ប្រកាសនេះជំនួស និងនិរាករណ៍ប្រកាសស្តីពីនីតិវិធីជាបទដ្ឋានសម្រាប់ការកំណត់អត្តសញ្ញាណនៃការសំអាតប្រាក់នៅគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ដែលបានប្រកាសឱ្យប្រើនៅថ្ងៃទី ២១ ខែតុលា ឆ្នាំ ២០០២ និង សារាចរណែនាំ ស្តីពីប្រតិបត្តិការសង្ស័យ និង គោលនយោបាយស្គាល់អតិថិជនដែលបានប្រកាសឱ្យប្រើនៅថ្ងៃទី ០៤ ខែតុលា ឆ្នាំ ២០០៣។

ប្រការ ៤០.-

អគ្គនាយកដ្ឋាន អគ្គលេខាធិការដ្ឋាន អគ្គបេឡា អគ្គាធិការដ្ឋាន គ្រប់នាយកដ្ឋាន អង្គភាព និងគ្រប់គ្រឹះស្ថានធនាគារ និងហិរញ្ញវត្ថុនៅក្រោមឱវាទ និងក្រោមអាណាព្យាបាលធនាគារជាតិនៃកម្ពុជាត្រូវអនុវត្តម៉ឺងម៉ាត់នូវប្រកាសនេះតាមភារកិច្ចរៀង១ខ្លួន។

ប្រការ ៤១.-

ប្រកាសនេះមានប្រសិទ្ធភាពអនុវត្តចាប់ពីថ្ងៃចុះហត្ថលេខានេះតទៅ ។

រាជធានីភ្នំពេញ ថ្ងៃទី ៣០ ខែឧសភា ឆ្នាំ ២០០៨

ទេសាភិបាល

ជា_ចាន់តូ

<u>កន្លែងទទួល</u>

- ដូចប្រការ ៤០ "ដើម្បីអនុវត្ត"
- កាលប្បវត្តិ
- ឯកសារ

<u>ចម្លងជូន</u>

- គ្រប់សមាជិកក្រុមប្រឹក្សាភិបាល
- ទីស្តីការគណៈរដ្ឋមន្ត្រី "ដើម្បីជ្រាបជាព័ត៌មាន"
- នាយកដ្ឋានរដ្ឋបាលនៃទីស្តីការគណៈរដ្ឋមន្ត្រី "ដើម្បីចុះផ្សាយក្នុងរាជកិច្ច"

ឧបសម្ព័ន្ធទី ១ នៃប្រកាសស្តីពីការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម

ការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម

យោងតាមច្បាប់ស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម

ការសំអាតប្រាក់មានន័យថា៖

១. ការបំប្លែង ឬការផ្ទេរទ្រព្យសម្បត្តិដោយដឹងថា ទ្រព្យសម្បត្តិនេះជាផលនៃបទល្មើសក្នុងគោលបំណងបិទបាំង ឬក្លែងប្រភពដើមមិនស្របច្បាប់នៃទ្រព្យសម្បត្តិទាំងនេះ ឬជួយបុគ្គលណាដែលបានពាក់ព័ន្ធក្នុងបទល្មើស ដើម្បីឱ្យបុគ្គលនោះគេចផុតពីផលវិបាកតាមផ្លូវច្បាប់នូវសកម្មភាពរបស់ខ្លួន ។

២. ការបិទបាំង ឬ ការក្លែងសភាវៈពិត ប្រភព ទីតាំង សិទ្ធិចាត់ចែង ចលនា ឬ កម្មសិទ្ធិ ឬ សិទ្ធិលើទ្រព្យ ~~សម្បត្តិ ដោយដឹងថាទ្រព្យសម្បត្តិទាំងនេះបានមកពីបទល្មើស ។~~

៣. ការធ្វើលទ្ធកម្ម ការកាន់កាប់ ឬ ការប្រើប្រាស់ទ្រព្យសម្បត្តិ ដោយដឹងថាទ្រព្យសម្បត្តិទាំងនេះបានមកពីបទល្មើស ។

៤. ការចូលរួម ការប៉ុនប៉ងប្រព្រឹត្ត ដោយជួយ និងជម្រុញឱ្យប្រព្រឹត្តសកម្មភាពណាមួយដែលបានកំណត់ស្របតាមមាត្រា ៣ នៃច្បាប់ស្តីពីការប្រឆាំងការសំអាតប្រាក់និងហិរញ្ញប្បទានភេរវកម្ម ។

ហិរញ្ញប្បទានភេរវកម្ម គឺជាការផ្តល់ដោយចេតនានូវសេវាហិរញ្ញវត្ថុ ឬ សេវាផ្សេងទៀត ក្នុងគោលបំណងប្រើប្រាស់សេវានេះ ឬដោយដឹងថាមូលនិធិនេះនឹងត្រូវបាន ឬ អាចប្រើទាំងមូល ឬ មួយផ្នែកសម្រាប់គាំទ្រភេរវកម្ម សកម្មភាពរបស់ភេរវករ ឬ អង្គការចាត់តាំងរបស់ភេរវកម្ម ។

ឧបសម្ព័ន្ធទី ២ នៃប្រកាស ស្ដីពី ការប្រឆាំងការសំអាតប្រាក់ និង ហិរញ្ញប្បទានភេរវកម្ម

ឧទាហរណ៍នៃប្រតិបត្តិការសង្ស័យ

ប្រតិបត្តិការសាច់ប្រាក់ ការដាក់ប្រាក់បញ្ញើ និង ការដកប្រាក់បញ្ញើ

១. ការដាក់ប្រាក់បញ្ញើជាសាច់ប្រាក់ដែលមានចំនួនច្រើនខុសប្រក្រតី ដោយឯកត្តបុគ្គល ឬក្រុមហ៊ុនដែលសកម្មភាពអាជីវកម្មរបស់គេធ្វើឡើងតាមរយៈមូលប្បទានប័ត្រ និងឧបករណ៍ដទៃទៀត ។

២. ការកើនឡើងយ៉ាងគំហុកនៃការដាក់ប្រាក់បញ្ញើជាសាច់ប្រាក់របស់ឯកត្តបុគ្គល ឬ អាជីវកម្មណាមួយដោយគ្មានមូលហេតុជាក់ស្ដែង ជាពិសេសប្រសិនបើ ប្រាក់បញ្ញើនេះត្រូវបានផ្ទេរក្នុងកំឡុងពេលដ៏ខ្លី ចេញពីគណនី និង/ឬ ទៅកាន់ទិសដៅដែលជាធម្មតាមិនជាប់ពាក់ព័ន្ធនឹងអតិថិជន ។

៣. គណនីក្រុមហ៊ុនមានប្រតិបត្តិការដាក់ និងដកជាសាច់ប្រាក់ ជាជាងប្រតិបត្តិការដែលធ្វើឡើងតាមរូបភាពជាឥណទាន ឬឥណពន្ធដែលជាធម្មតាជាប់ពាក់ព័ន្ធនឹងប្រតិបត្តិការអាជីវកម្ម (មូលប្បទានប័ត្រ លិខិតឥណទាន រូបិយាណត្តិ ។ល។) ។

៤. អតិថិជនដែលជានិច្ចកាល បង់ជាសាច់ប្រាក់ ដើម្បីស្នើសុំមូលប្បទានប័ត្រធនាគារ ការផ្ទេរប្រាក់ ឬ ឧបករណ៍រូបិយវត្ថុ ដែលអាចជួញដូរបាន ឬ ដែលអាចទូទាត់បានផ្សេងៗទៀត ។

៥. អតិថិជនដែលយកក្រដាសប្រាក់ប្រភេទតូចៗមានបរិមាណច្រើនមកប្ដូរយកក្រដាសប្រាក់ប្រភេទធំៗ ។

៦. សាខាធនាគារ និងគ្រឹះស្ថានហិរញ្ញវត្ថុដែលមានប្រតិបត្តិការជាសាច់ប្រាក់ច្រើនជាងធម្មតា (ស្ថិតិរបស់ទីស្នាក់ការកណ្ដាលបង្ហាញភាពមិនប្រក្រតីនៃប្រតិបត្តិការជាសាច់ប្រាក់) ។

៧. អតិថិជនដែលដាក់ប្រាក់បញ្ញើ ក្នុងនោះមានក្រដាសប្រាក់ ឬ ឧបករណ៍ទូទាត់ក្លែងក្លាយ ។

៨. អតិថិជនដែលផ្ទេរប្រាក់មានចំនួនច្រើនទៅ ឬមកពីបរទេស ដោយបញ្ជាឱ្យទូទាត់ជាសាច់ប្រាក់ ។

៩. ការទិញ ឬលក់រូបិយប័ណ្ណបរទេសដែលមានចំនួនច្រើន ដោយទូទាត់ជាសាច់ប្រាក់ ទោះបីជាអតិថិជនមានគណនីជាមួយធនាគារក៏ដោយ ។

១០. អតិថិជនដែលដាក់ប្រាក់បញ្ញើជាញឹកញាប់ ហើយមានចំនួនច្រើន ប៉ុន្តែ មូលប្បទានប័ត្រដែលដកប្រាក់ពីគណនីនោះត្រូវបានទូទាត់ឱ្យឯកត្តបុគ្គល និងក្រុមហ៊ុន ដែលជាធម្មតាមិនជាប់ពាក់ព័ន្ធនឹងអាជីវកម្មលក់រាយរបស់គេ ។

១១. ប្រាក់បញ្ញើរបស់អង្គភាពអាជីវកម្ម ដោយរួមបញ្ចូលឧបករណ៍រូបិយវត្ថុដែលជាធម្មតា មិនជាប់ពាក់ព័ន្ធនឹងអាជីវកម្មបែបនោះ ។

១២. ការរួមបញ្ចូលគ្នានៃការដាក់ប្រាក់បញ្ញើជាសាច់ប្រាក់និងឧបករណ៍រូបិយវត្ថុទៅក្នុងគណនីមួយ ដែលប្រតិបត្តិការបែបនេះហាក់ដូចជាមិនជាប់ពាក់ព័ន្ធនឹងការប្រើប្រាស់ជាធម្មតានៃគណនីនេះ ។

១៣. ប្រតិបត្តិការចំរុះដែលធ្វើឡើងក្នុងថ្ងៃតែមួយនៅសាខាតែមួយរបស់គ្រឹះស្ថានហិរញ្ញវត្ថុតែមួយ ប៉ុន្តែមានការប៉ុនប៉ងជាក់ស្តែង ដោយប្រើប្រាស់បេឡាករផ្សេងគ្នា ។

១៤. ការបែងចែកប្រាក់បញ្ញើតាមរយៈសាខាផ្សេងៗរបស់គ្រឹះស្ថានហិរញ្ញវត្ថុតែមួយ ឬតាមរយៈបុគ្គល ច្រើនរូបដែលចូលមកសាខាតែមួយក្នុងពេលដូចគ្នា ។

១៥. ការដាក់ ឬការដកសាច់ប្រាក់ ក្នុងចំនួនមួយទាបជាងតិចតួចនៃកម្រិតកំណត់លើការសំគាល់អត្តសញ្ញាណ ឬ លើកម្រិតរាយការណ៍ ។

១៦. អតិថិជនបង្ហាញប្រាក់ដែលមិនទាន់រាប់ ហើយបន្ទាប់ពីរាប់រួចអតិថិជននោះកាត់បន្ថយចំនួនប្រាក់ឱ្យនៅទាបជាងកម្រិតមួយដែលតម្រូវឱ្យរាយការណ៍ ឬសំគាល់អត្តសញ្ញាណ ។

១៧. ការដាក់ ឬ ដកឧបករណ៍រូបិយវត្ថុចំរុះ ត្រឹមចំនួនមួយទាបជាងតិចតួចនៃកម្រិតកំណត់ដែលត្រូវ រាយការណ៍ ~~ឬ សំគាល់អត្តសញ្ញាណ ជាពិសេសប្រសិនបើឧបករណ៍នោះមានចុះលេខតាមលំដាប់លំដោយ ។~~

គណនី

១៨. គណនីដែលដើរតួនាទីគណនីឆ្លងកាត់ (Pass through account) ដោយមានចំនួនឥណទាន និង ឥណពន្ធច្រើន ហើយសមតុល្យជាមធ្យមប្រចាំខែទាប ។

១៩. អតិថិជនដែលមានបំណងថែរក្សាគណនីអតិថិជន ឬ គណនីអ្នកទទួលអាណត្តិព្យាបាល ដែលមិនស៊ីសង្វាក់គ្នាទៅនឹងប្រភេទអាជីវកម្ម រួមទាំងប្រតិបត្តិការអាជីវកម្ម ដែលជាប់ពាក់ព័ន្ធនឹងឈ្មោះអ្នកតំណាង ។

២០. ការបើកគណនីច្រើនដោយបុគ្គលមួយរូប ដោយដាក់ប្រាក់បញ្ញើមានចំនួនតិចតួចជាច្រើន ដែលសរុបចំនួនទាំងអស់មិនស៊ីគ្នានឹងប្រាក់ចំណូលដែលបានរំពឹងទុករបស់បុគ្គលនោះ ។

២១. បុគ្គល ឬក្រុមហ៊ុនដែលមានគណនី មិនមានបង្ហាញពីសកម្មភាពធនាគារ ឬអាជីវកម្មផ្ទាល់ប្រក្រតី ប៉ុន្តែត្រូវបានប្រើប្រាស់ដើម្បីទទួល ឬបញ្ចេញប្រាក់ចំនួនច្រើន ដោយគ្មានគោលបំណង ឬទំនាក់ទំនងជាក់លាក់ចំពោះម្ចាស់គណនី និង/ឬ អាជីវកម្មរបស់គាត់ (ឧទាហរណ៍ កំណើនដ៏ច្រើននៃផលចំណូលលើគណនី) ។

២២. ការស្ទាក់ស្ទើរក្នុងការផ្តល់ព័ត៌មាននៅពេលបើកគណនី ការប៉ុនប៉ងកាត់បន្ថយកម្រិតព័ត៌មានឱ្យដល់កម្រិតអប្បបរមា ឬព័ត៌មានដែលត្រូវផ្តល់ឱ្យ មានការលំបាក ឬតម្លៃថ្លៃ សម្រាប់គ្រឹះស្ថានធនាគារ និង ហិរញ្ញវត្ថុផ្ទៀងផ្ទាត់ ។

២៣. អតិថិជនដែលមានគណនីនៅគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុជាច្រើនដែលស្ថិតក្នុងតំបន់តែមួយ ហើយប្រមូលប្រាក់ពីគណនីនៅគ្រឹះស្ថានផ្សេងៗនោះ ផ្ទេរទៅគណនីរបស់តតិយភាគី ជាទៀងទាត់ ។

២៤. ទូទាត់ជាមូលប្បទានប័ត្រមានចំនួនទឹកប្រាក់ច្រើនរបស់តតិយភាគី ដែលត្រូវបានបិដ្ឋិលេខដើម្បីជាផលប្រយោជន៍អតិថិជន ។

២៥. គណនីមិនដំណើរការដែលមានចំនួនទឹកប្រាក់តិចតួច ស្រាប់តែមួយរំពេចទទួលបានប្រាក់បញ្ញើជាច្រើន ហើយបន្ទាប់មកត្រូវបានដកចេញវិញជារៀងរាល់ថ្ងៃ រហូតដល់ចំនួនប្រាក់ផ្ទេរចូលនោះត្រូវបានដកអស់ ។

២៦. ការប្រើប្រាស់ឧបករណ៍ដាក់ប្រាក់សុវត្ថិភាពច្រើនដែលមិនស៊ីគ្នានឹងទំហំអាជីវកម្មរបស់អតិថិជន ។

២៧. អតិថិជនដែលចៀសវាងមិនធ្វើការទាក់ទង ជាមួយបុគ្គលិករបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុសម្រាប់ការធ្វើប្រតិបត្តិការអាជីវកម្ម ។

២៨. កំណើនការដាក់ប្រាក់បញ្ញើជាសាច់ប្រាក់ច្រើន ឬឧបករណ៍អាចជួញដូរបានរបស់ក្រុមហ៊ុន ឬសហគ្រាសវិជ្ជាជីវៈ ដោយប្រើប្រាស់គណនីរបស់អតិថិជន ឬក្រុមហ៊ុនក្នុងស្រុក ឬគណនីអាណត្តិព្យាបាល (Trust Account) ជាពិសេស ប្រសិនបើ ការដាក់ប្រាក់បញ្ញើទាំងនោះត្រូវបានផ្ទេរភ្លាមៗ រវាងគណនីក្រុមហ៊ុនរបស់អតិថិជន ផ្សេងទៀត និង គណនីអាណត្តិព្យាបាល ។

២៩. អតិថិជនដែលបដិសេធមិនព្រមផ្តល់ព័ត៌មាន ដែលក្នុងកាលៈទេសៈធម្មតា អាចធ្វើឱ្យអតិថិជនមានសិទ្ធិទទួលបានឥណទាន ឬទទួលបានសេវាកម្មធនាគារដទៃទៀត ដែលត្រូវបានចាត់ទុកថាមានតម្លៃ ។

៣០. បុគ្គលច្រើនរូប ដែលធ្វើការទូទាត់ទៅកាន់គណនីតែមួយ ដោយពុំមានការពន្យល់ឱ្យបានគ្រប់គ្រាន់ ។

៣១. មូលនិធិ ដែលឆ្លងកាត់គណនីដ៏លឿន ឧទាហរណ៍ដូចជា សមតុល្យដើមគ្រា និងចុងគ្រាប្រចាំថ្ងៃ មានចំនួនទាប ដែលមិនឆ្លុះបញ្ចាំងទៅនឹងបរិមាណដ៏ច្រើននៃលំហូរប្រាក់ដុល្លារឆ្លងកាត់គណនីមួយ ។

៣២. គណនីដែលបានបើកក្នុងនាម អ្នកប្តូរប្រាក់ដែលទទួលប្រាក់បញ្ញើតាមការចាត់ចែង (ឧទាហរណ៍ ចំនួនប្រាក់បញ្ញើថេរ ជាទៀងទាត់) ។

៣៣. គណនី ដែលបានធ្វើប្រតិបត្តិការក្នុងនាមក្រុមហ៊ុនបរទេសជាមួយនឹងចលនាមូលនិធិតាមការចាត់ចែង ។

៣៤. គណនីដែលទទួលបានប្រាក់បញ្ញើម្តងម្កាល ហើយក្នុងអំឡុងពេលខ្លះ គណនីនេះមិនមានសកម្មភាព ។ ដូច្នេះ គណនីបែបនេះត្រូវបានប្រើប្រាស់ ដើម្បីធ្វើឱ្យមានភាពស្របច្បាប់នៃប្រភពហិរញ្ញវត្ថុដែលសកម្មភាពក្លែងបន្លំបន្ថែមទៀតអាចត្រូវបានធ្វើឡើង ។

៣៥. គណនីដែលមានសិទ្ធិចុះហត្ថលេខាពីបុគ្គលច្រើនគ្នា ប៉ុន្តែ បុគ្គលទាំងនោះមិនមានទំនាក់ទំនងរវាងគ្នា នឹងគ្នាទាំងក្នុងចំណងទាក់ទងជាគ្រួសារ ឬអាជីវកម្ម ។

៣៦. គណនីដែលបើកដោយស្ថាប័ន ឬអង្គការស្របច្បាប់ដែលមានអាសយដ្ឋានដូចគ្នានឹងស្ថាប័ន ឬអង្គការស្របច្បាប់ដទៃទៀត ប៉ុន្តែបុគ្គលតែមួយ ឬបុគ្គលផ្សេងទៀតមានសិទ្ធិចុះហត្ថលេខា នៅពេលដែលមិនមានហេតុផលខាងផ្លូវច្បាប់ ឬសេដ្ឋកិច្ចជាក់ស្តែង សម្រាប់ការចាត់ចែងបែបនោះ (ឧទាហរណ៍ បុគ្គលមួយចំនួនដែលបម្រើការជានាយកសម្រាប់ក្រុមហ៊ុនច្រើន ដែលមានទីស្នាក់ការកណ្តាលនៅតំបន់តែមួយ ។ល។) ។

៣៧. គណនីដែលបានបើកក្នុងនាមស្ថាប័នស្របច្បាប់ដែលទើបតែបង្កើតឡើងថ្មីៗ ហើយកម្រិតនៃប្រាក់បញ្ញើខ្ពស់ជាងការរំពឹងទុក បើប្រៀបធៀបទៅនឹងប្រាក់ចំណូលរបស់ស្ថាបនិកនៃស្ថាប័ននោះ ។

៣៨. គណនីដែលបានបង្កើតក្នុងនាមស្ថាប័នស្របច្បាប់ ដែលជាប់ពាក់ព័ន្ធនឹងសកម្មភាពរបស់សមាគម ឬ អង្គការមូលនិធិដែលមានគោលដៅជាប់ពាក់ព័ន្ធនឹងការទាមទារ ឬ តម្រូវការរបស់អង្គការភេរវកម្ម ។

៣៩. គណនីដែលបានបង្កើតក្នុងនាមស្ថាប័នស្របច្បាប់ សមាគម ឬអង្គការមូលនិធិដែលអាចជាប់ទាក់ទងនឹងអង្គការភេរវកម្ម ហើយដែលបង្ហាញពីចលនាប្រាក់ខ្ពស់ជាងកំរិតប្រាក់ចំណូល ដែលបានរំពឹងទុក ។

ធនាគារកម្មអន្តរជាតិ និងហិរញ្ញប្បទានពាណិជ្ជកម្ម

៤០. អតិថិជនដែលត្រូវបានណែនាំឱ្យស្គាល់ដោយសាខា បុត្រសម្ព័ន្ធបរទេស ឬធនាគារផ្សេងៗទៀតដែលមានមូលដ្ឋាននៅក្នុងតំបន់សង្ស័យ (ឧទាហរណ៍ដូចជា ប្រទេសដែលគ្របដណ្តប់ដោយការផលិត គ្រឿងញៀន ឬ ចរាចរគ្រឿងញៀន ប្រទេសដែលកំណត់ដោយអាជ្ញាធរជាតិដែនដី ឬប្រទេសដែលមិនមានកិច្ចសហប្រតិបត្តិការរបស់ក្រុមការងារហិរញ្ញវត្ថុ) ។

៤១. ការប្រើប្រាស់លិខិតឥណទាន និងវិធីសាស្ត្រដទៃទៀតនៃហិរញ្ញប្បទានពាណិជ្ជកម្ម ដើម្បីចលនាមូលនិធិពីប្រទេសមួយទៅប្រទេសមួយដែលពាណិជ្ជកម្មបែបនេះ មិនស៊ីសង្វាក់គ្នាទៅនឹងសកម្មភាពអាជីវកម្មធម្មតារបស់អតិថិជន ។

៤២. អតិថិជនដែលទូទាត់ចំនួនប្រាក់ច្រើនហើយទៀងទាត់ រួមមានប្រតិបត្តិការតាមអេឡិចត្រូនិក (Wire transaction) ដែលមិនអាចសំគាល់អត្តសញ្ញាណឱ្យបានច្បាស់លាស់ ជាប្រតិបត្តិការពិតប្រាកដ ឬទទួលការទូទាត់ចំនួនច្រើន និងទៀងទាត់ពីប្រទេសដែលជាប់ពាក់ព័ន្ធនឹងការផលិត ការកែច្នៃ ឬលក់គ្រឿងញៀនដោយអង្គការភេរវកម្ម ឬកន្លែងគ្មានពន្ធ (Tax havens) ។

៤៣. បង្កើតសមតុល្យមានចំនួនច្រើន មិនស្របនឹងផលចំណូលដែលបានដឹងនៃអាជីវកម្មរបស់អតិថិជន និង ការផ្ទេរជាបន្តបន្ទាប់ទៅកាន់គណនីនៅបរទេស ។

៤៤. ការផ្ទេរមូលនិធិតាមអេឡិកត្រូនិកដែលមិនមានការពន្យល់ដោយអតិថិជន ចេញ ឬចូល ឬគ្មានការឆ្លងកាត់តាមរយៈគណនី ។

៤៥. ការស្នើសុំជារឿយៗ ឬការទូទាត់នូវមូលប្បទានប័ត្រទេសចរណ៍ ឬរូបិយណត្តិជារូបិប័ណ្ណបរទេស ឬ ឧបករណ៍អាចជួញដូរបានផ្សេងទៀត ដែលបានចេញផ្សាយ ឬជួញដូរពីបរទេស ។

៤៦. អតិថិជនដែលផ្ញើ ឬទទួលការផ្ទេរតាមអេឡិចត្រូនិកទៅកាន់/មកពីប្រទេសគ្មានពន្ធ (Tax havens countries) ជាពិសេសប្រសិនបើ មិនមានហេតុផលអាជីវកម្មជាក់ស្តែង សម្រាប់ការផ្ទេរប្រាក់បែបនេះ ឬការផ្ទេរដែលមិនសមស្របទៅនឹងសកម្មភាពអាជីវកម្ម ឬប្រវត្តិរបស់អតិថិជន ។

និយោជិត និងភ្នាក់ងាររបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ

៤៧. ការផ្លាស់ប្តូរអាកប្បកិរិយារបស់និយោជិត ឧទាហរណ៍ ជីវភាពរស់នៅ ដែលមានការចាយវាយច្រើន ការចៀសវាងមិនឈប់សំរាកក្នុងពេលវិស្សមកាល ។

៤៨. ការប្រែប្រួលលទ្ធផលការងាររបស់និយោជិត និងភ្នាក់ងារ ឧទាហរណ៍ដូចជា បុគ្គលិកផ្នែកលក់ ផលិតផល ជាសាច់ប្រាក់ដែលមានលទ្ធផលការងារកើនឡើង ដោយឥតរំពឹងទុក និងគួរឱ្យកត់សំគាល់ ។

៤៩. កិច្ចព្រមព្រៀងណាមួយជាមួយភ្នាក់ងារដែលអត្តសញ្ញាណរបស់អត្ថគាហកចុងក្រោយ ឬសមភាគីមិនត្រូវបានបញ្ចេញឱ្យដឹង ដែលមានលក្ខណៈផ្ទុយនឹងនីតិវិធីធម្មតាសម្រាប់ប្រភេទអាជីវកម្ម ។

៥០. លទ្ធផលការងារខ្លាំងភ្លាមៗរបស់បុគ្គលិកក្នុងការទំនាក់ទំនងជាពិសេស ឬក្នុងទំនាក់ទំនងសេវាធនាគារជាសម្ងាត់ ដូចជា សេវាកម្មធនាគារឯកជន ឬសេវាអាណត្តិព្យាបាល ឬការកើនឡើងភ្លាមៗនៃទ្រព្យសម្បត្តិ/ការចំណាយរបស់បុគ្គលិកនោះ ។

ធនាគារកម្មឯកជន និង សេវាកម្មអាណត្តិព្យាបាល

៥១. អ្នកផ្តល់គណនីធនាគារកម្មឯកជន និងគណនីអាណត្តិព្យាបាលដែលផ្ទេរឥណទានពីគណនីរបស់ពួកគេ ទៅឱ្យភាគីផ្សេងទៀត ឬអត្ថប្រយោជន៍អាជីវកម្មនៃភ្នាក់ងារកាន់កាប់គណនី ឬអត្ថគាហកផ្សេងទៀត ។

កម្ចីដែលមាន និងគ្មានការធានា

៥២. អតិថិជនដែលទូទាត់ឥណទានមានបញ្ហា ដោយឥតរំពឹងទុក ។

៥៣. ការស្នើសុំខ្ចីដោយដាក់បញ្ចាំទ្រព្យសម្បត្តិនៅគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ឬនៅតតិយភាគីដែលប្រភពដើមរបស់ទ្រព្យសម្បត្តិនោះមិនត្រូវបានដឹង ឬទ្រព្យសម្បត្តិនោះមិនស៊ីសង្វាក់គ្នានឹងស្ថានភាពរបស់អតិថិជន ។

៥៤. សំណើសុំរបស់អតិថិជនឱ្យគ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុផ្តល់ ឬចាត់ចែងការរួមចំណែកហិរញ្ញវត្ថុដល់កិច្ចសន្យាណាមួយដែលមិនមានភាពច្បាស់លាស់ ជាពិសេសជាប់ពាក់ព័ន្ធទៅនឹងទ្រព្យសម្បត្តិ ។

៥៥. អតិថិជនដែលទូទាត់សងដោយផ្នែក ឬទាំងស្រុង ចំពោះឥណទានដែលមានវត្ថុបញ្ចាំជាអចលនទ្រព្យ (Mortgage Loan) និងទ្រព្យផ្សេងៗទៀតដែលមិនមានភាពស៊ីគ្នានឹងសមត្ថភាពរកចំណូល ឬ មូលដ្ឋានទ្រព្យសកម្មរបស់ពួកគេ ។

ការផ្ទេរប្រាក់តាមអេឡិចត្រូនិក (Wire Transfer)

៥៦. ការផ្ទេរតាមអេឡិចត្រូនិកដែលតម្រូវឱ្យធ្វើឡើងមានចំនួនតិចតួច ដោយព្យាយាមចៀសវាងតម្រូវការនៃការសំគាល់អត្តសញ្ញាណ ឬរាយការណ៍ ។

៥៧. ការផ្ទេរតាមអេឡិចត្រូនិកទៅកាន់ ឬ សម្រាប់បុគ្គលដែលមិនត្រូវបានគេផ្តល់ឱ្យព័ត៌មានស្តីពីអ្នកផ្តើមប្រតិបត្តិការ ឬពីបុគ្គលដែលធ្វើប្រតិបត្តិការជំនួស ។

៥៨. ការប្រើប្រាស់គណនីអាជីវកម្ម ឬផ្ទាល់ខ្លួនចំរុះ ឬ គណនីរបស់អង្គការមិនរកប្រាក់ចំណេញ ឬ សប្បុរសធម៌ដើម្បីប្រមូល និងបន្ទាប់មកបង្វែរមូលនិធិភ្លាមៗឬក្នុងរយៈពេលដ៏ខ្លីទៅឱ្យអត្ថគាហកតូចៗ នៅបរទេស ។

បុគ្គលិកលក្ខណៈរបស់អតិថិជន ឬ សកម្មភាពអាជីវកម្មរបស់គេ

៥៩. មូលនិធិបានមកពីអាជីវកម្ម ដែលជាកម្មសិទ្ធិរបស់បុគ្គលមួយចំនួន ឬជាប់ពាក់ព័ន្ធនឹងបុគ្គលមួយចំនួន ដែលមានប្រភពដើមមកពីប្រទេស ដែលមានការព្រួយបារម្ភដូចគ្នា ដោយធ្វើសកម្មភាពជាតំណាងឱ្យប្រភេទអាជីវកម្មស្រដៀងគ្នា ។

៦០. អាសយដ្ឋានរួមគ្នារបស់បុគ្គលមួយចំនួនដែលពាក់ព័ន្ធនឹងប្រតិបត្តិការជាសាច់ប្រាក់ ជាពិសេសនៅពេលដែលអាសយដ្ឋានជាទីតាំងអាជីវកម្ម និង/ឬ ហាក់ដូចជាទាក់ទងនឹងមុខរបរ ដែលបានលើកឡើង (ឧទាហរណ៍ ដូចជា និស្សិត បុគ្គលគ្មានមុខរបរ បុគ្គលដែលធ្វើការងារដោយខ្លួនឯង ។ល។) ។

៦១. មុខរបរដែលបានលើកឡើងរបស់អតិថិជនមិនស៊ីគ្នាទៅនឹងកម្រិត ឬប្រភេទសកម្មភាព (ឧទាហរណ៍ ដូចជា និស្សិត ឬបុគ្គលគ្មានមុខរបរដែលទទួល ឬផ្ញើប្រាក់ចំនួនច្រើនតាមអេឡិចត្រូនិក ឬដកប្រាក់ជារៀងរាល់ពេលនូវចំនួនអតិបរមា នៅទីកន្លែងជាច្រើននៃតំបន់ភូមិសាស្ត្រដ៏ធំទូលាយមួយ) ។

៦២. ទាក់ទិននឹងអង្គការមិនរកប្រាក់ចំណេញ ឬសប្បុរសធម៌ ប្រតិបត្តិការហិរញ្ញវត្ថុត្រូវធ្វើឡើង ដោយមិនមានគោលបំណងសេដ្ឋកិច្ចសមហេតុផល ឬមិនជាប់ពាក់ព័ន្ធទៅនឹងសកម្មភាពអង្គការនោះ និង ភាគីផ្សេងទៀត នៅក្នុងប្រតិបត្តិការនេះ ។

៦៣. ភាពមិនស៊ីសង្វាក់គ្នាដែលមិនមានការពន្យល់ ដែលកើតចេញពីដំណើរការនៃការសំគាល់អត្តសញ្ញាណ ឬការផ្ទៀងផ្ទាត់អតិថិជន (ឧទាហរណ៍ ប្រទេសតាំងទីលំនៅបច្ចុប្បន្ន ឬពីមុន ប្រទេសដែលចេញលិខិតឆ្លងដែន ប្រទេសដែលបានទស្សនកិច្ចដោយផ្អែកលើលិខិតឆ្លងដែន ព្រមទាំងឯកសារផ្សេងៗ ដែលបញ្ជាក់ពីឈ្មោះ អាសយដ្ឋាន និងថ្ងៃខែឆ្នាំកំណើត) ។

ប្រតិបត្តិការជាប់ពាក់ព័ន្ធនឹងទីកន្លែងដែលមានការព្រួយបារម្ភ

៦៤. ការដាក់ប្រាក់បញ្ញើដែលធ្វើឡើងជាបន្ទាប់ក្នុងរយៈពេលដ៏ខ្លី ដោយអ្នកផ្ទេរប្រាក់តាមអេឡិចត្រូនិក ជាពិសេសទៅកាន់ឬឆ្លងកាត់ទីកន្លែង ដែលមានការព្រួយបារម្ភ (ឧទាហរណ៍ដូចជា ប្រទេសដែលត្រូវបានកំណត់ដោយអាជ្ញាធរជាតិដែនដី ឬប្រទេសដែលមិនមានកិច្ចសហប្រតិបត្តិការ ជាមួយក្រុមការងារ ហិរញ្ញវត្ថុ ។

៦៥. គណនីអាជីវកម្មដែលការផ្ញើប្រាក់តាមអេឡិចត្រូនិកចេញ-ចូលមានចំនួនច្រើនបានកើតឡើង និង មិនមានសកម្មភាពអាជីវកម្ម ឬគោលដៅសេដ្ឋកិច្ចជាក់លាក់ ជាពិសេសនៅពេលដែលសកម្មភាពផ្ទេរប្រាក់នេះ ធ្វើឡើងទៅកាន់ ឆ្លងកាត់ មកពីទីកន្លែង ដែលមានការព្រួយបារម្ភ ។

៦៦. អតិថិជនដែលទទួលបានឧបករណ៍ឥណទាន ឬជាប់ពាក់ព័ន្ធនឹងប្រតិបត្តិការហិរញ្ញប្បទានពាណិជ្ជកម្ម ដែលពាក់ព័ន្ធនឹងចលនាមូលនិធិទៅកាន់ ឬ មកពីទីកន្លែងដែលមានការបារម្ភ នៅពេលដែលមិនមានហេតុផលអាជីវកម្មសមស្រប ក្នុងការទំនាក់ទំនងទីកន្លែងទាំងនោះ ។

KINGDOM OF CAMBODIA
NATION RELIGION KING

NATIONAL BANK OF CAMBODIA

Number 67.08.089 Prokor

PRAKAS
ON
ANTI MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

The Governor of the National Bank of Cambodia

- With reference to the Constitution of the Kingdom of Cambodia;
- With reference to the Royal Kram NS/RKM/0196/27 of January 26. 1996 promulgating the *Law on the Organization and Conduct of the National Bank of Cambodia*;
- With reference to the Royal Kram NS/RKM/1199/13 of November 18. 1999 promulgating the *Law on Banking and Financial Institutions*;
- With reference to Royal Kram NS/RKM/0607/014 of June 24. 2007 promulgating the *Law on Anti Money Laundering and Combating the Financing of Terrorism*;
- With reference to the Royal Decree NS/ RKT/0508/526 of May 13, 2008 on the appointment of His Excellency Chea Chanto as Governor of the National Bank of Cambodia, which is equivalent to Senior Minister.
- Pursuant to the request of the General Direction
- Pursuant to the spirit of the meeting of the senior management of the National Bank of Cambodia dated May 27, 2008

DECIDES

Article 1 - Scope

For the purposes of the present Prakas the term 'banks and financial institutions" shall apply to the following institutions and professions, when they are regulated by the National Bank of Cambodia and referred to as "reporting entities" in the *Law on Anti Money Laundering and Combating the Financing of Terrorism*:

a) banks, including branches of foreign banks;

b) micro-finance institutions;

c) credit cooperatives;

d) leasing companies;

e) exchange offices/moneychangers;

f) money remittance services;

g) dealers in precious metals, stones and gems;

h) Any other institution or profession that is designated by the Financial Intelligence Unit to fall within the scope of the *Law on Anti-Money Laundering and Combating the Financing of Terrorism* and is supervised by the National Bank of Cambodia.

Article 2 – Customer Acceptance Policy

Banks and financial institutions should develop customer acceptance policies ~~and procedures and should have reasonable measures, including risk profile,~~ in their internal policy and procedures to address different risks posed by each type of customer or by each individual customer.

Article 3 – Risk Profiling

3.1 In creating the risk profile of a type of customer or an individual customer, banks and financial institutions should at least take into consideration the following factors:

- the origin of the customer and location of business;
- background and personal particulars of the customer
- nature of the customer's business;
- structure of ownership for a corporate customer; and
- any other information indicating the customer is of higher risk

3.2 Following the initial acceptance of the customer, banks and financial institutions should continuously monitor the customer's account activity pattern to ensure it is in line with the customer profile. Unjustified and unreasonable differences should cause banks and financial institutions to reassess the customer as higher risk.

Article 4 – Prohibition of Anonymous Account and Accounts in Fictitious Names

Banks and financial institutions should ensure that an account is opened and maintained in the name of the account holder at all times. In addition, banks and financial institutions should establish customer identity as outlined in articles 6 and 7 of the present Prakas and ensure that no customer is allowed to open or operate an anonymous account or an account in a fictitious, false or incorrect name.

Article 5 – Customer Due Diligence

5.1 Banks and financial institutions must conduct customer due diligence and obtain satisfactory evidence and properly establish in its records the identity and legal

existence of persons applying to do business with them. Such evidence must be substantiated by reliable documents.

5.2 The customer due diligence should be conducted, when:

- establishing business relationship with the customer such as opening an account, granting a safe deposit facility or engaging in any other business dealings;
- carrying out an occasional or one off transaction, that involves a sum in excess of USD 10,000 (or 40 million Riels or foreign currency equivalent) or wire-transfer in excess of USD 1,000 (or 4 million Riels or foreign currency equivalent).
- banks and financial institutions have any suspicion of money laundering or financing of terrorism; or
- banks and financial institutions have any doubts about the veracity or adequacy of previously obtained information.

5.3 The customer due diligence undertaken by banks and financial institutions should at least comprise the following:

- identify the customer and verify the identity of the customer using reliable, independent source documents, data or information referred to in articles 6 or 7;
- determine if the customer conducting business is acting on behalf of another person or beneficial owner;
- understanding the beneficial ownership and control structure of the customer. Beneficial owner is defined in article 8;
- obtain information on the purpose and intended nature of the business relationship; and
- conduct on-going due diligence and scrutiny, to ensure the information provided is updated and relevant and ensure that the transactions being conducted are consistent with the bank's or financial institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

5.4 Unwillingness of the customer to provide the information requested and to cooperate with banks and financial institutions' customer due diligence process may itself be a factor of suspicion.

5.5 Banks and financial institutions should not open the account, commence business relations or perform transaction, or in the case of existing business relations with customers, it should terminate such business relations if the customer fails to comply with the customer due diligence requirements. Such situation warrants a suspicious transaction report to be submitted to the Financial Intelligence Unit.

Article 6 - Individual Customers

6.1 In establishing a business relationship with an individual customer, banks and financial institutions should obtain from the individual customer at least the full name, date of birth, identity card/passport number/identity document reference number, occupation/business, address and nationality.

6.2 Banks and financial institutions should require the individual to furnish the original and make copies of one or more of the following documents:

- National identity card;
- Passport; or
- Identity documents preferably bearing a photograph of the customer, issued by an official authority.

Article 7 - Corporate Customers

7.1 In establishing a business relationship with a corporate customer, banks and financial institutions should require the company/business to furnish the original and make copies of at least the following documents:

- Memorandum/Article/Certificate of Incorporation/Partnership
- Identification document of Directors/Shareholders/Partners
- Board of Directors'/Directors' Resolution
- Authorisation for any person to represent the company/business
- Authorisation or permit to conduct business

7.2 In addition, banks and financial institutions should conduct a basic search or enquiry on the background of such company/business to ensure that it has not been, or is not in the process of being, dissolved or wound-up.

7.3 The identity of all account signatories shall be verified according to customer due diligence for individual customers. When signatories change, care should be taken to ensure that the identity of all current signatories has been verified.

7.4 To verify the information provided, banks and financial institutions should check with the Registry of Companies/Businesses on the authenticity of the information provided on the identity of the company/business and its directors, owners, shareholders and office bearers.

7.5 Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements i.e. a public company listed on a recognised stock exchange, it is not necessary to seek to identify and verify the identity of the shareholders of that public company.

7.6 Banks and financial institutions should also understand the ownership and control structure of corporate customers and determine the source of funds of the company/business. This will assist banks and financial institutions in ascertaining any suspicion concerning the changes to the ownership or control structure and in developing the customer profile and expected activity through the company/business account.

Article 8 - Beneficial Owner

Banks and financial institutions should conduct customer due diligence as stringent as the one imposed on individual customer when they suspect a transaction is conducted on behalf of a beneficial owner and not the customer who is conducting such transaction. Beneficial owner is the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being

conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Article 9 – Non-Government Organization and Foundation

9.1 Banks and financial institutions should require a Non-Government Organization or foundation establishing business relationship to furnish the constitution documents or other similar documents to ensure that it is properly constituted and registered.

9.2 The identity of all account signatories shall be verified according to customer due diligence for individual customers. When signatories change, care should be taken to ensure that the identity of all current signatories has been verified.

9.3 Banks and financial institutions should take steps to understand who is in control and makes decisions regarding the Non-Government Organization/foundation, and the use of the funds.

Article 10 - Trust and Nominee Accounts

10.1 Banks and financial institutions need to establish whether the customer is acting on behalf of another person as trustee, nominee or agent.

10.2 Banks and financial institutions should take reasonable measures to understand the ownership and control structures and the relationship among the relevant parties in handling a trust or nominee account and obtain evidence of the identity of the settler, trustee, nominee, authorised signatories, persons exercising effective control and the beneficiaries.

10.3 Banks and financial institutions should ensure customer due diligence requirements are completed for beneficial owners, when the trust or nominee account is established.

10.4 Banks and financial institutions require a written assurance from the trust or nominee that evidence of the identity of the beneficiaries has been obtained, recorded and retained, and that the trust or nominee is satisfied regarding the source of funds. In addition, identification information must be immediately available to banks and financial institutions upon request.

Article 11 - Client Accounts

Banks and financial institutions should satisfy themselves about transactions passing through lawyers and accountants clients' accounts that give cause for concern, and should report those transactions to Financial Intelligence Unit, if any suspicion is aroused.

Article 12 - Shell Companies

Banks and financial institutions should not open an account for or conduct business with a shell company, which do not conduct any commercial activities or have any form of commercial presence in the country but are legal entities through

which financial transactions may be conducted.

Article 13 - Reliance on Intermediaries or Other third Parties for CDD or Introduced Business

13.1 Banks and financial institutions should be wary and ensure that they do not fall complacent and completely rely on the customer due diligence conducted by the intermediaries or other third parties they use. The ultimate responsibility of customer due diligence always remains with banks and financial institutions.

13.2 Banks and financial institutions must be satisfied that the introducing intermediary:

- has carried out customer due diligence by identifying the customer and verify that identity using reliable, independent source documents, data or information;
- has identified the beneficial owner and in respect of corporate customers understands the ownership and control structure of the customer;
- understands the purpose and nature of the business relationship;
- has put in place a system to provide the bank or financial institution with access to the identification documents, data or information upon request and without delay;
- allows periodic review by banks and financial institutions to verify the due diligence undertaken; and
- is properly regulated and supervised for AML/CFT purposes by the respective authority.

Article 14 – Non Face-to-Face Customers

14.1 Banks and financial institutions should pay special attention in establishing and conducting non-face-to-face business relationships and undertake customer due diligence through face-to-face interaction, or through an intermediary as required by article 13 of the present Prakas, prior to establishing such business relationships with their customers.

14.2 Banks and financial institutions are also required to implement monitoring and reporting mechanisms to identify potential money laundering and financing of terrorism activities.

Article 15 - Correspondent Banking

15.1 Banks and financial institutions should take the necessary measure to ensure that they are not exposed to the threat of money laundering and financing of terrorism through correspondent accounts they have with other banks and financial institutions.

15.2 Banks and financial institutions entering a correspondent relationship should gather and assess at least the following information on the correspondent banks and financial institutions;

- board of director and management;
- business activities and products;
- subjected legislations, regulation and supervision;
- AML/CFT measures and controls; and

- annual reports.

15.3 Banks and financial institutions should establish or continue a correspondent banking relationship with the correspondent banks and financial institutions only if it is satisfied with the assessment of the information gathered.

15.4 Banks and financial institutions should also document the responsibilities of the respective parties in relation to the correspondent banking relationship.

15.5 The decision and approval to establish or continue a correspondent banking relationship should be made at the Senior Management level.

15.6 Banks and financial institutions, should ensure that such correspondent banking relationship do not include correspondent banks and financial institutions that have no physical presence and which is unaffiliated with a regulated financial group.

15.7 Banks and financial institutions should exercise enhanced due diligence with respect to correspondent banks and financial institutions which allow direct use of the correspondent account by their customers to transact business on their own behalf such as payable–through accounts. Banks and financial institutions should implement customer due diligence for such customers as required for intermediaries introducing business.

15.8 Banks and financial institutions should pay special attention to correspondent banking relationship with correspondent banks and financial institutions from countries which have insufficiently implemented the internationally accepted AML/CFT measures. Enhanced due diligence is needed to assess the money laundering and financing of terrorism risks.

Article 16 - Remittance / Wire Transfer

16.1 Banks and financial institutions conducting or participating in an outgoing remittance/wire transfer transaction should include with it the necessary originator's name, address, account number, identification number or customer reference number and the details of the transaction.

16.2 Banks and financial institutions facilitating or acting as intermediary to a remittance/wire transfer transaction should ensure such originators information is still retained with remittance/wire transfer message.

16.3 Banks and financial institutions receiving a remittance/wire transfer message with incomplete originators information should conduct enhanced due diligence and may consider it as a factor of suspicion.

16.4 It is not necessary to include all the above information in the message accompanying a remittance/wire transfer transaction of less than USD 1,000/Riel 4 Million or its equivalent in any other currencies.

16.5 Banks and financial institutions should pay attention to wire transfers by higher risk customers and consider such factors as the name of the beneficiary, the destination and amount of the remittance/wire transfer. The customer should be

asked to provide further explanation of the nature of any remittance/wire transfer which is inconsistent with the customer's usual business/activity.

Article 17 - Politically Exposed Persons (PEPs)

17.1 Banks and financial institutions should check current and new customers to determine whether they are Politically Exposed Persons, as defined in article 3 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism, as part of the customer due diligence process. Banks and financial institutions should gather sufficient information from the said customer and research further data or information to determine the level of AML/CFT risk.

17.2 Once a PEP is identified, banks and financial institutions should take reasonable measures to establish the source of wealth and funds of such persons.

17.3 The decisions to enter into or continue business relationships with these PEPs should be made by the senior management of banks and financial institutions.

17.4 Banks and financial institutions should develop a risk profile of each PEP based on information collected from the customer and obtained through independent research and understand the full nature of the business relationship and transaction activity. There should be on-going monitoring of the relationship and activity against the risk profile and any concerns arising from the monitoring process should be reported to senior management and, if appropriate, also reported to the Financial Intelligence Unit.

Article 18 - Private Banking

18.1 Private banking businesses are provided to high net worth customers and very important people and its exclusive, confidential and private nature gives rise to the possibility of abuse by money launderers and financiers of terrorism.

18.2 Banks and financial institutions should give special attention to customers of private banking business. The identification and verification procedures should be more stringent than normal identification procedures. In particular, additional verification measures should be implemented regarding identification of customer, nature of business and source of funds.

18.3 All new and existing customers within the private banking service must undergo approval by senior management other than the manager of the private banking relationship who processes and recommends the application.

18.4 The compliance officers and auditors must be allowed to audit and review the transactions of private banking customers.

Article 19 - Moneychangers

19.1 Banks and financial institutions must pay special attention to and ensure that the moneychangers who maintain accounts with them are licensed and only conduct legitimate currency exchange transactions. Banks and financial institutions should ensure that the nature and volume of transactions in the moneychangers account reflect the nature of their business.

19.2 If banks and financial institutions identify any discrepancies in the activities of the moneychangers account, they should submit a suspicious transaction report to the Financial Intelligence Unit.

Article 20 - Other Higher Risk Customers

20.1 Banks and financial institutions shall conduct enhanced customer due diligence for all categories of higher risk customers, including those high risk customers mentioned in articles 18 and 19 of the present Prakas, to ensure that banks and financial institutions are not abused by money launderers and financiers of terrorism.

20.2 Enhanced due diligence should include at least:

- more detailed information from the customer, in particular, on the purpose of the business relationship and source of funds;
- independent research and sourcing of additional information about the customer; and
- approval by senior management.

Article 21 - Existing Accounts

21.1 Banks and financial institutions should take necessary measures to ensure that the records of existing customers remain up-to-date and relevant. Further evidence of the identity of existing customers should, where necessary, be obtained to ensure compliance with customer due diligence standards set by the present Prakas.

21.2 Banks and financial institutions should conduct regular reviews on existing records of customers. These reviews should at least, be conducted when:

- a significant transaction is to take place;
- there is a material change in the way the account is operated;
- the customer's particulars change substantially; or
- information held on the customer is insufficient.

21.3 In the event that the circumstances above do not arise, banks and financial institutions should, based on risk assessment, obtain additional information in line with their current standards from those existing customers that are of higher risk.

Article 22 – Record keeping

22.1 Banks and financial institutions should keep all records, documents and copies of documents involved in all forms of transactions for at least 5 years after the date of the transaction. All identification data, files, records, documents, business correspondence and copies of documents obtained on a customer must be maintained for at least 5 years after the accounts have been closed or the business relations with the customer have ended.

22.2 Where the records are subjected to an on-going investigation or suspicious transaction report submitted, they shall be retained beyond the stipulated

retention period until it is confirmed by the relevant authority that such records are no longer needed.

Article 23 – Audit Trail

23.1 Banks and financial institutions must ensure that the retained documents and records are able to create an audit trail on individual transactions that would enable the supervisory and enforcement agencies to trace funds.

23.2 The records kept must enable banks and financial institutions to establish the history and nature of and reconstruct each transaction. The records shall include at least:

- the origin of funds, such as method of receipt and or name of originator of wire transfer;
- the identity of the person undertaking the transaction if not an account holder;
- the type of transaction; and
- the instruction and the destination of fund transfers.

Article 24 – Record Format

Banks and financial institutions should retain the relevant document as originals or copies, on microfilm or in electronic form, provided that such forms are secured and retrievable upon request and provided in an accurate and timely manner

Article 25 – On-Going Monitoring

25.1 Banks and financial institutions should conduct on-going due diligence for all customer relationships, using a risk-based approach. The risk-based approach to on-going customer due diligence should ensure that the risk profile of the customer is up-to date.

25.2 Banks and financial institutions shall pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, to determine whether the transactions have an apparent or visible or lawful purpose.

Article 26 – Management Information System

Banks and financial institutions should put in place an adequate management information system for identifying and detecting transactions that they suspect or have reasonable grounds to suspect related to proceeds from an unlawful activity or the customer is involved in money laundering or financing of terrorism. The management information systems should provide banks and financial institutions timely information on a regular basis to enable them to detect suspicious activity.

Article 27 – Special Attention

Banks and financial institutions should conduct on-going due diligence with regards to business relationships and transactions with individuals, business, company and financial institutions from countries which have insufficiently implemented the internationally accepted AML/CFT measures. Such business relationships and transactions should require banks and financial institutions to make

further detailed inquiries, about their background and purpose, to establish the findings in writing, and to make them available to the competent authorities.

Article 28 – Cash Transaction Reporting

28.1 Banks and financial institutions are required to report to the Financial Intelligence Unit cash transactions exceeding USD 10,000 (or 40 million Riels or foreign currency equivalent).

28.2 Cash transactions shall be provided to the Financial Intelligence Unit, within 14 days of the date of the transaction and be submitted on the approved 'Cash Transaction Report' form issued by the Financial Intelligence Unit or using the approved format for electronic reporting. A copy of the approved Cash Transaction Report form is attached at Appendix IV.

28.3 Reportable cash transactions include multiple cash transactions for a customer / account where the total amount of the combined transactions exceeds USD 10,000 (or 40 million Riels or foreign currency equivalent) on any one day.

Article 29 – Suspicious Transaction Reporting

29.1 Banks and financial institutions are required to establish a reporting system and to promptly submit suspicious transaction reports to the Financial Intelligence Unit when any of its employees suspects or has reasonable grounds to suspect that the transaction involves proceeds of an offence or are related to money laundering or financing of terrorism or they have any other grounds of suspicion about a customer transaction. Some examples of suspicious transactions are listed in Appendix II .of the present Prakas. These examples are not exhaustive and only provide examples of basic ways in which money may be laundered or used for the financing of terrorism. Banks and financial institutions should establish their own internal guidelines on suspicious transaction reporting incorporating the relevant provisions in the Law on Anti Money Laundering and Combating the Financing of Terrorism and the relevant provisions in the present Prakas, including a list of suspicious transactions indicators.

29.2 Banks and financial institutions should also submit a suspicious transaction report when a new or existing customer fails to complete the customer due diligence without reasonable excuse, regardless of whether the bank or financial institutions accept, reject, continue or terminate the business relationship with such customer.

Article 30 - Reporting Mechanisms

30.1 Banks and financial institutions should appoint an officer at the senior management level to be the compliance officer responsible for the submission of suspicious transaction reports to the Financial Intelligence Unit. The appointed compliance officer should be the point of reference for the Financial Intelligence Unit. Banks and financial institutions should ensure that all suspicious transaction reports prepared by employees are properly channelled to the compliance officer.

30.2 The employees of banks and financial institutions should report suspicious transactions to the compliance officer even if they do not know precisely what the underlying unlawful activity is or whether such activities have occurred

30.3 Once the suspicious transaction report reaches the compliance officer, the compliance officer should promptly evaluate and establish whether there are reasonable grounds for suspicion and promptly, within 24 hours, submit the suspicious transaction report to the Financial Intelligence Unit unless the compliance officer considers, and records his/her opinion, that such reasonable grounds do not exist.

30.4 The suspicious transaction report submitted by the compliance officer shall be in writing and using the approved form as attached in Appendix III and delivered by safe hand, secure mail or secure electronic transmission to Financial Intelligence Unit.

30.5 Banks and financial institutions should ensure that when preparing and submitting a suspicious transaction report, information about the suspicious transaction, the customer and the reporting of the matter remains confidential and is available only to staff, on a strict 'need to know' basis.

30.6 Banks and financial institutions should authorise their compliance officer to cooperate with the Financial Intelligence Unit in providing additional information and documentation requested and to address further enquiries with regard to the submitted suspicious transaction report.

Article 31 - Prohibition of Tipping Off

31.1 Banks and financial institutions must ensure that the reporting system put in place for the submission of suspicious transaction reports is operated in a confidential manner.

31.2 Banks and financial institutions must ensure that the customer reported on, is not informed of the existence of the suspicious transaction report or does not become aware of such suspicious transaction report. Staff should be made aware that article 15 of the Law on Anti Money Laundering and Combating the Financing of Terrorism prohibits any individual having knowledge of a suspicious transaction report from communicating such information or reports to any natural or legal persons other than the FIU, except where so authorized by the FIU.

Article 32 - Others Issues

32.1 Banks and financial institutions should maintain a complete file on all suspicious transaction reports submitted by their employees to its compliance officer and such reports that have been further submitted to the Financial Intelligence Unit.

32.2 Banks and financial institutions must take reasonable measures to ensure that all their officers and employees involved in conducting or facilitating customer transactions are aware of these reporting procedures.

Article 33 – Detection and Reporting of the Financing of Terrorism

33.1 Banks and financial institutions should take the necessary measures to ensure compliance with the United Nations Security Council (UNSC) Resolutions and relevant regulations and legislation on financing of terrorism.

33.2 Banks and financial institutions should extend the suspicious transaction report system and mechanism to cover suspicion of financing of terrorism.

33.3 Banks and financial institutions should maintain a database of names and particulars of terrorist in the United Nations list and they should consolidate their database with the other recognised lists of designated persons. Information contained in the database should be updated and relevant and made easily accessible to employees for the purpose of identifying suspicious transactions and freezing accounts / funds.

33.4 Banks and financial institutions should conduct checks of the names of new and existing customers against the names in the database. If there is a name match, the banks and financial institutions should take reasonable measures to verify and confirm the identity of its customer. If the customer and the person listed in the database are the same person, the bank or financial institution should immediately freeze the customer's accounts and inform the Financial Intelligence Unit. Where banks and financial institutions suspect that a transaction is terrorist-related, it should make a suspicious transaction reports to the Financial Intelligence Unit.

Article 34 – Risk Management

34.1 The Board of Directors of banks and financial institutions should establish an effective internal control system for AML/CFT compliant with legal and regulatory requirements. It is responsibility of the senior management to ensure such internal controls are implemented effectively.

34.2 The Board of Directors and senior management should be aware of and understand the AML/CFT measures required by law, the regulators, the industry's standards and best practices as well as the importance of putting in place AML/CFT measures to prevent their bank or financial institution from being abused by money launderers and financiers of terrorism. The Board of Directors should oversight the overall AML/CFT measures undertaken by the bank or financial institution.

34.3 The Board of Directors and senior management should be aware of the money laundering and financing of terrorism risks associated with all its business products and services.

34.4 The Board of Directors should ensure that its bank or financial institution has, at the minimum, policies on AML/CFT procedures and controls. The senior management should assist the Board of Directors in formulating the policies and ensure that the policies are in line with the risks associated with the nature of business, and complexity and volume of the transactions undertaken by the bank or financial institution.

34.5 The Board of Directors should ensure that the procedures for AML/CFT measures including those required for customer acceptance policy, customer due diligence, record keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are in place.

34.6 The Board of Directors should assess the implementation of approved AML/CFT policies by the senior management via periodic reports.

34.7 The Board of Directors should define the lines of authority and responsibilities for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls. The Board of Directors should ensure the:

- appointment of a compliance officer to ensure that the policies, procedures and controls are in place; and
- effectiveness of internal audit in assessing and evaluating the controls in place to counter money laundering and financing of terrorism.

34.8 The Board of Directors should review and assess the policies and procedures on the AML/CFT measures in line with changes and developments in its products, services and technology systems, as well as trends in money laundering and financing of terrorism techniques. The senior management should implement the necessary changes to the policies and procedures with the approval of the Board of Directors to ensure that the current policies are sound and appropriate.

34.9 The Board of Directors and senior management should ensure that there are adequate ongoing AML/CFT training programs in place.

Article 35 - Staff Integrity

Senior management should ensure that its bank or financial institution establish an employee assessment system, approved by the Board of Directors, to adequately screen its employees, both existing and new, to ensure that the integrity of its employees is not compromised. The employee assessment system should at least examine personal information including criminal records, employment and financial history of its new employees as part of the recruitment process.

Article 36 - Compliance Officer

36.1 Senior management is responsible to appoint the compliance officer at senior management level with the approval of the Board of Directors. Senior management should ensure that the compliance officer effectively discharges his/her AML/CFT responsibilities. The compliance officer should act as the reference point for the AML/CFT measures the bank or financial institution has established, including employee training and reporting of suspicious transactions.

36.2 Banks and financial institutions should upon the appointment or change in the appointment of the compliance officer inform the Financial Intelligence Unit of the details of the compliance officer including the name, address, telephone number, facsimile number, e-mail address and other relevant background.

36.3 Banks and financial institutions should ensure that the roles and responsibilities of the compliance officer are clearly defined and documented. The roles and responsibilities of the AML/CFT compliance officer should include at least ensuring:

- implementation of the policies for AML/CFT measures;
- the appropriate AML/CFT procedures including customer acceptance policy, customer due diligence, record keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are implemented effectively;
- regular assessment of the AML/CFT mechanisms to ensure that the mechanisms are sufficient to address the changing trends;

- the channel of communication from the respective employees to the compliance officer is secured and that any information is kept confidential;
- compliance with the AML/CFT legal and regulatory requirements;
- all employees are aware of AML/CFT measure including policies, control mechanisms and channel of reporting to ensure the effectiveness of such measures;
- the identification of money laundering and financing of terrorism risks associated with new products or services or arising from the bank's or the financial institution's operational changes, including the introduction of new technology and processes.

36.4 Compliance officers should have the necessary knowledge and expertise to effectively discharge his/her responsibilities, including knowledge on AML/CFT obligations required under the relevant laws and regulations and an understanding of developments in money laundering and financing of terrorism techniques

Article 37 - Staff Training and Awareness Programmes

37.1 Banks and financial institutions should have an awareness and training programme on AML/CFT practices and measures for its employees. The training and awareness programme must be extended to all new and existing employees.

37.2 Senior management should ensure that proper channels of communication are in place to inform all levels of employees in banks and financial institutions of their AML/CFT policies and procedures.

37.3 Employees should be aware of AML/CFT policies and controls in place and the requirements as specified in the present Prakas and in banks and financial institutions AML/CFT internal manual.

37.4 The AML/CFT internal manual should at least contain the following:

- the *Law on Anti-Money Laundering and Combating the Financing of Terrorism*;
- the present Prakas;
- the FATF Forty plus Nine Recommendations;
- the Customer Due Diligence Paper by Basel Committee on Banking Supervision; and
- the bank's and financial institution's measures to meet all AML/CFT requirements.

37.5 Banks and financial institutions should at least adapt to their needs the following training packages for the various sectors of employees within their institutions:

- *New Employees*
  A general background to money laundering and financing of terrorism, the requirement and obligation to identify and report suspicious transactions to the appropriate designated point within banks and financial institutions, and the importance of not tipping off the customer.

- *Front-Line Employees*

Employees who deal directly with the customers as the first point of contact with potential money launderers and financiers of terrorism should be trained in identifying suspicious transactions, the measures to be taken once a transaction is deemed to be suspicious, factors that may give rise to suspicions, large cash reporting and enhanced customer due diligence.

- *Employees - Account Opening/New Customers*
  Employees, who are responsible for account opening or the acceptance of new customers, should at least receive the equivalent training given to front-line employees. In addition, they should be trained in customer identification and verification, opening of accounts and establishing business relationship with customers.

- *Supervisors and Managers*
  Supervisors and managers should receive a higher level of instruction covering all aspects of AML/CFT procedures including the penalties for non-compliance to the AML/CFT requirement, and procedures in addressing combating the financing of terrorism issues.

37.6 These training and awareness programmes should be conducted regularly with refresher courses provided for employees. New employees should be trained within three months of commencement of employment and front line employees, supervisors and managers should have refresher training annually.

Article 38 - Internal Audit

38.1 The Board of Directors should ensure that internal auditors undertake audit of the effectiveness and compliance with AML/CFT requirements of the relevant laws and regulation as well as the present Prakas.

38.2 The Board of Director should ensure that the roles and responsibilities of the internal auditor are clearly defined and documented and at least include:

- testing the effectiveness of the policies, procedures and control for AML/CFT measures;
- ensuring effectiveness of AML/CFT control mechanisms including the appointment of compliance officers, staff training and awareness programmes, employee screening mechanisms and AML/CFT internal manual; and
- ensuring that measures put in place are in line with current developments and changes of the relevant AML/CFT requirements.

38.3 Banks and financial institutions should inform the Financial Intelligence Unit and the National Bank of Cambodia upon the appointment or change in the appointment of the internal auditor and on the approach and procedures adopted by the internal auditors.

38.4 The internal auditor should submit a written report on the audit findings to the Board of Directors on a regular basis. The annual audit report should highlight inadequacies of any AML/CFT measures and control systems within the bank or the financial institution, and the Board of Directors should ensure that necessary steps are taken to rectify the situation. Audit findings and reports on AML/CFT should be submitted to the National Bank of Cambodia after consideration by the Board of Directors.

Article 39 -

The present Prakas supersedes the existing Prakas on Standardised Procedures for Identification of Money Laundering at the Banking and Financial Institution issued on October 21, 2002 and Circular on Suspicious Transactions and Know your Customer Policies issued on October 04, 2003.

Article 40 -

The General direction, the General Secretariat, the General Inspection, the General Cashier and all departments of the National Bank of Cambodia, all Banking and Financial Institutions under NBC's supervisory authority shall strictly implement the present Prakas.

Article 41-

The present Prakas shall have effect from the signing date.

Phnom Penh, May 30, 2008

Governor
Signed : Chea Chanto

cc:
- All members of the Board of Directors
- The parties concerned as stated in article 40
- File
- CM "for info"
- Administration Department of CM "for publication in the National Gazette"

Appendix I

DESCRIPTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

Pursuant to the Law on Anti-Money Laundering and Combating the Financing of Terrorism

"*Money laundering*" shall mean:

1. The conversion or transfer of property, knowing that such property is the proceeds of offence, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;

2. The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of offence;

3. The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of offence;

4. Participation in, and attempts to commit and aiding and abetting, any of the acts defined in accordance with this article;

"Financing of terrorism" shall mean:

"*Financing of terrorism*" shall mean the wilful provision or collection of funds, directly or indirectly, through whatever means, with the intention that such funds be used or in the knowledge that they are or may be used, in full or in part, for the purpose of supporting terrorism, terrorist acts or terrorist organizations.

Appendix II

EXAMPLES OF SUSPICIOUS TRANSACTIONS

Cash Transactions, Deposit and Withdrawal

1. Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
2. Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period of time, out of the account and/or to a destination not normally associated with the customer.
3. Company accounts whose transactions, both deposits and withdrawals, are denominated in cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.)
4. Customers who constantly pay in or deposit cash to cover requests for bankers' draft, money transfers or other negotiable and readily marketable money instruments.
5. Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.
6. Branches of banks and financial institutions that have a great deal more cash transactions than usual (Head Office statistics detect aberrations in cash transactions).
7. Customers whose deposits contain counterfeit notes or forged instruments.
8. Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.
9. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the institution.
10. Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their retail business.
11. Deposits for a business entity in combinations of monetary instruments that are atypical of the activity normally associated with such a business.
12. Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.
13. Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

14. The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

15. The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

16. The customer presents funds that have not been counted and upon counting reduces the fund involved to an amount just below what would trigger reporting or identification requirements.

17. The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

Accounts

18. Accounts that appear to act as pass through accounts with high volumes of credits and debits and low average monthly balances.

19. Customers who wish to maintain a number of trustee or client accounts, which do not appear consistent with the type of business, including transactions, which involve nominee names.

20. The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

21. Any individual or company whose account shows no normal personnel banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

22. Reluctance to provide normal information when opening an account, attempts to reduce the level of information provided to the minimum or providing information that is difficult or expensive for banks and financial institutions to verify.

23. Customers who appear to have accounts with several bank and micro finance institutions within the same locality, but choose to consolidate monies from such accounts on regular basis for onward transmission of the funds to another 3rd party account.

24. Paying in large third party cheques endorsed in favour of the customer.

25. An inactive account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

26. Greater use of safe deposit facilities, which does not commensurate with the customer profile.

27. Customer avoiding contact with employees of banks and financial institutions for transaction.

28. Substantial increases in deposits of cash or negotiable instrument by a professional firm or company, using client accounts or in-house company, or trust accounts, especially if the deposits are promptly transferred between other client's company and trust accounts.

29. Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

30. Large number of individuals making payment into the same account without an adequate explanation.

31. High velocity of funds through an account, i.e., low beginning and ending daily balances, which do not reflect the large volume of dollars flowing through an account.

32. An account opened in the name of a money-changer that receives structured deposits (e.g. constant amount of deposit regularly).

33. An account operated in the name of an off-shore company with structured movement of funds.

34. Accounts that receive relevant periodical deposits and are inactive at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.

35. An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

36. An account opened by a legal entity or an organisation that has the same address as other legal entities or organisations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

37. An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the founders of the entity.

38. An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation.

39. An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organisation and that shows movements of funds above the expected level of income.

International Banking/Trade Finance

40. Customer introduced by an overseas branch, affiliate or other bank based locations of specific concern (for example, countries where production of drugs or drug trafficking may be prevalent, countries designated by national authorities, FATF's non-cooperative countries and territories, etc.).

41. Use of Letter of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

42. Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions, or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs, prescribed terrorist organizations or tax havens.

43. Building up of large balance, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

44. Unexplained electronic fund transfers by customers on an in-and-out basis or without passing, through an account.

45. Frequent requests for or paying in of travellers' cheques or foreign currency drafts or other negotiable instruments to be issued or originating from overseas.

46. Customers sending and receiving wire transfer to/from tax haven countries, particularly if there are no apparent business reasons for such transfers or such transfers are not consistent with the customers' business or history.

Banks and financial institutions employees and agents

47. Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.

48. Changes in employee or agent performance, e.g. the salesman selling products for cash has a remarkable or unexpected increase in performance.

49. Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

50. Sudden strong performance by employees in special relationship/confidential relationship banking services such as trust or private banking services or sudden increase in the wealth/spending of such employees.

Private banking and trust services

51. The grantors of private banking and trust accounts that direct loans from their accounts to other parties or business interests of account principals or beneficiaries.

Secured and Unsecured Lending

52. Customers who repay problem loans unexpectedly.

53. Request to borrow against assets held by banks and financial institutions or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

54. Request by a customer for a bank and micro finance institution to provide or arrange financial contribution to a deal which is unclear, particularly, where property is involved.

55. Customers who unexpectedly repay in part or full a mortgage or other loan in a way inconsistent with their earning capacity or asset base.

Wire transfer

56. Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

57. Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided.

58. Use of multiple personal and business accounts or the accounts of non-profit organisations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

Characteristic of customer or his business activity

59. Funds generated by a business owned by individuals or involved by multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

60. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).

61. Stated occupation of the customer does not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

62. Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

63. Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

Transaction linked to locations of concern

64. Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).

65. A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.

66. A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.