ព្រះរាជក្រម

នស/រកម/១១១៩/ ០១៧

យើង

ព្រះករុណាព្រះបាទសម្តេចព្រះបរមនាថ នរោត្តម សីហមុនី
សមានភូមិជាតិសាសនា រក្ខតខត្តិយា ខេមរាជ្ជរាស្ត្រ ពុទ្ធិន្ទ្រាធរាមហាក្សត្រ
ខេមរាជនា សម្ភូហោតាស កម្ពុជឯករាជ្យបូរណសន្តិ សុតមង្គលា សិរីវិបុលា
ខេមរស្រីពិរាស្ត្រ ព្រះចៅក្រុងកម្ពុជាធិបតី

- បានទ្រង់យល់រដ្ឋធម្មនុញ្ញនៃព្រះរាជាណាចក្រកម្ពុជា
- បានទ្រង់យល់ព្រះរាជក្រឹត្យលេខ នស/រកត/០៩១៨/៩២៥ ចុះថ្ងៃទី៦ ខែកញ្ញា ឆ្នាំ២០១៨ ស្តីពីការតែងតាំងរាជរដ្ឋាភិបាលនៃព្រះរាជាណាចក្រកម្ពុជា
- បានទ្រង់យល់ព្រះរាជក្រមលេខ នស/រកម/០៦១៨/០១២ ចុះថ្ងៃទី២៨ ខែមិថុនា ឆ្នាំ២០១៨ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃគណៈរដ្ឋមន្ត្រី
- បានទ្រង់យល់ព្រះរាជក្រមលេខ នស/រកម/០១៩៦/១៦ ចុះថ្ងៃទី២៤ ខែមករា ឆ្នាំ១៩៩៦ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីការបង្កើតក្រសួងពាណិជ្ជកម្ម
- បានទ្រង់យល់សេចក្តីក្រាបបង្គំទូលថ្វាយរបស់សម្តេចអគ្គមហាសេនាបតីតេជោ ហ៊ុន សែន នាយករដ្ឋមន្ត្រីនៃព្រះរាជាណាចក្រកម្ពុជា

ប្រកាសឱ្យប្រើ

ច្បាប់ស្តីពីពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក ដែលរដ្ឋសភាបានអនុម័តកាលពីថ្ងៃទី៨ ខែតុលា ឆ្នាំ២០១៩ នាសម័យប្រជុំរដ្ឋសភា លើកទី៣ នីតិកាលទី៦ ហើយដែលព្រឹទ្ធសភាបានពិនិត្យចប់សព្វគ្រប់លើទម្រង់និងគតិច្បាប់នេះទាំងស្រុងកាលពីថ្ងៃទី១៨ ខែតុលា ឆ្នាំ២០១៩ នាសម័យប្រជុំជាវិសាមញ្ញ នីតិកាលទី៤ ហើយដែលមានសេចក្តីទាំងស្រុងដូចតទៅ៖

ច្បាប់

ស្តីពី

ពាណិជ្ជកម្មតាមប្រព័ន្ធ

អេឡិចត្រូនិក

ROYAUME DU CAMBODGE
MINISTÈRE DU PALAIS ROYAL

ជំពូកទី១
បទប្បញ្ញត្តិទូទៅ

មាត្រា១ .. គោលបំណង

ច្បាប់នេះមានគោលបំណង៖

១. គ្រប់គ្រងពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកក្នុងព្រះរាជាណាចក្រកម្ពុជានិងជាមួយអន្តរជាតិ។

២. បង្កើតភាពប្រាកដប្រជាផ្នែកគតិយុត្តក្នុងប្រតិបត្តិការពាណិជ្ជកម្មនិងរដ្ឋប្បវេណី តាមប្រព័ន្ធអេឡិចត្រូនិក។

៣. ផ្តល់ទំនុកចិត្តដល់សាធារណជនក្នុងការប្រើប្រាស់ទំនាក់ទំនងអេឡិចត្រូនិក។

មាត្រា២ .. គោលដៅ

ច្បាប់នេះមានគោលដៅដូចខាងក្រោម៖

១. កំណត់អំពីយថាភូតភាព សុក្រឹតភាព និងភាពអាចជឿទុកចិត្តបាននៃទម្រង់អេឡិចត្រូនិក។

២. ជំរុញការអភិវឌ្ឍក្របខ័ណ្ឌគតិយុត្តនិងធុរកិច្ច ដើម្បីអនុវត្តពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកប្រកបដោយសុវត្ថិភាព។

៣. បង្ការនិងបង្ក្រាបអំពើដែលបង្កការខូចខាតដល់ទិន្នន័យនិងប្រព័ន្ធព័ត៌មាន។

៤. លុបបំបាត់ឧបសគ្គទាំងឡាយដែលរាំងស្ទះដល់ការធ្វើពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក ហើយដែលកើតចេញពីភាពមិនប្រាកដប្រជានៃលក្ខខណ្ឌតម្រូវចំពោះលិខិតជាលាយលក្ខណ៍អក្សរនិងហត្ថលេខា។

៥. សម្រួលដល់ការតម្កល់ឯកសារតាមប្រព័ន្ធអេឡិចត្រូនិកជាមួយស្ថាប័នសាធារណៈ និងលើកកម្ពស់ការផ្តល់សេវាកម្មប្រកបដោយប្រសិទ្ធភាពរបស់ស្ថាប័នសាធារណៈ តាមរយៈការប្រើប្រាស់កំណត់ត្រាតាមប្រព័ន្ធអេឡិចត្រូនិកដែលអាចជឿទុកចិត្តបាន។

៦. បង្កើតវិធាន បទប្បញ្ញត្តិ និងស្តង់ដា ដែលទាក់ទងនឹងយថាភូតភាពនិងសុក្រឹតភាពរបស់កំណត់ត្រាតាមប្រព័ន្ធអេឡិចត្រូនិក។

មាត្រា៣ .. វិសាលភាព

ច្បាប់នេះត្រូវអនុវត្តលើសកម្មភាព ឯកសារ និងប្រតិបត្តិការពាណិជ្ជកម្មនិងរដ្ឋប្បវេណីទាំងអស់ដែលធ្វើឡើងតាមប្រព័ន្ធអេឡិចត្រូនិក លើកលែងតែសកម្មភាព ឯកសារ និងប្រតិបត្តិការទាក់ទងនឹង៖

១. ការបង្កើតឬការអនុវត្តលិខិតប្រគល់សិទ្ធិ។

២. ការបង្កើតឬការចុះហត្ថលេខាលើមតកសាសន៍ លិខិតកែមតកសាសន៍ ឬបញ្ជាផ្សេងៗទៀតទាក់ទិននឹងសន្តតិកម្ម។

៣. រាល់តុបសន្យាសម្រាប់ការលក់ ការផ្ទេរ ឬការបោះបង់សិទ្ធិលើអចលនទ្រព្យឬផលប្រយោជន៍ផ្សេងៗទៀតក្នុងទ្រព្យនោះ។

៤. ការផ្ទេរអចលនវត្ថុឬផលប្រយោជន៍ណាមួយដែលពាក់ព័ន្ធនឹងអចលនវត្ថុនោះ។

៥. ករណីលើកលែងផ្សេងទៀតដែលត្រូវកំណត់ដោយអនុក្រឹត្យ។

មាត្រា៤ .. និយមន័យ

វាក្យសព្ទសំខាន់ៗដែលប្រើក្នុងច្បាប់នេះត្រូវបានកំណត់និយមន័យដូចមានក្នុងសទ្ទានុក្រមដែលមានចែងក្នុងឧបសម្ព័ន្ធនៃច្បាប់នេះ។

ជំពូកទី២
សុពលភាពនៃទំនាក់ទំនងអេឡិចត្រូនិក

មាត្រា៥ .. ការទទួលស្គាល់លក្ខណៈគតិយុត្តនៃទំនាក់ទំនងអេឡិចត្រូនិក

គ្មានបុគ្គលណាម្នាក់អាចបដិសេធមិនទទួលស្គាល់សុពលភាព អានុភាពគតិយុត្ត ភាពអាចទទួលយកបានឬភាពដែលអាចយកទៅអនុវត្តបាននៃទំនាក់ទំនងអេឡិចត្រូនិក ដោយគ្រាន់តែសម្អាងលើមូលហេតុដែលថាវាធ្វើឡើងក្នុងទម្រង់អេឡិចត្រូនិកឬស្ថិតនៅក្នុងទំនាក់ទំនងអេឡិចត្រូនិកទេ។

មាត្រា៦ .. លក្ខខណ្ឌតម្រូវជាលាយលក្ខណ៍អក្សរ

១. នៅពេលដែលបទប្បញ្ញត្តិណាមួយ តម្រូវឱ្យផ្តល់ព័ត៌មានជាលាយលក្ខណ៍អក្សរ ឬធ្វើកំណត់ត្រាជាលាយលក្ខណ៍អក្សរ ត្រូវចាត់ទុកថា លក្ខខណ្ឌតម្រូវនេះត្រូវបានបំពេញប្រសិនបើព័ត៌មាននេះធ្វើឡើងក្នុងទម្រង់អេឡិចត្រូនិក ហើយអាចចូលប្រើប្រាស់បាន និងអាចទាញយកទៅប្រើប្រាស់នៅពេលក្រោយបាន។

២. នៅពេលដែលលក្ខខណ្ឌក្នុងបញ្ញត្តិនៃកថាខណ្ឌទី១ខាងលើ ត្រូវយកមកអនុវត្តលក្ខខណ្ឌតម្រូវតាមច្បាប់ដែលទាមទារឱ្យបុគ្គលណាមួយផ្តល់សំណៅចម្លងច្រើនច្បាប់ក្នុងពេលតែមួយស្តីអំពីព័ត៌មានណាមួយឬកិច្ចការណាមួយទៅឱ្យបុគ្គលមួយផ្សេងទៀត បុគ្គលដែលផ្តល់អាចបំពេញលក្ខខណ្ឌនេះដោយគ្រាន់តែផ្តល់ក្រោមទម្រង់អេឡិចត្រូនិកតែមួយច្បាប់បាន។

មាត្រា៧ .. លក្ខខណ្ឌតម្រូវចំពោះហត្ថលេខា

១. នៅពេលដែលមានបទប្បញ្ញត្តិណាមួយតម្រូវឱ្យមានហត្ថលេខារបស់បុគ្គលណាមួយ លក្ខខណ្ឌតម្រូវនេះត្រូវចាត់ទុកថាបានបំពេញតាមរយៈការចុះហត្ថលេខាអេឡិចត្រូនិក ប្រសិនបើហត្ថលេខាអេឡិចត្រូនិកដែលបានប្រើនោះ ត្រូវបានបង្កើតឡើងតាមរយៈមធ្យោបាយដែលៈ

ក. អាចកំណត់អត្តសញ្ញាណបុគ្គល និងបង្ហាញការឯកភាពរបស់បុគ្គលនោះលើព័ត៌មាន ឬកំណត់ត្រាដែលមាននៅក្នុងទំនាក់ទំនងអេឡិចត្រូនិកនោះ។

ខ. អាចជឿជាក់បាន ស្របតាមចរិតលក្ខណៈ គោលបំណង និងកាលៈទេសៈ ដែលទំនាក់ទំនងអេឡិចត្រូនិកនោះត្រូវបានបង្កើតឡើងឬត្រូវបានប្រាស្រ័យទាក់ទង។



២. ទោះបីជាបទប្បញ្ញត្តិណាមួយកំណត់អំពីលក្ខខណ្ឌតម្រូវឱ្យមានចុះហត្ថលេខា ឬគ្រាន់តែកំណត់អំពីផលវិបាកនៃការមិនចុះហត្ថលេខាក៏ដោយ ក៏បញ្ញត្តិនៃកថាខណ្ឌទី១ខាងលើត្រូវយកមកអនុវត្តដែរ។

មាត្រា៨ .. លក្ខខណ្ឌតម្រូវសម្រាប់រក្សាព័ត៌មានតាមទម្រង់ដើម

លក្ខខណ្ឌគតិយុត្តក្នុងការរក្សាព័ត៌មានដែលមិនត្រូវបានធ្វើឡើងក្នុងទម្រង់អេឡិចត្រូនិក អាចត្រូវបានបំពេញដោយការរក្សាព័ត៌មាននោះក្រោមទម្រង់អេឡិចត្រូនិក ប្រសិនបើ៖

១. ទម្រង់អេឡិចត្រូនិកនោះជាមធ្យោបាយដែលអាចជឿទុកចិត្តបានដើម្បីកំណត់ភាពពេញលេញរបស់ព័ត៌មាននោះ។ និង

២. ព័ត៌មាននោះអាចចូលយកបានដោយងាយស្រួល សម្រាប់យកទៅប្រើប្រាស់បានពេលក្រោយ។

មាត្រា៩ .. ទម្រង់បែបបទដែលកំណត់

នៅពេលដែលបទប្បញ្ញត្តិណាមួយតម្រូវឱ្យព័ត៌មានធ្វើឡើងក្នុងទម្រង់បែបបទណាមួយ លក្ខខណ្ឌតម្រូវនោះត្រូវជំនួសដោយការផ្តល់ព័ត៌មានតាមទម្រង់អេឡិចត្រូនិកបាន ប្រសិនបើទម្រង់អេឡិចត្រូនិកនោះត្រូវបំពេញលក្ខខណ្ឌទាំងអស់ដូចខាងក្រោម៖

១. មានផ្ទុកព័ត៌មានដូចគ្នាឬដូចគ្នាភាគច្រើនទៅនឹងទម្រង់បែបបទដែលបានកំណត់។

២. អាចចូលទៅមើលបាន អាចយល់បាន និងអាចទាញយកមកប្រើប្រាស់បាននៅពេលក្រោយ។ និង

៣. អាចឱ្យបុគ្គលដែលទទួលបានព័ត៌មាននោះរក្សាទុកបាន។

មាត្រា១០ .. លក្ខខណ្ឌតម្រូវលើការរក្សាទុកកំណត់ត្រា

១. នៅពេលដែលបទប្បញ្ញត្តិណាមួយតម្រូវឱ្យរក្សាទុកនូវឯកសារ កំណត់ត្រា ឬព័ត៌មានជាក់លាក់ណាមួយ លក្ខខណ្ឌតម្រូវនោះត្រូវចាត់ទុកថាបានបំពេញ ប្រសិនបើ ការរក្សាទុកនោះបំពេញលក្ខខណ្ឌទាំងអស់ដូចខាងក្រោម៖

ក. ព័ត៌មានដែលមាននៅក្នុងទំនាក់ទំនងអេឡិចត្រូនិកនោះអាចចូលប្រើប្រាស់បាន និងសម្រាប់យកទៅប្រើប្រាស់នាពេលអនាគត។

ខ. ទំនាក់ទំនងអេឡិចត្រូនិកត្រូវបានរក្សាទុកក្នុងទម្រង់ដើមដែលត្រូវបានបង្កើតឡើង ផ្ញើ ឬទទួលបាន ឬក្នុងទម្រង់ដែលអាចត្រូវបានបង្ហាញពីសុក្រឹតភាពនៃព័ត៌មាននោះ។ និង

គ. ព័ត៌មានទាំងនោះត្រូវរក្សាទុកដើម្បីឱ្យបុគ្គលណាម្នាក់អាចកំណត់បាននូវប្រភពដើម និងគោលដៅនៃទំនាក់ទំនងអេឡិចត្រូនិកនោះ កាលបរិច្ឆេទ និងពេលវេលាដែលទំនាក់ទំនងអេឡិចត្រូនិកនោះត្រូវបានផ្ញើឬទទួល។

២. កាតព្វកិច្ចក្នុងការរក្សាឯកសារ កំណត់ត្រា ឬព័ត៌មានស្របតាមកថាខណ្ឌ១ មិនរាប់បញ្ចូលព័ត៌មានណាមួយ សម្រាប់តែធ្វើការបញ្ជូនឬទទួលសារនោះឡើយ។

មាត្រា១១ .. លក្ខខណ្ឌតម្រូវស្តីពីភស្តុតាង

គ្មានបទប្បញ្ញត្តិណាមួយក្នុងការអនុវត្តវិធានស្តីពីភស្តុតាង អាចជំទាស់ការទទួលយកទំនាក់ទំនងអេឡិចត្រូនិកជាភស្តុតាង ដោយគ្រាន់តែឈរលើមូលដ្ឋានដែលថា៖

១. ភស្តុតាងនោះជាទំនាក់ទំនងអេឡិចត្រូនិក។ ឬ

២. ភស្តុតាងនោះមិនស្ថិតក្នុងទម្រង់ដើម។

មាត្រា១២ .. ការបង្កើតកិច្ចសន្យានិងសុពលភាពកិច្ចសន្យា

១. សំណើ ស្វីការ និងកិច្ចសន្យា អាចធ្វើឡើងតាមមធ្យោបាយអេឡិចត្រូនិកបាន។

២. កិច្ចសន្យាក្នុងទម្រង់អេឡិចត្រូនិកដូចមានចែងក្នុងបញ្ញត្តិនៃកថាខណ្ឌទី១ខាងលើ មានសុពលភាព អានុភាពគតិយុត្ត និងភាពអាចអនុវត្តបាន នៅពេលដែលសំណើនិងស្វីការត្រូវគ្នា។

មាត្រា១៣ .. អានុភាពរវាងគូភាគី

អ្នកផ្ញើនិងអ្នកទទួលនៃទំនាក់ទំនងអេឡិចត្រូនិក មិនត្រូវបដិសេធអានុភាពគតិយុត្ត សុពលភាព និងភាពអាចអនុវត្តបាននៃការបង្ហាញឆន្ទៈ ឬសេចក្តីថ្លែងផ្សេងៗរបស់ខ្លួនឡើយ។

មាត្រា១៤ .. ការអនុវត្តដោយឡែកតាមការព្រមព្រៀងរបស់គូភាគី

១. តាមការព្រមព្រៀង គូភាគីដែលចូលរួមក្នុងការបង្កើត ការផ្ញើ ការទទួល ការរក្សាទុក ឬដំណើរការទំនាក់ទំនងអេឡិចត្រូនិក អាចអនុវត្តផ្សេងពីបទប្បញ្ញត្តិដូចមានចែងនៅក្នុងជំពូកទី២ នៃច្បាប់នេះ លើកលែងតែមានការកំណត់ផ្សេងពីនេះ។

២. ទោះជាមានបទប្បញ្ញត្តិដូចមានចែងក្នុងជំពូកទី២ គូភាគីនៃកិច្ចសន្យា ឬប្រតិបត្តិការណាមួយអាចៈ

ក. មិនប្រើប្រាស់កំណត់ត្រាអេឡិចត្រូនិក ទំនាក់ទំនងអេឡិចត្រូនិក ឬហត្ថលេខាអេឡិចត្រូនិកក្នុងកិច្ចសន្យា ឬប្រតិបត្តិការណាមួយតាមការព្រមព្រៀងគ្នា។ ឬ

ខ. ដាក់លក្ខខណ្ឌតម្រូវបន្ថែមផ្សេងៗដែលពាក់ព័ន្ធនឹងទម្រង់ ឬយថាភូតភាពនៃកិច្ចសន្យា ឬប្រតិបត្តិការតាមការព្រមព្រៀងគ្នា។

ជំពូកទី៣
ជំណើរការនៃទំនាក់ទំនងអេឡិចត្រូនិក

មាត្រា១៥ .. ពេលវេលានិងទីកន្លែងនៃការបញ្ជូនចេញនិងការទទួលព័ត៌មានក្នុងទំនាក់ទំនងអេឡិចត្រូនិក

១. ព័ត៌មានក្នុងទំនាក់ទំនងអេឡិចត្រូនិកមួយត្រូវចាត់ទុកថា បានបញ្ជូនចេញនៅពេលដែលៈ

ក. ព័ត៌មាននោះ បានចាកចេញពីប្រព័ន្ធព័ត៌មានដែលស្ថិតនៅក្រោមការគ្រប់គ្រងរបស់អ្នកផ្ញើឬរបស់ភាគីដែលផ្ញើជំនួសក្នុងនាមអ្នកផ្ញើ។ ឬ

ខ. ក្នុងករណីដែលព័ត៌មាននោះ ត្រូវបានបញ្ជូនតែមិនទាន់បានចាកចេញពីប្រព័ន្ធព័ត៌មានដែលស្ថិតក្រោមការគ្រប់គ្រងរបស់អ្នកផ្ញើឬរបស់ភាគីដែលផ្ញើជំនួសព័ត៌មានត្រូវចាត់ទុកថា បានបញ្ជូនចេញនៅពេលដែលព័ត៌មាននោះត្រូវបានទទួលក្នុងពេលណាមួយ។



២. ព័ត៌មានក្នុងទំនាក់ទំនងអេឡិចត្រូនិកមួយត្រូវបានសន្មតថាបានបញ្ជូនចេញពីទីតាំងអាជីវកម្មរបស់អ្នកផ្ញើ ទោះបីព័ត៌មាននោះត្រូវបានផ្ញើចេញពីទីតាំងណាក៏ដោយ។

៣. ពេលវេលានៃការទទួលព័ត៌មានគឺពេលដែលព័ត៌មាននោះ អាចទាញយកបានដោយអ្នកទទួលនៅក្នុងអាសយដ្ឋានអេឡិចត្រូនិកដែលអ្នកទទួលបានបញ្ជាក់ជាមុន។ ព័ត៌មានត្រូវបានសន្មតថាបានទទួលនៅទីកន្លែងដែលជាទីតាំងអាជីវកម្មរបស់អ្នកទទួល។

៤. ប្រសិនបើអាសយដ្ឋានអេឡិចត្រូនិកមិនត្រូវបានផ្តល់ដោយអ្នកទទួល នោះពេលវេលាទទួលបានព័ត៌មាន គឺជាពេលវេលាដែលអ្នកទទួលបានដឹងអំពីការផ្ញើចេញនិងអាចទាញយកព័ត៌មាននោះ តាមរយៈអាសយដ្ឋានអេឡិចត្រូនិកណាមួយ ហើយសន្មតថាបានទទួលនៅទីកន្លែងដែលជាទីតាំងអាជីវកម្មរបស់អ្នកទទួល។

៥. ប្រសិនបើអាសយដ្ឋានអេឡិចត្រូនិកត្រូវបានផ្តល់ដោយអ្នកទទួល ព័ត៌មានក្នុងទំនាក់ទំនងអេឡិចត្រូនិកត្រូវបានសន្មតថាបានទទួលនៅពេលព័ត៌មាននោះបានទៅដល់អាសយដ្ឋានអេឡិចត្រូនិករបស់អ្នកទទួល ហើយត្រូវបានចាត់ទុកថាបានទទួលនៅទីកន្លែងដែលជាទីតាំងអាជីវកម្មរបស់អ្នកទទួល។

មាត្រា១៦ .. សំណើបង្កើតកិច្ចសន្យា

រាល់ការស្នើសុំចុះកិច្ចសន្យា តាមរយៈទំនាក់ទំនងអេឡិចត្រូនិកដែលមិនសំដៅតែដល់បុគ្គលណាមួយជាក់លាក់ផ្សេងទៀត ត្រូវបានចាត់ទុកថាជាការអញ្ជើញឱ្យធ្វើសំណើបង្កើតកិច្ចសន្យាតែប៉ុណ្ណោះ។ ការស្នើសុំចុះកិច្ចសន្យានោះ នឹងត្រូវចាត់ទុកថាជាសំណើបង្កើតកិច្ចសន្យា ប្រសិនបើការស្នើសុំនោះបានបង្ហាញឱ្យឃើញច្បាស់អំពីឆន្ទៈរបស់ខ្លួនថានឹងត្រូវជាប់កាតព្វកិច្ចនៅពេលមានស្វីការពីភាគីម្ខាងទៀត។

មាត្រា១៧ .. ការប្រើប្រាស់ប្រព័ន្ធស្វ័យប្រវត្តសម្រាប់បង្កើតកិច្ចសន្យា

កិច្ចសន្យាដែលបង្កើតឡើងដោយអន្តរកម្មរវាងប្រព័ន្ធស្វ័យប្រវត្តនៃបុគ្គលមួយ ជាមួយរូបវន្តបុគ្គលណាមួយឬជាមួយប្រព័ន្ធស្វ័យប្រវត្តនៃបុគ្គលផ្សេងទៀត មិនអាចត្រូវបានបដិសេធអំពីសុពលភាព អានុភាពគតិយុត្ត ឬភាពអាចអនុវត្តបាននៃកិច្ចសន្យានោះឡើយ ដោយសម្អាងលើហេតុផលអវត្តមាននៃរូបវន្តបុគ្គលក្នុងការពិនិត្យឬក្នុងការចូលធ្វើសកម្មភាពដោយផ្ទាល់ក្នុងប្រព័ន្ធស្វ័យប្រវត្តឬក្នុងការបង្កើតកិច្ចសន្យា។

មាត្រា១៨ .. កំហុសឆ្គងនៃការបញ្ចូលព័ត៌មានក្នុងទំនាក់ទំនងអេឡិចត្រូនិក

នៅពេលដែលបុគ្គលបញ្ចូលព័ត៌មានខុសនៅក្នុងទំនាក់ទំនងអេឡិចត្រូនិកជាមួយប្រព័ន្ធស្វ័យប្រវត្តរបស់ភាគីម្ខាងទៀត ហើយប្រព័ន្ធស្វ័យប្រវត្តនេះមិនផ្តល់ឱកាសឱ្យបុគ្គលនោះធ្វើការកែប្រែព័ត៌មានដែលខុស បុគ្គលឬភាគីដែលជំនួសមុខឱ្យបុគ្គលដែលបញ្ចូលព័ត៌មាននោះមានសិទ្ធិកែតម្រូវ ឬដកចេញនូវព័ត៌មានដែលខុសនោះបាន ក្នុងករណីៈ



ក. បុគ្គលនោះបានជូនដំណឹងទៅភាគីម្ខាងទៀតអំពីកំហុសដែលបានកើតឡើងឱ្យបានឆាប់បផុត ដើម្បីត្រូវបង្ហាញថាខ្លួនបានបញ្ចូលព័ត៌មានខុសនៅក្នុងទំនាក់ទំនងអេឡិចត្រូនិក។ និង

២. បុគ្គលនោះមិនទទួលបានផលប្រយោជន៍ណាមួយ ដោយសារការបញ្ចូលព័ត៌មានខុសនេះ មុនពេលដែលខ្លួនធ្វើការជូនដំណឹងទៅឱ្យភាគីម្ខាងទៀត ហើយមិនបង្កការខូចខាតដល់ផលប្រយោជន៍របស់ភាគីម្ខាងទៀតឬតតិយជនណាមួយ។

បញ្ញត្តិដែលមានចែងក្នុងមាត្រានេះ មិនអនុវត្តចំពោះវិស័យមូលបត្រឡើយ។

ជំពូកទី៤
កំណត់ត្រាអេឡិចត្រូនិកនិងហត្ថលេខាអេឡិចត្រូនិកដែលមានសុវត្ថិភាព

មាត្រា១៩ .. កំណត់ត្រាអេឡិចត្រូនិកដែលមានសុវត្ថិភាព

កំណត់ត្រាអេឡិចត្រូនិកមួយត្រូវបានចាត់ទុកថាជាកំណត់ត្រាអេឡិចត្រូនិកដែលមានសុវត្ថិភាព លុះត្រាតែបានអនុវត្តស្របតាមនីតិវិធីសុវត្ថិភាពត្រឹមត្រូវ ដែលធានាបានថាកំណត់ត្រាអេឡិចត្រូនិកនោះ មិនត្រូវបានកែប្រែ គិតចាប់ពីពេលវេលាកំណត់ជាក់លាក់ណាមួយរហូតដល់ពេលធ្វើការពិនិត្យផ្ទៀងផ្ទាត់។

មាត្រា២០ .. ហត្ថលេខាអេឡិចត្រូនិកដែលមានសុវត្ថិភាព

១. ហត្ថលេខាអេឡិចត្រូនិកដែលមានសុវត្ថិភាព លុះត្រាតែគោរពទៅតាមលក្ខខណ្ឌខាងក្រោម៖

ក. ផ្សារភ្ជាប់ទៅកាន់ហត្ថលេខីតែម្នាក់គត់។

ខ. កំណត់បានអត្តសញ្ញាណរបស់ហត្ថលេខី។

គ. ត្រូវបានបង្កើតឡើងដោយប្រើប្រាស់មធ្យោបាយដែលស្ថិតនៅក្រោមការគ្រប់គ្រងរបស់ហត្ថលេខី។

ឃ. បញ្ជាក់អំពីពេលវេលានិងកាលបរិច្ឆេទនៃការចុះហត្ថលេខា។ និង

ង. បញ្ជាក់អំពីស្ថានភាពដើមនៃសារ ឬកំណត់ត្រាអេឡិចត្រូនិកដែលត្រូវបានផ្សារភ្ជាប់ដោយហត្ថលេខានោះ។

២. បញ្ញត្តិនៃកថាខណ្ឌទី១ខាងលើ មិនកម្រិតលទ្ធភាពរបស់បុគ្គលណាមួយក្នុងទំនាក់ទំនងអេឡិចត្រូនិកឡើយ ក្នុងការ៖

ក. កំណត់លក្ខខណ្ឌបន្ថែមផ្សេងទៀតពាក់ព័ន្ធនឹងភាពអាចជឿជាក់បានរបស់ហត្ថលេខាអេឡិចត្រូនិក។ ឬ

ខ. លើកភស្តុតាងអំពីភាពមិនអាចជឿជាក់បាននៃហត្ថលេខាអេឡិចត្រូនិក។

មាត្រា២១ .. ការសន្មតទាក់ទងនឹងកំណត់ត្រានិងហត្ថលេខាអេឡិចត្រូនិកដែលមានសុវត្ថិភាព

១. លើកលែងតែមានភស្តុតាងផ្ទុយ ក្នុងដំណើរការដែលពាក់ព័ន្ធនឹងកំណត់ត្រាអេឡិចត្រូនិកដែលមានសុវត្ថិភាព កំណត់ត្រាអេឡិចត្រូនិកដែលមានសុវត្ថិភាពត្រូវបានសន្មតថាជាកំណត់ត្រាអេឡិចត្រូនិកដែលមិនត្រូវបានកែប្រែចាប់តាំងពីពេលជាក់លាក់ណាមួយ។



២. លើកលែងតែមានភស្តុតាងផ្ទុយ ក្នុងដំណើរការពាក់ព័ន្ធនឹងហត្ថលេខាអេឡិចត្រូនិកដែលមានសុវត្ថិភាព ហត្ថលេខាអេឡិចត្រូនិកដែលមានសុវត្ថិភាពត្រូវបានសន្មតដូចខាងក្រោម៖

ក. ហត្ថលេខាអេឡិចត្រូនិកនោះ គឺជាហត្ថលេខារបស់បុគ្គលពាក់ព័ន្ធ។ និង

ខ. ហត្ថលេខាអេឡិចត្រូនិកនោះ ត្រូវបានចុះហត្ថលេខាដោយបុគ្គលមានឆន្ទៈក្នុងការចុះហត្ថលេខា ឬបានឯកភាពលើកំណត់ត្រាអេឡិចត្រូនិកនោះ។

៣. ក្នុងករណីដែលគ្មានកំណត់ត្រាអេឡិចត្រូនិកសុវត្ថិភាព ឬហត្ថលេខាអេឡិចត្រូនិកសុវត្ថិភាព គ្មានបញ្ញត្តិណាមួយនៅក្នុងជំពូកទី៤ អាចសន្មតបានជាមុនអំពីយថាភូតភាព ឬសុក្រឹតភាពនៃកំណត់ត្រាអេឡិចត្រូនិក ឬហត្ថលេខាអេឡិចត្រូនិកនោះឡើយ។

មាត្រា២២ .. ការលួចប្រើប្រាស់អត្តសញ្ញាណ

បុគ្គលទាំងឡាយមិនត្រូវប្រើប្រាស់អត្តសញ្ញាណ កំណត់ត្រា ហត្ថលេខាអេឡិចត្រូនិក អាសយដ្ឋានអេឡិចត្រូនិក លេខសម្ងាត់ ឬភិនភាគសម្គាល់របស់បុគ្គលផ្សេងទៀតដោយទុច្ចរិត ឬដោយគ្មានការអនុញ្ញាត ក្នុងប្រតិបត្តិការពាណិជ្ជកម្ម ឬមិនមែនពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក។

មាត្រា២៣ .. ស្ថាប័នមានសមត្ថកិច្ចគ្រប់គ្រងនីតិវិធីសុវត្ថិភាព

១. ក្រសួងប្រៃសណីយ៍និងទូរគមនាគមន៍ជាស្ថាប័នមានសមត្ថកិច្ចក្នុងការគ្រប់គ្រងនីតិវិធីសុវត្ថិភាព សម្រាប់កំណត់ត្រាអេឡិចត្រូនិកនិងហត្ថលេខាអេឡិចត្រូនិក។

២. ការគ្រប់គ្រងនីតិវិធីសុវត្ថិភាពសម្រាប់កំណត់ត្រាអេឡិចត្រូនិកនិងហត្ថលេខាអេឡិចត្រូនិកត្រូវកំណត់ដោយលិខិតបទដ្ឋានគតិយុត្ត។

ជំពូកទី៥
អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក

មាត្រា២៤ .. ការទទួលខុសត្រូវរបស់អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក

១. អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក មិនទទួលខុសត្រូវផ្នែករដ្ឋប្បវេណីឬព្រហ្មទណ្ឌពាក់ព័ន្ធនឹងព័ត៌មានដែលមានក្នុងកំណត់ត្រាអេឡិចត្រូនិកដែលពាក់ព័ន្ធនឹងការផ្តល់សេវារបស់អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកនោះឡើយ ក្នុងករណីដែលខ្លួនមិនមែនជាអ្នកផ្ញើកំណត់ត្រានោះ និងក្នុងករណីដែល៖

ក. អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកនោះមិនបានដឹងថាព័ត៌មានដែលបានផ្ញើនោះបង្កឱ្យមានការទទួលខុសត្រូវផ្នែករដ្ឋប្បវេណីឬព្រហ្មទណ្ឌ។

ខ. អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកនោះមិនបានដឹងអំពីអង្គហេតុឬកាលៈទេសៈដែលអាចឱ្យស្មានទុកថាព័ត៌មាននោះអាចបង្កឱ្យមានការទទួលខុសត្រូវផ្នែករដ្ឋប្បវេណីឬព្រហ្មទណ្ឌ។ ឬ

គ. អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកបានដឹងនាពេលក្រោយថាព័ត៌មាន ឬអង្គហេតុ ឬកាលៈទេសៈដែលអាចឱ្យស្មានទុកថា ព័ត៌មាននោះ

អាចបង្កឱ្យមានការទទួលខុសត្រូវខាងផ្នែករដ្ឋប្បវេណី ឬព្រហ្មទណ្ឌ ហើយបានអនុវត្ត តាមនីតិវិធីចំពោះព័ត៌មានខុសច្បាប់ និងការបរិហារកេរ្តិ៍ដូចមានចែងក្នុងមាត្រា២៥ ខាងក្រោម។

២. អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក មិនតម្រូវឱ្យតាមដាន ត្រួតពិនិត្យកំណត់ត្រាអេឡិចត្រូនិកណាមួយដែលដំណើរការដោយប្រព័ន្ធអេឡិចត្រូនិកដែលស្ថិត ក្រោមការគ្រប់គ្រងរបស់ខ្លួននោះឡើយ ទោះបីជាដំណើរការនៃកំណត់ត្រាអេឡិចត្រូនិកនោះ អាចបង្កើតជាបទល្មើស ឬនាំឱ្យមានការទទួលខុសត្រូវរដ្ឋប្បវេណីក៏ដោយ លើកលែងតែមានការ កំណត់ផ្សេងពីនេះ។

៣. បញ្ញត្តិនៃមាត្រានេះមិនត្រូវយកមកអនុវត្តដើម្បីឱ្យអន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្ម តាមប្រព័ន្ធអេឡិចត្រូនិករួចផុតពី៖

ក. កាតព្វកិច្ចដែលបង្កើតឡើងដោយច្បាប់ ឬលិខិតបទដ្ឋានគតិយុត្តនានា។

ខ. កាតព្វកិច្ចអនុលោមតាមបទបញ្ជា ឬសេចក្តីបង្គាប់របស់តុលាការ ឬអាជ្ញាធរមាន សមត្ថកិច្ចផ្សេងទៀត។ ឬ

គ. កាតព្វកិច្ចតាមកិច្ចសន្យា។

មាត្រា២៥ .. ការទទួលខុសត្រូវផ្នែកព័ត៌មានឬហេតុការណ៍

១. ក្នុងករណីដែលអន្តរការី ឬបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកបាន ដឹងថាព័ត៌មានក្នុងកំណត់ត្រាអាចបង្កឱ្យមានការទទួលខុសត្រូវខាងផ្នែករដ្ឋប្បវេណីឬព្រហ្មទណ្ឌ អន្តរការី ឬបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកត្រូវចាត់វិធានការជាបន្ទាន់ដូច ខាងក្រោម៖

ក. ដកព័ត៌មានចេញពីប្រព័ន្ធព័ត៌មានដែលស្ថិតក្រោមការគ្រប់គ្រង់របស់អន្តរការី និង បុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក ហើយឈប់ផ្តល់សេវាពាក់ព័ន្ធ នឹងព័ត៌មាននោះ។

ខ. រក្សាទុកព័ត៌មានជាភស្តុតាងនិងជូនដំណឹងដល់ក្រសួងប្រៃសណីយ៍និងទូរគមនាគមន៍ និងក្រសួង ស្ថាប័នមានសមត្ថកិច្ចពាក់ព័ន្ធនានាអំពីអង្គហេតុនិងអត្តសញ្ញាណនៃ ជនសង្ស័យ។

២. ក្នុងករណីដែលអន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកដឹង អំពីហេតុការណ៍ណាមួយ ឬស្ថានភាពណាមួយដែលអាចបណ្តាលឱ្យមានការទទួលខុសត្រូវខាង ផ្នែករដ្ឋប្បវេណីឬព្រហ្មទណ្ឌ អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក ត្រូវរក្សាទុកព័ត៌មានជាភស្តុតាងនិងជូនដំណឹងដល់ក្រសួងប្រៃសណីយ៍និងទូរគមនាគមន៍ និង ក្រសួង ស្ថាប័នមានសមត្ថកិច្ចពាក់ព័ន្ធនានា។

៣. នៅពេលបានដឹងឬទទួលដំណឹងពាក់ព័ន្ធនឹងព័ត៌មានក្នុងកំណត់ត្រាអេឡិចត្រូនិក ដែលអាចបង្កឱ្យមានការទទួលខុសត្រូវផ្នែករដ្ឋប្បវេណីឬព្រហ្មទណ្ឌ ក្រសួងប្រៃសណីយ៍និង

ទូរគមនាគមន៍ ឬក្រសួង ស្ថាប័នមានសមត្ថកិច្ចពាក់ព័ន្ធ អាចបញ្ជាឱ្យអន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក៖

ក. ដកព័ត៌មានចេញពីប្រព័ន្ធព័ត៌មានដែលស្ថិតក្រោមការគ្រប់គ្រងរបស់ខ្លួន។

ខ. ផ្អាកឬឈប់ផ្តល់សេវាដល់បុគ្គលនោះ។ ឬ

គ. ផ្អាកឬឈប់ផ្តល់សេវាពាក់ព័ន្ធនឹងកំណត់ត្រាអេឡិចត្រូនិក។

៤. អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មអេឡិចត្រូនិកមិនត្រូវទទួលខុសត្រូវផ្នែករដ្ឋប្បវេណី តាមកិច្ចសន្យាឬក្រៅកិច្ចសន្យា ឬកំណត់ដោយច្បាប់ ចំពោះការអនុវត្តដោយសុទ្ធចិត្តតាមបញ្ជារបស់ក្រសួងប្រៃសណីយ៍និងទូរគមនាគមន៍ឬក្រសួង ស្ថាប័នមានសមត្ថកិច្ចពាក់ព័ន្ធ។

៥. បុគ្គលដែលជូនដំណឹងអំពីសកម្មភាពខុសច្បាប់ទៅដល់អន្តរការីឬបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក ដោយដឹងថាការជូនដំណឹងនោះខុសពីការពិតឬមានលក្ខណៈបោកបញ្ឆោត ត្រូវទទួលខុសត្រូវខាងផ្នែករដ្ឋប្បវេណីឬព្រហ្មទណ្ឌពីអំពើនោះ។

មាត្រា២៦ .. ការផ្តល់លិខិតអនុញ្ញាតឬអាជ្ញាបណ្ណ

១. អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក ត្រូវស្នើសុំការអនុញ្ញាតឬអាជ្ញាបណ្ណពីក្រសួងពាណិជ្ជកម្មនិងក្រសួងប្រៃសណីយនិងទូរគមនាគមន៍។

២. ក្រសួងពាណិជ្ជកម្មផ្តល់លិខិតអនុញ្ញាតឬអាជ្ញាបណ្ណរួមមាន៖

ក. លិខិតអនុញ្ញាតប្រកបអាជីវកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកសម្រាប់រូបវន្តបុគ្គល។

ខ. អាជ្ញាបណ្ណឱ្យប្រតិបត្តិការផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកសម្រាប់នីតិបុគ្គល។

៣. ក្រសួងប្រៃសណីយ៍និងទូរគមនាគមន៍ផ្តល់វិញ្ញាបនបត្រសេវាអនឡាញ។

៤. ការលើកលែង ការកំណត់ប្រភេទអាជ្ញាបណ្ណ បែបបទ និងនីតិវិធីនៃការផ្តល់ការអនុញ្ញាតឬអាជ្ញាបណ្ណ ត្រូវកំណត់ដោយអនុក្រឹត្យ។

មាត្រា២៧ .. ក្រមសីលធម៌វិជ្ជាជីវៈនិងបទប្បញ្ញត្តិសម្រាប់អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក

១. អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកត្រូវអនុវត្តតាមក្រមសីលធម៌វិជ្ជាជីវៈ និងបទប្បញ្ញត្តិនានាពាក់ព័ន្ធនឹងពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកដែលកំណត់ដោយប្រកាសអន្តរក្រសួងរវាងក្រសួងពាណិជ្ជកម្មនិងក្រសួងប្រៃសណីយនិងទូរគមនាគមន៍។

២. ក្រមសីលធម៌វិជ្ជាជីវៈ ដែលបានលើកឡើងក្នុងបញ្ញត្តិនៃកថាខណ្ឌទី១ខាងលើត្រូវកំណត់និងរៀបរៀងឡើងដោយក្រសួងពាណិជ្ជកម្មនិងក្រសួងប្រៃសណីយនិងទូរគមនាគមន៍ ដោយសហការជាមួយក្រសួង ស្ថាប័ននិងភាគីពាក់ព័ន្ធ។

មាត្រា២៨ .. កាតព្វកិច្ចពន្ធ ការលើកទឹកចិត្ត និងការអនុគ្រោះ

អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក ត្រូវស្ថិតនៅក្រោមនីតិរួមនៃរបបសារពើពន្ធជាធរមាន និងទទួលបានការលើកទឹកចិត្តនិងការអនុគ្រោះនានា ស្របតាមច្បាប់និងបទប្បញ្ញត្តិជាធរមាន។

ជំពូកទី៦
កិច្ចការពារអ្នកប្រើប្រាស់

មាត្រា២៩ .- ព័ត៌មានអប្បបរមាក្នុងពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក

១. បុគ្គលដែលប្រើប្រាស់ទំនាក់ទំនងអេឡិចត្រូនិកដើម្បីលក់ទំនិញឬសេវាទៅឱ្យអ្នកប្រើប្រាស់ត្រូវផ្តល់ព័ត៌មានត្រឹមត្រូវ ច្បាស់លាស់ និងងាយយល់បាន ហើយត្រូវមានព័ត៌មានយ៉ាងតិចដូចខាងក្រោម៖

ក. ឈ្មោះឬនាមករណ៍ស្របច្បាប់របស់បុគ្គល អាសយដ្ឋានអាជីវកម្មដែលបានចុះបញ្ជី និងមធ្យោបាយអេឡិចត្រូនិកសម្រាប់ទំនាក់ទំនងឬលេខទូរសព្ទ។

ខ. ទម្រង់ទំនាក់ទំនងដែលរហ័ស ងាយស្រួល និងមានប្រសិទ្ធភាពរវាងអ្នកប្រើប្រាស់ជាមួយអ្នកលក់។

គ. ខចែង លក្ខខណ្ឌ និងសោហ៊ុយរបស់ទំនិញឬសេវានានាដែលពាក់ព័ន្ធនឹងប្រតិបត្តិការពាណិជ្ជកម្ម ជាពិសេស ខចែង លក្ខខណ្ឌ និងមធ្យោបាយទូទាត់ប្រាក់ និងព័ត៌មានលម្អិតពាក់ព័ន្ធនឹងការដកឬលុបចោលការបញ្ជាទិញ ការបញ្ឈប់ ការប្រគល់ និងការប្តូរទំនិញ និងការសងប្រាក់មកវិញ។ និង

ឃ. ទំនិញនិងសេវាជាក់ស្តែងដែលដាក់លក់។

២. ព័ត៌មានដែលមានចែងក្នុងបញ្ញត្តិនៃកថាខណ្ឌទី១ខាងលើ ចាំបាច់ត្រូវមានលក្ខណៈគ្រប់គ្រាន់ ដើម្បីឱ្យអ្នកប្រើប្រាស់អាចធ្វើការសម្រេចចិត្តលើប្រតិបត្តិការពាណិជ្ជកម្មនិងរក្សាទុកជាព័ត៌មាន។

៣. បញ្ញត្តិនៃមាត្រានេះមិនយកមកអនុវត្តចំពោះវិស័យមូលបត្រនិងធានារ៉ាប់រងឡើយ។

មាត្រា៣០ .- ទំនាក់ទំនងពាណិជ្ជកម្មដែលមិនបានស្នើសុំ

បុគ្គលណាក៏ដោយ ទោះបីជាមានទីតាំងអាជីវកម្មក្នុងឬក្រៅព្រះរាជាណាចក្រកម្ពុជាដែលផ្ញើទំនាក់ទំនងពាណិជ្ជកម្មដែលមិនបានស្នើសុំទៅកាន់អ្នកប្រើប្រាស់ដែលស្ថិតនៅក្នុងឬក្រៅព្រះរាជាណាចក្រកម្ពុជា តាមរយៈប្រព័ន្ធផ្សព្វផ្សាយ ឬតាមរយៈអន្តរការី ឬអ្នកផ្តល់សេវាទូរគមនាគមន៍ ត្រូវផ្តល់ជម្រើសច្បាស់លាស់និងងាយស្រួលសម្រាប់ឱ្យអ្នកប្រើប្រាស់អាចធ្វើការបដិសេធមិនទទួលយកទំនាក់ទំនងពាណិជ្ជកម្មដែលមិនបានស្នើសុំនោះ។

មាត្រា៣១ .- ការបង្កើតប្រព័ន្ធអេឡិចត្រូនិកក្លែងបន្លំនិងកូដព្យាបាទ

១. បុគ្គលទាំងឡាយមិនត្រូវបង្កើតប្រព័ន្ធអេឡិចត្រូនិក ក្នុងគោលបំណងក្លែងបន្លំឬបង្កការភាន់ច្រឡំ ដើម្បីទាញយកផលប្រយោជន៍ ឬក្នុងគោលបំណងទាក់ទាញឱ្យមានការប្រើប្រាស់ឬធ្វើប្រតិបត្តិការណាមួយនាំឱ្យមានព្យសនកម្មដល់បុគ្គលដែលប្រើប្រាស់នោះឬតតិយជនឡើយ។



២. បុគ្គលទាំងឡាយមិនត្រូវបង្កើត ផ្តល់ បង្កលទ្ធភាព ចែកចាយ ឬបញ្ជូននូវលេខកូដចម្លងមេរោគ ក្នុងគោលបំណងទុច្ចរិត តាមមធ្យោបាយអេឡិចត្រូនិក ទៅក្នុងឧបករណ៍ឬប្រព័ន្ធអេឡិចត្រូនិករបស់មនុស្សផ្សេងទៀតឡើយ។

មាត្រា៣២ .. ការការពារទិន្នន័យ

១. បុគ្គលដែលរក្សាព័ត៌មានជាលក្ខណៈឯកជនក្រោមទម្រង់អេឡិចត្រូនិក ត្រូវប្រើគ្រប់មធ្យោបាយដើម្បីធានាថា ព័ត៌មាននោះត្រូវបានការពារប្រកបដោយសុវត្ថិភាពគ្រប់កាលៈទេសៈ សមហេតុផល ដើម្បីជៀសវាង ការបាត់បង់ ការចូល ការប្រើប្រាស់ ការកែប្រែ ការបែកធ្លាយ ឬការលាតត្រដាងព័ត៌មានទាំងនោះ លើកលែងតែមានការអនុញ្ញាតពីម្ចាស់នៃព័ត៌មាននោះឬពីភាគីផ្សេងទៀតដែលអនុញ្ញាតដោយច្បាប់។

២. បុគ្គលទាំងឡាយមិនត្រូវជ្រៀតជ្រែកក្នុងប្រព័ន្ធអេឡិចត្រូនិក ចូលប្រើប្រាស់ ទាញយក ថតចម្លង ស្រង់យក ធ្វើឱ្យបែកធ្លាយ លុបបំបាត់ ឬកែប្រែទិន្នន័យ ដែលស្ថិតក្រោមការរក្សាទុករបស់បុគ្គលផ្សេងទៀត ដោយទុច្ចរិត ឬគ្មានការអនុញ្ញាតឡើយ។

មាត្រា៣៣ .. ការអនុវត្តបទប្បញ្ញត្តិទាក់ទងនឹងកិច្ចការពារអ្នកប្រើប្រាស់

បុគ្គលដែលប្រើប្រាស់ទំនាក់ទំនងអេឡិចត្រូនិកក្នុងសកម្មភាពពាណិជ្ជកម្មជាមួយអ្នកប្រើប្រាស់ក៏ត្រូវអនុវត្តតាមបទប្បញ្ញត្តិនានាទាក់ទងនឹងកិច្ចការពារអ្នកប្រើប្រាស់ផងដែរ។

ជំពូកទី៧
សកម្មភាពនិងប្រតិបត្តិការរបស់រដ្ឋតាមប្រព័ន្ធអេឡិចត្រូនិក

មាត្រា៣៤ .. ការទទួលស្គាល់ទំនាក់ទំនងអេឡិចត្រូនិកដោយស្ថាប័នរដ្ឋ

១. ក្រសួងឬស្ថាប័នរដ្ឋនានាអាចប្រើប្រាស់ទម្រង់អេឡិចត្រូនិកសម្រាប់សកម្មភាពនិងប្រតិបត្តិការ ដូចខាងក្រោម៖

ក. ការទទួលចុះបញ្ជីឯកសារ ឬការបំពេញលក្ខខណ្ឌតម្រូវ សម្រាប់បង្កើតឬរក្សាទុកឯកសារ។

ខ. ការចេញអាជ្ញាបណ្ណឬលិខិតអនុញ្ញាត។

គ. ការកំណត់មធ្យោបាយនិងរបៀបក្នុងការទូទាត់ប្រាក់។ ឬ

ឃ. សកម្មភាពផ្សេងទៀតដែលកំណត់ដោយក្រសួង ឬស្ថាប័នរដ្ឋ។

២. នៅពេលដែល ក្រសួង ឬស្ថាប័នរដ្ឋសម្រេចប្រើប្រាស់ទំនាក់ទំនងអេឡិចត្រូនិកសម្រាប់សកម្មភាព ឬប្រតិបត្តិការណាមួយ ដូចមានចែងក្នុងបញ្ញត្តិនៃកថាខណ្ឌទី១ខាងលើ ក្រសួងឬស្ថាប័ននោះអាចបញ្ជាក់៖

ក. របៀបនិងទម្រង់ដែលព័ត៌មានក្នុងទំនាក់ទំនងអេឡិចត្រូនិកត្រូវទទួលចុះបញ្ជី បង្កើតរក្សាទុក ឬបោះផ្សាយ។

ខ. ប្រភេទនៃហត្ថលេខាដែលតម្រូវឱ្យធ្វើនៅពេលដែលមានការតម្រូវឱ្យចុះហត្ថលេខាក្នុងទំនាក់ទំនងអេឡិចត្រូនិកនោះ។

គ. របៀបនិងទម្រង់ដែលហត្ថលេខានោះត្រូវភ្ជាប់ក្នុងទំនាក់ទំនងអេឡិចត្រូនិក។

ឃ. ដំណើរការគ្រប់គ្រងនិងនីតិវិធីដែលសមស្របដើម្បីធានាសុក្រឹតភាព សុវត្ថិភាព និងការរក្សាការសម្ងាត់នៃទំនាក់ទំនងអេឡិចត្រូនិក ឬការទូទាត់ប្រាក់ និង

ង. លក្ខខណ្ឌកំណត់ផ្សេងទៀតដែលផ្តល់តម្លៃសមមូលរវាងឯកសារ ឬការទូទាត់ក្នុងទម្រង់អេឡិចត្រូនិក ជាមួយនឹងឯកសារ ឬការទូទាត់ក្នុងទម្រង់ជាលាយលក្ខណ៍អក្សរ។

ជំពូកទី៨
ភស្តុតាងអេឡិចត្រូនិក

មាត្រា៣៥ .. ការទទួលយកជាទូទៅនូវភស្តុតាងអេឡិចត្រូនិក

គ្មានបទប្បញ្ញត្តិនៃវិធានស្តីពីភស្តុតាងណាមួយដែលយកមកអនុវត្ត ដើម្បីបដិសេធក្នុងការទទួលយកជាទូទៅនូវកំណត់ត្រាអេឡិចត្រូនិកធ្វើជាភស្តុតាង ដោយហេតុផលគ្រាន់តែសម្អាងលើមូលដ្ឋានថា វាជាកំណត់ត្រាអេឡិចត្រូនិកនោះឡើយ ទោះបីជាភស្តុតាងនោះមិនស្ថិតក្នុងទម្រង់ដើមក៏ដោយ។

មាត្រា៣៦ .. សុក្រឹតភាពនៃប្រព័ន្ធអេឡិចត្រូនិក

១. នៅក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់ សុពលភាពនៃភស្តុតាងអេឡិចត្រូនិកអាចត្រូវបានបញ្ជាក់តាមរយៈសុក្រឹតភាពនៃប្រព័ន្ធអេឡិចត្រូនិក ដែលបានកត់ត្រាឬរក្សាទុកនូវទិន្នន័យណាមួយ។

២. លើកលែងតែមានភស្តុតាងផ្ទុយ ប្រព័ន្ធអេឡិចត្រូនិកដែលបានប្រើប្រាស់សម្រាប់កត់ត្រា ឬរក្សាទុកកំណត់ត្រាអេឡិចត្រូនិក ត្រូវបានសន្មតថាមានសុក្រឹតភាព ក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់ តាមលក្ខខណ្ឌណាមួយដូចខាងក្រោម៖

ក. ក្នុងករណីមានភស្តុតាងគាំទ្រដល់អង្គហេតុណាមួយដែលបញ្ជាក់ថាប្រព័ន្ធអេឡិចត្រូនិកឬឧបករណ៍ស្រដៀងគ្នាផ្សេងទៀត បានដំណើរការជាប្រក្រតីនៅពេលដែលកំណត់ត្រាអេឡិចត្រូនិកនោះត្រូវបានកត់ត្រាឬរក្សាទុកឬនៅពេលដែលយកទៅធ្វើជាភស្តុតាង ឬក្នុងករណីដែលប្រព័ន្ធអេឡិចត្រូនិក ឬឧបករណ៍ ស្រដៀងគ្នាផ្សេងទៀតនោះមិនបានដំណើរការជាប្រក្រតី ឬឈប់ដំណើរការទាំងស្រុង ប៉ុន្តែមិនធ្វើឱ្យប៉ះពាល់ដល់សុក្រឹតភាពនៃកំណត់ត្រាអេឡិចត្រូនិក ហើយគ្មានមូលហេតុ សមស្របណាផ្សេងយកមកជំទាស់សុក្រឹតភាពនៃកំណត់ត្រានោះ។

ខ. ក្នុងករណីមានភស្តុតាងអាចបង្ហាញបានថា កំណត់ត្រាអេឡិចត្រូនិកត្រូវបានកត់ត្រា ឬរក្សាទុក ដោយភាគីដែលមានផលប្រយោជន៍ផ្ទុយគ្នាទៅនឹងភាគីម្ខាងទៀតដែលប្រើប្រាស់កំណត់ត្រាអេឡិចត្រូនិកនោះជាភស្តុតាងក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់។ ឬ

គ. នៅពេលដែលមានភស្តុតាងអាចបង្ហាញបានថា កំណត់ត្រាអេឡិចត្រូនិកត្រូវបានកត់ត្រាឬរក្សាទុកជាប្រក្រតីក្នុងគោលបំណងអាជីវកម្មធម្មតាដោយបុគ្គលដែលមិនមែនជាភាគីក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់ ហើយបុគ្គលនោះមិនបានកត់ត្រា ឬរក្សាទុកនូវកំណត់ត្រាអេឡិចត្រូនិកក្រោមការគ្រប់គ្រងរបស់ភាគីដែលប្រើប្រាស់កំណត់ត្រាអេឡិចត្រូនិកនោះជាភស្តុតាងក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់។

មាត្រា៣៧ .. សុក្រឹតភាពនៃព័ត៌មាន

១. លើកលែងតែមានភស្តុតាងផ្ទុយពីនេះ កំណត់ត្រាអេឡិចត្រូនិកដែលបានកត់ត្រាឬរក្សាទុកនៅក្នុងប្រព័ន្ធអេឡិចត្រូនិកត្រូវបានសន្មតថាមានសុក្រឹតភាពនៅក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់ ប្រសិនបើកំណត់ត្រាអេឡិចត្រូនិកនោះ៖

ក. នៅពេញលេញនិងគ្មានការកែប្រែក្រៅពីការធ្វើបដិលេខបន្ថែមណាមួយ ឬការផ្លាស់ប្តូរដែលមិនសំខាន់ណាមួយដែលកើតឡើងនៅក្នុងដំណើរការជាប្រក្រតីនៃទំនាក់ទំនងការរក្សាទុកឬការបង្ហាញ។

ខ. ត្រូវបានបញ្ជាក់ឬចុះហត្ថលេខានៅក្នុងទម្រង់អេឡិចត្រូនិក តាមរយៈមធ្យោបាយដែលផ្តល់ឱ្យដោយអ្នកផ្តល់នីតិវិធីសុវត្ថិភាពដែលមានអាជ្ញាបណ្ណត្រឹមត្រូវ។

គ. មានសុក្រឹតភាពនិងមានខ្លឹមសារដែលត្រូវបានបញ្ជាក់ដោយក្រសួងឬស្ថាប័នមានសមត្ថកិច្ច។

ឃ. ត្រូវបានកត់ត្រាទុកនៅក្នុងឧបករណ៍រក្សាទុកឬតាមមធ្យោបាយអេឡិចត្រូនិកផ្សេងទៀតដែលមិនអនុញ្ញាតឱ្យមានការកែប្រែទៅលើកំណត់ត្រាអេឡិចត្រូនិក។

ង. ត្រូវបានត្រួតពិនិត្យនិងបញ្ជាក់ពីសុក្រឹតភាព ដោយអ្នកជំនាញដែលត្រូវបានតែងតាំងដោយតុលាការ។

ច. នៅពេលដែលមានភស្តុតាងគាំទ្រដល់អង្គហេតុណាមួយ ដែលបញ្ជាក់ថាប្រព័ន្ធអេឡិចត្រូនិកឬឧបករណ៍ស្រដៀងគ្នាផ្សេងទៀតបានដំណើរការជាប្រក្រតីនៅគ្រប់រយៈពេលសំខាន់ៗ ឬក្នុងករណីដែលប្រព័ន្ធអេឡិចត្រូនិកឬឧបករណ៍ស្រដៀងគ្នាផ្សេងទៀតនោះមិនបានដំណើរការជាប្រក្រតីឬឈប់ដំណើរការទាំងស្រុង តែសុក្រឹតភាពនៃកំណត់ត្រាមិនរងការប៉ះពាល់ដោយសារស្ថានភាពទាំងនោះទេ ហើយគ្មានមូលហេតុសមស្របណាផ្សេងទៀតដែលចោទជាមន្ទិលសង្ស័យលើសុក្រឹតភាពនៃកំណត់ត្រានោះឡើយ។ ឬ

ឆ. នៅពេលដែលមានភស្តុតាងអាចបង្ហាញបានថាកំណត់ត្រាអេឡិចត្រូនិកត្រូវបានកត់ត្រាឬរក្សាទុកដោយភាគីដែលចូលរួមនៅក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់នោះ ហើយដែលភាគីមានទំនាស់ផលប្រយោជន៍ផ្ទុយគ្នាទៅនឹងភាគីម្ខាងទៀត ដែលមានបំណងប្រើប្រាស់កំណត់ត្រាអេឡិចត្រូនិកនោះ។

២. នៅពេលដែលមានភស្តុតាងអាចបង្ហាញបានថាកំណត់ត្រាអេឡិចត្រូនិកត្រូវបានកត់ត្រាឬរក្សាទុកតាមធម្មតានិងក្នុងគោលបំណងអាជីវកម្មធម្មតា ដោយបុគ្គលដែលមិនមែនជាភាគីនៅក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់ ហើយបុគ្គលនោះមិនបានកត់ត្រាឬរក្សាទុកនូវកំណត់ត្រាអេឡិចត្រូនិក ឬតាមការគ្រប់គ្រងរបស់ភាគីដែលមានបំណងប្រើប្រាស់កំណត់ត្រាអេឡិចត្រូនិកនោះ។

៣. នៅពេលដែលរបាយការណ៍ត្រូវបានកត់ត្រាទុកនៅក្នុងកំណត់ត្រាអេឡិចត្រូនិក ដែលត្រូវបានបង្កើតឡើងដោយប្រព័ន្ធអេឡិចត្រូនិក មិនត្រូវបានចាត់ទុកថាជាពាក្យចចាមអារ៉ាម ទេនោះ របាយការណ៍ទាំងនោះអាចទទួលយកបាន ប្រសិនបើលក្ខខណ្ឌដូចដែលមានចែងនៅក្នុងបញ្ញត្តិនៃកថាខណ្ឌទី២ ទាក់ទងនឹងកំណត់ត្រាអេឡិចត្រូនិកនោះត្រូវបានបំពេញ។

មាត្រា៣៨ .. ឯកសារដែលបានបោះពុម្ពចេញ

ឯកសារដែលបានបោះពុម្ពចេញត្រឹមត្រូវស្របនឹងខ្លឹមសារដើមចេញពីកំណត់ត្រាអេឡិចត្រូនិក អាចយកមកប្រើប្រាស់ជាភស្តុតាងបានក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់។

មាត្រា៣៩ .. បន្ទុកក្នុងការបង្ហាញអំពីយថាភូតភាពនៃភស្តុតាងអេឡិចត្រូនិក

១. បុគ្គលដែលស្នើសុំបង្ហាញកំណត់ត្រាអេឡិចត្រូនិកក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់ ណាមួយ បុគ្គលនោះត្រូវទទួលបន្ទុកបង្ហាញពីយថាភូតភាពនៃកំណត់ត្រាអេឡិចត្រូនិកដោយ មានភស្តុតាងគាំទ្រដល់កំណត់ត្រាដែលបានបង្ហាញ។

២. ក្នុងករណីមានបទប្បញ្ញត្តិណាមួយការពារបុគ្គលងាយរងគ្រោះដែលរាប់បញ្ចូលទាំងអ្នក ប្រើប្រាស់និងកុមារ ហើយដែលមានកំណត់អំពីបន្ទុកនៃការបង្ហាញភស្តុតាងដែលផ្តល់ប្រយោជន៍ ដល់បុគ្គលទាំងនោះច្រើនជាងច្បាប់នេះ បទប្បញ្ញត្តិនោះត្រូវមានអាទិភាពជាងមាត្រានេះ។

មាត្រា៤០ .. បទដ្ឋាននៃការកត់ត្រាឬការរក្សាទុកកំណត់ត្រាអេឡិចត្រូនិក

ដើម្បីកំណត់បានថាកំណត់ត្រាអេឡិចត្រូនិកត្រូវទទួលយកឬមិនទទួលយកក្នុងបទប្បញ្ញត្តិ ផ្សេងទៀត ការបង្ហាញភស្តុតាងអាចត្រូវធ្វើឡើងដោយផ្អែកលើបទដ្ឋាន នីតិវិធី ការប្រើឬការអនុវត្ត នៃការកត់ត្រាឬរក្សាទុកកំណត់ត្រាអេឡិចត្រូនិក ដោយត្រូវពិនិត្យពិចារណាអំពីប្រភេទអាជីវកម្ម ចរិតលក្ខណៈ និងគោលបំណងនៃកំណត់ត្រាអេឡិចត្រូនិកនោះ។

មាត្រា៤១ .. ការចេញលិខិតបញ្ជាក់យថាភូតភាព

១. ក្នុងករណីដែលបុគ្គលណាមួយមានបំណងចង់បង្ហាញយថាភូតភាពនៃកំណត់ត្រា អេឡិចត្រូនិកមួយដើម្បីធ្វើជាភស្តុតាង បុគ្គលនោះអាចស្នើសុំភស្តុតាងនោះពីអ្នកជំនាញពាក់ព័ន្ធ នឹងយថាភូតភាពនៃកំណត់ត្រាអេឡិចត្រូនិកនោះក្រោមទម្រង់ជាលិខិតបញ្ជាក់។

២. លិខិតបញ្ជាក់យថាភូតភាពដូចមានចែងក្នុងបញ្ញត្តិនៃកថាខណ្ឌទី១ខាងលើត្រូវចេញ ដោយ៖

ក. ក្រសួង ស្ថាប័នមានសមត្ថកិច្ច ឬបុគ្គលដែលទទួលខុសត្រូវពាក់ព័ន្ធនឹងប្រតិបត្តិការ ឬការគ្រប់គ្រងអ្នកបង្កើតនីតិវិធីសុវត្ថិភាពជាក់លាក់ណាមួយ ឬអ្នកបង្កើតនីតិវិធី សុវត្ថិភាពដែលទទួលស្គាល់ដោយតុលាការ។ ឬ

ខ. អ្នកជំនាញដែលតែងតាំងឬដែលទទួលស្គាល់ដោយតុលាការ។

៣. បុគ្គលដែលមានសមត្ថកិច្ចក្នុងការចេញលិខិតបញ្ជាក់យថាភូតភាព ដូចមានចែងក្នុង បញ្ញត្តិនៃកថាខណ្ឌទី២ខាងលើ មិនត្រូវក្លែងឬចេញលិខិតបញ្ជាក់យថាភូតភាពនៃកំណត់ត្រាឬ ភស្តុតាងអេឡិចត្រូនិកដែលមានលក្ខណៈក្លែងបន្លំឬមិនមែនជាការពិតនោះឡើយ។

មាត្រា៤២ .. នីតិវិធីផ្សេងទៀតក្នុងការបង្កើតភស្តុតាងអេឡិចត្រូនិក

បន្ថែមលើមធ្យោបាយបង្ហាញភស្តុតាងដូចមានចែងក្នុងច្បាប់នេះ ភស្តុតាងអេឡិចត្រូនិកអាចត្រូវបានបង្កើតឡើង តាមបច្ចេកទេសនិងនីតិវិធីផ្សេងទៀតដូចជា ការបញ្ជាក់ដោយសាក្សី ឬស្ថាប័នមានសមត្ថកិច្ច កំណត់ត្រាក្នុងមធ្យោបាយអេឡិចត្រូនិកដែលមិនអនុញ្ញាតឱ្យមានការកែប្រែបាន និងលទ្ធផលកោសល្យវិច័យលើប្រព័ន្ធអេឡិចត្រូនិកតាមការរកឃើញរបស់យុត្តាធិការតុលាការ។

មាត្រា៤៣ .. ការបំពានលើកូដនីយកម្ម

បុគ្គលទាំងឡាយមិនត្រូវដាក់កូដក្នុងទំនាក់ទំនងពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកដែលជាភស្តុតាងអាចនាំទៅដល់ការចោទប្រកាន់ ឬការដាក់កូដលើទិន្នន័យ ឬភស្តុតាងក្នុងប្រព័ន្ធអេឡិចត្រូនិកដែលទាក់ទិននឹងបទល្មើសឡើយ។

មាត្រា៤៤ .. ការទទួលយកកំណត់ត្រាអេឡិចត្រូនិកពីបរទេស

ភស្តុតាងអេឡិចត្រូនិកដែលបញ្ជាក់ដោយក្រសួងឬស្ថាប័នមានសមត្ថកិច្ចនៃបណ្តារដ្ឋបរទេសត្រូវបានទទួលយកជាភស្តុតាង ប្រសិនបើប្រព័ន្ធអេឡិចត្រូនិកដែលកត់ត្រាឬរក្សាទុកកំណត់ត្រាអេឡិចត្រូនិកនោះមានសុក្រឹតភាពស្របតាមបទដ្ឋាន ដូចមានចែងក្នុងជំពូកទី៨នៃច្បាប់នេះ។

មាត្រា៤៥ .. ការទទួលយកព័ត៌មានអេឡិចត្រូនិកមកពីបរទេស

ដើម្បីកំណត់ថាព័ត៌មានក្នុងទម្រង់អេឡិចត្រូនិកមួយអាចទទួលយកឬមិនអាចទទួលយកបាន ឬអាចទទួលយកបានត្រឹមកម្រិតណាមួយនោះ មិនត្រូវគិតពីទីតាំងដែលព័ត៌មាននោះត្រូវបានបង្កើតឡើងឬត្រូវបានប្រើប្រាស់ ឬទីតាំងអាជីវកម្មដែលបានបង្កើតឡើងនៅបរទេសនោះឡើយ ឱ្យតែកំណត់ត្រាអេឡិចត្រូនិកនោះអាចចូលនិងទាញយកមកប្រើបាននៅក្នុងដែនសមត្ថកិច្ចនៃព្រះរាជាណាចក្រកម្ពុជា។

ជំពូកទី៩
ការទូទាត់និង/ឬការផ្ទេរប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក

មាត្រា៤៦ .. ប្រតិបត្តិការទូទាត់តាមប្រព័ន្ធអេឡិចត្រូនិក

១- បុគ្គលណាដែលធ្វើប្រតិបត្តិការប្រព័ន្ធទូទាត់ ផ្តល់សេវាទូទាត់ ចេញផ្សាយឧបករណ៍ទូទាត់ប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក ឬផ្តល់មធ្យោបាយទូទាត់ប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក ឬធ្វើប្រតិបត្តិការណាដែលត្រូវបានចាត់ទុកថាជាការផ្តល់ការទូទាត់សងប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិកដល់សាធារណជនត្រូវស្នើសុំការអនុញ្ញាតឬអាជ្ញាបណ្ណជាមុនពីធនាគារជាតិនៃកម្ពុជា។

២- ធនាគារជាតិនៃកម្ពុជាជាស្ថាប័នមានសមត្ថកិច្ចក្នុងការរៀបចំបទប្បញ្ញត្តិទាក់ទងនឹងការទូទាត់ប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក។

មាត្រា៤៧ .. ការទទួលខុសត្រូវរបស់បុគ្គលផ្តល់សេវាទូទាត់

១. បុគ្គលផ្តល់សេវាទូទាត់មិនត្រូវផ្តល់ជូនអតិថិជននូវឧបករណ៍ទូទាត់ ដែលអតិថិជនមិនបានស្នើសុំនោះទេ លើកលែងតែករណីដែលបណ្ណទូទាត់នោះជាបណ្ណទូទាត់ហួសរយៈពេលប្រើប្រាស់ ឬដល់ពេលត្រូវផ្លាស់ប្តូរ។

២. មុនពេលធ្វើប្រតិបត្តិការផ្ទេរប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក បុគ្គលផ្តល់សេវាត្រូវបញ្ជាក់ឱ្យបានច្បាស់ពីអត្តសញ្ញាណរបស់អតិថិជននិងផ្ទៀងផ្ទាត់ឡើងវិញនូវភាពត្រឹមត្រូវនៃការផ្ទេរប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក។ បុគ្គលផ្តល់សេវាទូទាត់ត្រូវទទួលខុសត្រូវលើករណីដូចខាងក្រោម៖

ក. ប្រតិបត្តិការកើតឡើងដោយគ្មានការអនុញ្ញាតពីអតិថិជន។

ខ. ប្រតិបត្តិការកើតឡើងបន្ទាប់ពីដឹងថាមានការបន្លំ បាត់បង់ ឬចោរកម្មនៃឧបករណ៍ផ្ទេរប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក។

គ. ប្រតិបត្តិការកើតឡើងបន្ទាប់ពីមានការជូនដំណឹងពីអតិថិជនដូចមានចែងក្នុងមាត្រា៤៨ខាងក្រោម។

ឃ. ការខកខានមិនបានប្រតិបត្តិតាមបញ្ជារបស់អតិថិជនឬការប្រតិបត្តិខុសពីបញ្ជារបស់អតិថិជន។ ឬ

ង. ភាពមិនប្រក្រតីនៃប្រព័ន្ធបច្ចេកទេស កំហុសក្នុងការប្រើប្រាស់ប្រព័ន្ធបច្ចេកទេស ឬភាពខ្វះខាតនៃឧបករណ៍ផ្ទេរប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក។

៣. បុគ្គលផ្តល់សេវាទូទាត់អាចរួចផុតពីការទទួលខុសត្រូវបានតែក្នុងករណីប្រធានសក្តិ ឬជាកំហុសរបស់អតិថិជនផ្ទាល់ប៉ុណ្ណោះ។

៤. ក្នុងករណីដែលបុគ្គលផ្តល់សេវាទូទាត់ត្រូវទទួលខុសត្រូវ បុគ្គលផ្តល់សេវាទូទាត់ត្រូវសងថ្លៃខូចខាតជូនអតិថិជនក្នុងរយៈពេលមិនឱ្យលើសពី៣០(សាមសិប)ថ្ងៃ គិតចាប់ពីថ្ងៃបានទទួលការជូនដំណឹងពីអតិថិជនដូចមានចែងក្នុងមាត្រា៤៨នៃច្បាប់នេះ នូវកម្រៃប្រតិបត្តិការដែលបានខាតបង់សោហ៊ុយ និងការពិន័យក្នុងការបង់ការប្រាក់យឺតយ៉ាវដែលកើតចេញពីប្រតិបត្តិការនេះ ដោយ មិនទាន់គិតបញ្ចូលការសងថ្លៃខូចខាតដទៃទៀតដែលអាចកើតឡើងចំពោះអតិថិជន។

៥. បុគ្គលទាំងឡាយមិនត្រូវចេញផ្សាយបណ្ណទូទាត់ ឬកែប្រែបណ្ណទូទាត់ទៅជាទម្រង់ណាមួយដែលខុសពីទម្រង់ដើម ដោយគ្មានការអនុញ្ញាតក្នុងគោលបំណងទុច្ចរិត ឆបោក ឬក្លែងបន្លំដែលនាំឱ្យមានព្យសនកម្មដល់បុគ្គលមួយផ្សេងទៀតឡើយ។

មាត្រា៤៨ .. ការទទួលខុសត្រូវរបស់អតិថិជន

១. អតិថិជនត្រូវជូនដំណឹងដល់បុគ្គលផ្តល់សេវាទូទាត់ អំពីប្រតិបត្តិការដែលកើតឡើងដោយគ្មានការអនុញ្ញាត កំហុសឆ្គង ឬភាពមិនត្រឹមត្រូវផ្សេងទៀតនៅក្នុងគណនីរបស់ខ្លួន។

២. អតិថិជនត្រូវជូនដំណឹងដល់បុគ្គលផ្តល់សេវាទូទាត់ឬគ្រឹះស្ថានដែលទទួលបានការអនុញ្ញាតពីបុគ្គលផ្តល់សេវាទូទាត់អំពីករណីបាត់បង់ឬអំពើចោរកម្មលើឧបករណ៍/មធ្យោបាយផ្ទេរប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក ឬការលួចយកទិន្នន័យសម្រាប់ប្រើប្រាស់ជាមួយឧបករណ៍ទូទាត់។ ការជូនដំណឹងនេះអាចធ្វើឡើងជាលាយលក្ខណ៍អក្សរឬតាមមធ្យោបាយអេឡិចត្រូនិកណាមួយដែលទទួលយកដោយបុគ្គលផ្តល់សេវាទូទាត់ ហើយត្រូវជូនដំណឹងជាបន្ទាន់តាមលទ្ធភាពដែលអាចធ្វើទៅបានឬមិនឱ្យលើសរយៈពេល២(ពីរ)ថ្ងៃ បន្ទាប់ពីបានដឹងថាមានករណីចោរកម្ម ឬបាត់បង់ឧបករណ៍ទូទាត់កើតឡើង។

៣. ក្នុងករណីមានភស្តុតាងគ្រប់គ្រាន់បញ្ជាក់ថាការបាត់បង់ឬការខូចខាតក្នុងករណីខាងលើជាកំហុសរបស់អតិថិជន បុគ្គលផ្តល់សេវាទូទាត់មានសិទ្ធិទាមទារឱ្យអតិថិជនទទួលខុសត្រូវទាំងស្រុងចំពោះការបាត់បង់ឬការខូចខាតនោះ។

៤. ក្នុងករណីមិនមានភស្តុតាងបញ្ជាក់អំពីកំហុសរបស់អតិថិជនទេ បុគ្គលផ្តល់សេវាទូទាត់ត្រូវទទួលខុសត្រូវទាំងស្រុងចំពោះការបាត់បង់ឬការខូចខាតនោះ ដោយឥតលក្ខខណ្ឌ។

ជំពូកទី១០
សមត្ថកិច្ច ការប្តឹងតវ៉ា និងនីតិវិធីនៃការផាកពិន័យ

មាត្រា៤៩ .. សមត្ថកិច្ច

ការព្រមានជាលាយលក្ខណ៍អក្សរ ការបញ្ឈប់សកម្មភាពឬប្រតិបត្តិការអាជីវកម្ម ការព្យួរ ការដកហូត ឬការលុបចោលលិខិតអនុញ្ញាតឬអាជ្ញាបណ្ណ និងការផាកពិន័យ ជាសមត្ថកិច្ចរបស់ក្រសួងពាណិជ្ជកម្មនិងក្រសួងប្រៃសណីយនិងទូរគមនាគមន៍។

ក្នុងករណីដែលបុគ្គលមិនអនុវត្តតាមវិធានការខាងលើ ក្រសួងពាណិជ្ជកម្មនិងក្រសួងប្រៃសណីយនិងទូរគមនាគមន៍ អាចធ្វើបណ្តឹងទៅតុលាការមានសមត្ថកិច្ច។

មាត្រា៥០ .. នីតិវិធីនៃការប្តឹងតវ៉ា

១. បុគ្គលដែលមិនសុខចិត្តនឹងការព្រមានជាលាយលក្ខណ៍អក្សរ ការបញ្ឈប់សកម្មភាពឬប្រតិបត្តិការអាជីវកម្ម ការព្យួរ ការដកហូត ឬការលុបចោលលិខិតអនុញ្ញាតឬអាជ្ញាបណ្ណ និងការផាកពិន័យរបស់ក្រសួងពាណិជ្ជកម្មនិងក្រសួងប្រៃសណីយនិងទូរគមនាគមន៍ មានសិទ្ធិប្តឹងតវ៉ាទៅរដ្ឋមន្ត្រីក្រសួងពាណិជ្ជកម្មនិងក្រសួងប្រៃសណីយនិងទូរគមនាគមន៍។

២. រដ្ឋមន្ត្រីក្រសួងពាណិជ្ជកម្មនិងក្រសួងប្រៃសណីយនិងទូរគមនាគមន៍ត្រូវសម្រេចក្នុងរយៈពេល៣០(សាមសិប)ថ្ងៃយ៉ាងយូរ។

៣. បុគ្គលណាមួយដែលមិនសុខចិត្តនឹងសេចក្តីសម្រេចរបស់រដ្ឋមន្ត្រីក្រសួងពាណិជ្ជកម្មនិងក្រសួងប្រៃសណីយនិងទូរគមនាគមន៍ មានសិទ្ធិប្តឹងតវ៉ាទៅតុលាការមានសមត្ថកិច្ចនៃព្រះរាជាណាចក្រកម្ពុជាបានក្នុងរយៈពេល៣០(សាមសិប)ថ្ងៃយ៉ាងយូរ គិតចាប់ពីថ្ងៃទទួលបានសេចក្តីជូនដំណឹងនៃសេចក្តីសម្រេចនោះ។

មាត្រា៥១ .. នីតិវិធីនៃការជាកពិន័យ

នីតិវិធីនៃការជាកពិន័យ ការបង់ប្រាក់ជាកពិន័យ ការគ្រប់គ្រងបង្កាន់ដៃបង់ប្រាក់ពិន័យ និងការចាត់ចែងប្រាក់ចំណូលដែលបានពីការជាកពិន័យ ដូចមានចែងនៅក្នុងបទប្បញ្ញតិច្បាប់នេះ ត្រូវកំណត់ដោយប្រកាសអន្តរក្រសួងរវាងរដ្ឋមន្ត្រីក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ រដ្ឋមន្ត្រីក្រសួងពាណិជ្ជកម្ម និងរដ្ឋមន្ត្រីក្រសួងប្រៃសណីយ៍និងទូរគមនាគមន៍។

ជំពូកទី១១
ទោសប្បញ្ញត្តិ

មាត្រា៥២ .. ទណ្ឌកម្ម

ទណ្ឌកម្មនៅក្នុងច្បាប់នេះរួមមាន ការព្រមានជាលាយលក្ខណ៍អក្សរ ការបញ្ឈប់សកម្មភាពឬប្រតិបត្តិការអាជីវកម្ម ការព្យួរការដកហូតឬការលុបចោលលិខិតអនុញ្ញាតឬអាជ្ញាបណ្ណ ការជាកពិន័យ ទោសដាក់ពន្ធនាគារ និងទោសពិន័យជាប្រាក់។

មាត្រា៥៣ .. អំពើល្មើសលើការលួចប្រើប្រាស់អត្តសញ្ញាណ

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី៦(ប្រាំមួយ)ខែទៅ៣(បី)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី ១ ០០០ ០០០(មួយលាន)រៀលទៅ៦ ០០០ ០០០(ប្រាំមួយលាន)រៀល ចំពោះបុគ្គលណាដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃមាត្រា២២។

មាត្រា៥៤ .. អំពើល្មើសលើការមិនរាយការណ៍អំពីព័ត៌មានឬហេតុការណ៍

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី១(មួយ)ខែទៅ១(មួយ)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី១០០ ០០០ (មួយសែន)រៀលទៅ២ ០០០ ០០០(ពីរលាន)រៀល ចំពោះអំពើរបស់អន្តរការីនិងបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិកដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃកថាខណ្ឌទី១និងកថាខណ្ឌទី២នៃមាត្រា២៥។

មាត្រា៥៥ .. អំពើផ្តល់ពត៌មានមិនពិត

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី១(មួយ)ខែទៅ១(មួយ)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី១០០ ០០០ (មួយសែន)រៀលទៅ២ ០០០ ០០០(ពីរលាន)រៀល ចំពោះបុគ្គលណាដែលប្រព្រឹត្តអំពើដូចមានចែងក្នុងបញ្ញត្តិនៃកថាខណ្ឌទី៥នៃមាត្រា២៥។

មាត្រា៥៦ .. ការធ្វើប្រតិបត្តិការដោយគ្មានការអនុញ្ញាត

ត្រូវបញ្ឈប់សកម្មភាពឬប្រតិបត្តិការអាជីវកម្មនិងត្រូវទទួលការជាកពិន័យជាប្រាក់មិនលើសពី១០ ០០០ ០០០(ដប់លាន)រៀល ចំពោះបុគ្គលទាំងឡាយណាដែលប្រព្រឹត្តផ្ទុយនឹងបញ្ញត្តិនៃកថាខណ្ឌទី១នៃមាត្រា២៦។

ក្នុងករណីធ្លាប់ទទួលរងនូវវិធានការដូចមានចែងក្នុងកថាខណ្ឌទី១ជាស្ថាពររួចហើយហើយមានប្រព្រឹត្តបទល្មើសដដែលនេះ ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី១(មួយ)ឆ្នាំទៅ៣(បី)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី២ ០០០ ០០០(ពីរលាន)រៀលពី៦ ០០០ ០០០(ប្រាំមួយលាន)រៀល។

មាត្រា៥៧ .. អំពើល្មើសលើការមិនអនុវត្តតាមបទប្បញ្ញតិស្តីពីព័ត៌មានអប្បបរមាក្នុងពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក

ត្រូវទទួលការព្រមានជាលាយលក្ខណ៍អក្សរ ចំពោះបុគ្គលណាដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃកថាខណ្ឌទី១និងកថាខណ្ឌទី២នៃមាត្រា២៩។

ក្នុងករណីទទួលរងនូវការព្រមានជាលាយលក្ខណ៍អក្សរម្តងរួចហើយ នៅតែបន្តប្រព្រឹត្តល្មើសដូចមានចែងក្នុងកថាខណ្ឌទី១ខាងលើនេះ ត្រូវព្យួរឬដកហូតអាជ្ញាបណ្ណឬលិខិតអនុញ្ញាតជាបុគ្គលផ្តល់ពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក។

មាត្រា៥៨ .. អំពើល្មើសលើការផ្ញើទំនាក់ទំនងពាណិជ្ជកម្មដែលមិនបានស្នើសុំ

ត្រូវទទួលការព្រមានជាលាយលក្ខណ៍អក្សរ ចំពោះបុគ្គលណាដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃមាត្រា៣០។

ក្នុងករណីទទួលរងនូវការព្រមានជាលាយលក្ខណ៍អក្សរម្តងរួចហើយ នៅតែបន្តប្រព្រឹត្តល្មើស ដូចមានចែងក្នុងកថាខណ្ឌទី១ខាងលើនេះ ត្រូវព្យួរឬដកហូតអាជ្ញាបណ្ណឬលិខិតអនុញ្ញាតជាអន្តរការីឬបុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក ឬបិទមិនឱ្យដំណើរការនូវប្រព័ន្ធផ្សព្វផ្សាយឬមធ្យោបាយអេឡិចត្រូនិករបស់អ្នកផ្ញើ។

មាត្រា៥៩ .. អំពើល្មើសលើការក្លែងប្រព័ន្ធអេឡិចត្រូនិកនិងកូដព្យាបាទ

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី៦(ប្រាំមួយ)ខែទៅ៣(បី)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី ១ ០០០ ០០០(មួយលាន)រៀលទៅ៦ ០០០ ០០០(ប្រាំមួយលាន)រៀល ចំពោះបុគ្គលណាដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃមាត្រា៣១។

មាត្រា៦០ .. អំពើល្មើសលើការមិនអនុវត្តកាតព្វកិច្ចការពារទិន្នន័យ

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី១(មួយ)ឆ្នាំទៅ២(ពីរ)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី២ ០០០ ០០០ (ពីរលាន)រៀលទៅ៤ ០០០ ០០០(បួនលាន)រៀល ចំពោះបុគ្គលដែលរក្សាព័ត៌មានជាលក្ខណៈឯកជនក្រោមទម្រង់អេឡិចត្រូនិក ដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃកថាខណ្ឌទី១នៃមាត្រា៣២។

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី១(មួយ)ឆ្នាំទៅ២(ពីរ)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី២ ០០០ ០០០ (ពីរលាន)រៀលទៅ៤ ០០០ ០០០(បួនលាន)រៀល ចំពោះបុគ្គលណាដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃកថាខណ្ឌទី២នៃមាត្រា៣២។

មាត្រា៦១ .. អំពើល្មើសលើការបំពានលើការចេញលិខិតបញ្ជាក់យថាភូតភាព

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី១(មួយ)ខែទៅ១(មួយ)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី១០០ ០០០ (មួយសែន)រៀលទៅ២ ០០០ ០០០(ពីរលាន)រៀល ចំពោះបុគ្គលទាំងឡាយដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃកថាខណ្ឌទី៣នៃមាត្រា៤១។

មាត្រា៦២ .. អំពើល្មើសលើការបំពានលើកូដនីយកម្ម

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី១(មួយ)ឆ្នាំទៅ៣(បី)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី២ ០០០ ០០០ (ពីរលាន)រៀលទៅ៦ ០០០ ០០០(ប្រាំមួយលាន)រៀល ចំពោះបុគ្គលទាំងឡាយដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃមាត្រា៤៣។

មាត្រា៦៣ .. អំពើល្មើសលើការធ្វើប្រតិបត្តិការទូទាត់តាមប្រព័ន្ធអេឡិចត្រូនិក

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី១(មួយ)ឆ្នាំទៅ៥(ប្រាំ)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី១ ០០០ ០០០ (មួយលាន)រៀលទៅ១០ ០០០ ០០០(ដប់លាន)រៀល ចំពោះបុគ្គលទាំងឡាយដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃកថាខណ្ឌទី១នៃមាត្រា៥៦។

មាត្រា៦៤ .. អំពើល្មើសលើការក្លែងបន្លំឧបករណ៍ទូទាត់សងប្រាក់ជាអេឡិចត្រូនិក

ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី១(មួយ)ឆ្នាំទៅ៣(បី)ឆ្នាំនិងត្រូវពិន័យជាប្រាក់ពី២ ០០០ ០០០ (ពីរលាន)រៀលទៅ៦ ០០០ ០០០(ប្រាំមួយលាន)រៀល ចំពោះបុគ្គលទាំងឡាយដែលប្រព្រឹត្តអំពើផ្ទុយនឹងបញ្ញត្តិនៃកថាខណ្ឌទី៥នៃមាត្រា៥៧។

មាត្រា៦៥ .. ការទទួលខុសត្រូវព្រហ្មទណ្ឌរបស់នីតិបុគ្គល

១. នីតិបុគ្គលអាចត្រូវប្រកាសថាត្រូវទទួលខុសត្រូវព្រហ្មទណ្ឌតាមលក្ខខណ្ឌដែលមានចែងក្នុងមាត្រា៤២(ការទទួលខុសត្រូវព្រហ្មទណ្ឌរបស់នីតិបុគ្គល)នៃក្រមព្រហ្មទណ្ឌ ចំពោះបទល្មើសដែលមានចែងក្នុងមាត្រា៥៣ដល់មាត្រា៥៥ កថាខណ្ឌទី២នៃមាត្រា៥៦និងមាត្រា៥៩ដល់មាត្រា៦៤នៃច្បាប់នេះ។

២. នីតិបុគ្គលត្រូវពិន័យជាប្រាក់ទ្វេដង ព្រមទាំងទោសបន្ថែមណាមួយឬច្រើន ដូចតទៅនេះ៖

ក. ការរំលាយតាមបែបបទកំណត់ដោយមាត្រា១៧០(ការរំលាយនិងការជម្រះបញ្ជីនៃនីតិបុគ្គល)នៃក្រមព្រហ្មទណ្ឌ។

ខ. ការដាក់ឱ្យស្ថិតនៅក្រោមការពិនិត្យតាមដានរបស់តុលាការ តាមបែបបទកំណត់ដោយមាត្រា១៧១(ការដាក់ឱ្យស្ថិតនៅក្រោមការត្រួតពិនិត្យតាមដានរបស់តុលាការ)នៃក្រមព្រហ្មទណ្ឌ។

គ. ការហាមឃាត់ចំពោះការធ្វើសកម្មភាពមួយឬច្រើន តាមបែបបទកំណត់ដោយមាត្រា១៧២ (ការហាមឃាត់ចំពោះការធ្វើសកម្មភាព)នៃក្រមព្រហ្មទណ្ឌ។

ឃ. ការបិទផ្សាយសេចក្តីសម្រេចផ្តន្ទាទោស តាមបែបបទកំណត់ដោយមាត្រា១៨០ (ការបិទផ្សាយសេចក្តីសម្រេច)នៃក្រមព្រហ្មទណ្ឌ។

ង. ការផ្សាយសេចក្តីសម្រេចផ្តន្ទាទោសនៅក្នុងសារព័ត៌មានសរសេរ សារព័ត៌មានអេឡិចត្រូនិក ឬការផ្សាយតាមគ្រប់មធ្យោបាយទូរគមនាគមន៍សោតទស្សន៍ តាមបែបបទកំណត់ដោយមាត្រា១៨១(ការផ្សាយសេចក្តីសម្រេចតាមមធ្យោបាយទូរគមនាគមន៍សោតទស្សន៍ ជាអាទិ៍)នៃក្រមព្រហ្មទណ្ឌ។

ជំពូកទី១២
អវសានប្បញ្ញត្តិ

មាត្រា៦៦ .- ការទុកជានិរាករណ៍

បទប្បញ្ញត្តិទាំងឡាយណាដែលផ្ទុយនឹងច្បាប់នេះ ត្រូវចាត់ទុកជានិរាករណ៍។

មាត្រា៦៧ .- ការអនុវត្តច្បាប់នេះ

ក្រោយពីចូលជាធរមាន ច្បាប់នេះត្រូវផ្សព្វផ្សាយរយៈពេល៦(ប្រាំមួយ)ខែ ទើបអនុវត្ត។

ថ្ងៃសៅរ៍ ៦កើត ខែកត្តិក ឆ្នាំកុរ ឯកស័ក ព.ស. ២៥៦៣
ធ្វើនៅព្រះបរមរាជវាំង ថ្ងៃទី ១២ ខែ តុលា ឆ្នាំ២០១៩

ត.រស. ១៩១១.១៦៤

នរោត្តម សីហមុនី

នរោត្តម សីហមុនី

បានយកសេចក្តីក្រាបបង្គំទូលថ្វាយព្រះមហាក្សត្រ
សូមទ្បាយព្រះហស្តលេខា
នាយករដ្ឋមន្ត្រី

សម្តេចអគ្គមហាសេនាបតីតេជោ ហ៊ុន សែន

បានចម្លងត្រឹមត្រូវតាមច្បាប់ដើម
ឧបនាយករដ្ឋមន្ត្រីប្រចាំការ
រដ្ឋមន្ត្រីទទួលបន្ទុកនីស្តីការគណៈរដ្ឋមន្ត្រី

កិត្តិនីតិកោសលបណ្ឌិត ចិន ឈិន

បានយកសេចក្តីគោរពជម្រាបជូន
សម្តេចអគ្គមហាសេនាបតីតេជោនាយករដ្ឋមន្ត្រី
រដ្ឋមន្ត្រីក្រសួងពាណិជ្ជកម្ម

ប៉ាន សូរស័ក្តិ

ឧបសម្ព័ន្ធ
និយមន័យ

វាក្យសព្ទសំខាន់ៗដែលប្រើនៅក្នុងច្បាប់នេះត្រូវបានកំណត់និយមន័យដូចតទៅ៖

១. **ការចូលប្រើប្រាស់/អាក់សេស(Access)** សំដៅដល់ការចូលទៅប្រើកម្មវិធីកុំព្យូទ័រ ប្រព័ន្ធកុំព្យូទ័រ ប្រព័ន្ធឬបណ្តាញអេឡិចត្រូនិក ដើម្បីទាក់ទង បញ្ជូន រក្សាទុក ឬទាញយកនូវទិន្នន័យ ព័ត៌មានឬឯកសារផ្សេងៗទៀតក្នុងប្រព័ន្ធអេឡិចត្រូនិកតាមគ្រប់មធ្យោបាយ។

២. **អ្នកទទួល(Addressee)** សំដៅដល់បុគ្គលដែលទទួលទំនាក់ទំនងអេឡិចត្រូនិក ស្របតាមឆន្ទៈរបស់អ្នកផ្ញើ លើកលែងតែអន្តរការីក្នុងការប្រាស្រ័យទាក់ទងតាមប្រព័ន្ធអេឡិចត្រូនិក។

៣. **ប្រព័ន្ធស្វ័យប្រវត្តិ(Automated System)** សំដៅដល់កម្មវិធីកុំព្យូទ័រ ប្រព័ន្ធកុំព្យូទ័រ ប្រព័ន្ធ ឬបណ្តាញអេឡិចត្រូនិក ឬមធ្យោបាយអេឡិចត្រូនិកផ្សេងទៀតដែលត្រូវបានប្រើប្រាស់សម្រាប់ជូនដំណឹងឬឆ្លើយតបដោយស្វ័យប្រវត្តិដោយគ្មានអន្តរាគមន៍ពីរូបវន្តបុគ្គលណាមួយ។

៤. **បណ្ណ/កាតទូទាត់(Card)** សំដៅដល់បណ្ណ/កាតធនាគារ បណ្ណឥណទាន/ឥណពន្ធ ស្មាតកាត (Smart Card) ឬបណ្ណ/កាតទូទាត់ ទោះបីក្នុងទម្រង់អេឡិចត្រូនិកដែលផ្ទុកតម្លៃ ហើយមានមុខងារសម្រាប់ទូទាត់។

៥. **កម្មវិធីចម្លងមេរោគ(Contaminant)** សំដៅដល់កម្មវិធីអេឡិចត្រូនិកដែលត្រូវបានបង្កើតឡើងដើម្បី៖

(ក) កែប្រែ បំផ្លាញ កត់ត្រា បញ្ជូនទិន្នន័យឬកម្មវិធីនៅក្នុងប្រព័ន្ធអេឡិចត្រូនិក ឬ

(ខ) ជ្រៀតជ្រែកតាមគ្រប់មធ្យោបាយនូវដំណើរការប្រក្រតីរបស់ប្រព័ន្ធឬបណ្តាញអេឡិចត្រូនិក។

៦. **ម្ចាស់បណ្ណ/កាតទូទាត់(Cardholder)** សំដៅដល់បុគ្គលដែលមានឈ្មោះចារឹកនៅលើបណ្ណ/កាត និងជាបុគ្គលដែលទទួលប្រយោជន៍ពីបណ្ណ/កាតទូទាត់នោះ។

៧. **ទំនាក់ទំនង(Communication)** សំដៅដល់អំណះអំណាង សេចក្តីថ្លែងការណ៍ ការទាមទារ សេចក្តីជូនដំណឹង សំណូមពរ សំណើ ឬស្នើការ ដែលគូភាគីត្រូវធ្វើឬសម្រេចចិត្តធ្វើពាក់ព័ន្ធនឹងការបង្កើតឬការអនុវត្តកិច្ចសន្យា។

៨. **បណ្ណ/កាតទូទាត់ក្លែងក្លាយ(Counterfeit card)** សំដៅដល់បណ្ណ/កាតទូទាត់ទាំងឡាយណាដែលត្រូវបានបង្កើតឡើងដោយការបង្ហាញឬការពិពណ៌នាដែលត្រូវបានប្រឌិតឡើង កែប្រែក្លែងបន្លំ ឬបណ្ណ/កាតទូទាត់ដែលមានសមាសធាតុណាមួយនៃបណ្ណ/កាតទូទាត់នោះមានលក្ខណៈខុសច្បាប់។



៩. **ទិន្នន័យ(Data)** សំដៅដល់បណ្តុំលេខ អក្សរ និមិត្តសញ្ញា សារ រូបភាព សំឡេង វីដេអូ ព័ត៌មាន ឬកម្មវិធីអេឡិចត្រូនិក ដែលត្រូវបានរៀបចំក្នុងទម្រង់សមស្របសម្រាប់ប្រើប្រាស់ក្នុងមូលដ្ឋានទិន្នន័យឬប្រព័ន្ធអេឡិចត្រូនិក។

១០. អេឡិចត្រូនិក(Electronic) សំដៅដល់អ្វីដែលពាក់ព័ន្ធនឹងបច្ចេកវិទ្យាដែលមានចរន្តអគ្គិសនី ឌីជីថល ម៉ាញេទិច អុបទិក ជីវមាត្រ អេឡិចត្រូគីមី វ៉ាយអឺឡេស (wireless) អេឡិចត្រូម៉ាញេទិក ឬបច្ចេកវិទ្យាដែលមានមុខងារប្រហាក់ប្រហែលផ្សេងទៀត។

១១. អាសយដ្ឋានអេឡិចត្រូនិក(Electronic Address) សំដៅដល់លេខឬអាសយដ្ឋានប្រើប្រាស់សម្រាប់ផ្ញើឬទទួលការជូនដំណឹង ឯកសារ ព័ត៌មាន ឬទំនាក់ទំនងតាមមធ្យោបាយអេឡិចត្រូនិក។

១២. យថាភូតភាព(Authenticity) សំដៅដល់ភាពត្រឹមត្រូវនិងអាចជឿទុកចិត្តបាននៃទំនាក់ទំនងអេឡិចត្រូនិក។

១៣. ពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក(Electronic Commerce) សំដៅដល់សកម្មភាពទិញ លក់ ជួល ផ្លាស់ប្តូរទំនិញឬសេវា ដោយរាប់បញ្ចូលទាំងសកម្មភាពពាណិជ្ជកម្មនិងរដ្ឋប្បវេណី ព្រមទាំងសកម្មភាពនិងប្រតិបត្តិការនានារបស់រដ្ឋ តាមប្រព័ន្ធអេឡិចត្រូនិក។

១៤. ឧបករណ៍ទូទាត់អេឡិចត្រូនិក(Electronic Payment Instrument) សំដៅដល់បណ្ណ/កាតទូទាត់ ឬឧបករណ៍ទូទាត់ទាំងឡាយណាដែលមានទម្រង់ជាអេឡិចត្រូនិក ហើយមានមុខងារសម្រាប់ទូទាត់សងប្រាក់។

១៥. ទំនាក់ទំនងអេឡិចត្រូនិក(Electronic Communication) សំដៅដល់ព័ត៌មានដែលត្រូវបានទាក់ទង ដំណើរការ កត់ត្រាទុក បង្ហាញឡើង បង្កើតឡើង រក្សាទុក ទទួលបាន ឬបញ្ជូនតាមមធ្យោបាយអេឡិចត្រូនិក។

១៦. ឧបករណ៍អេឡិចត្រូនិក(Electronic device) សំដៅដល់ឧបករណ៍ទាំងឡាយណាដែលបង្កើតឡើងដើម្បីគ្រង់គ្រង បញ្ជា និងប្រតិបត្តិការតាមប្រព័ន្ធអេឡិចត្រូនិក។

១៧. ភស្តុតាងអេឡិចត្រូនិក(Electronic evidence) សំដៅដល់ព័ត៌មាន ទិន្នន័យ ឬឯកសារនានាដែលបានបង្កើតឡើង រក្សាទុក ផ្ញើចេញ ឬទទួលក្នុងទម្រង់ឬទំនាក់ទំនងអេឡិចត្រូនិក សម្រាប់ជាសំអាងទាក់ទងនឹងអង្គហេតុណាមួយក្នុងដំណើរការនីតិវិធីតាមផ្លូវច្បាប់ ហើយព័ត៌មាន ទិន្នន័យ ឬឯកសារនោះមានយថាភូតភាពស្របតាមច្បាប់ស្តីពីពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក។

១៨. ទម្រង់អេឡិចត្រូនិក(Electronic form) សំដៅដល់ទម្រង់នៃព័ត៌មាន ទិន្នន័យ ឬឯកសារដែលបង្កើត បញ្ជូន ទទួលបាន ឬរក្សាទុកក្នុងប្រព័ន្ធអេឡិចត្រូនិក។

១៩. ការផ្ទេរប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិក(Electronic fund transfer) សំដៅដល់ប្រតិបត្តិការទាំងឡាយណាដែលធ្វើឡើងតាមរយៈបញ្ជារផ្ទេរប្រាក់អេឡិចត្រូនិក ឬតាមឧបករណ៍អេឡិចត្រូនិកចល័ត ឬតាមឧបករណ៍អេឡិចត្រូនិកដែលមានមុខងារស្រដៀងគ្នា ដើម្បីបញ្ជាឱ្យគ្រឹះស្ថានធនាគារ និងមិរញ្ញវត្ថុធ្វើការចុះឥណពន្ធឬឥណទានក្នុងគណនី។

២០. កំណត់ត្រាអេឡិចត្រូនិក(Electronic record) សំដៅដល់កំណត់ត្រាដែលត្រូវបានបង្កើតឡើង ទាក់ទង ទទួល រក្សាទុក ឬដំណើរការក្នុងប្រព័ន្ធអេឡិចត្រូនិក ឬសម្រាប់បញ្ជូនពីប្រព័ន្ធអេឡិចត្រូនិកមួយទៅប្រព័ន្ធអេឡិចត្រូនិកមួយទៀត។

២១. បុគ្គលផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក(Electronic-Commerce service provider) សំដៅដល់បុគ្គលដែលប្រើប្រាស់មធ្យោបាយអេឡិចត្រូនិកដើម្បីផ្តត់ផ្គង់ទំនិញនិង/ឬសេវា លើកលែងគ្រឹះស្ថានធានារ៉ាប់រង។

២២. ហត្ថលេខាអេឡិចត្រូនិក(Electronic Signature) សំដៅដល់រាល់ហត្ថលេខាដែលត្រូវបានបង្កើតឡើងតាមមធ្យោបាយអេឡិចត្រូនិកសម្រាប់ប្រើប្រាស់កំណត់អត្តសញ្ញាណរបស់ហត្ថលេខីដែលរួមមាន ហត្ថលេខាឌីជីថល ហត្ថលេខាជីវមាត្រ និងហត្ថលេខាដទៃទៀត។

២៣. ប្រព័ន្ធអេឡិចត្រូនិក(Electronic system) សំដៅដល់ឧបករណ៍អេឡិចត្រូនិកឬបណ្តុំឧបករណ៍តភ្ជាប់គ្នាឬទាក់ទងគ្នា តាមរយៈកម្មវិធីអេឡិចត្រូនិក ដែលអាចធ្វើឱ្យដំណើរការដោស្វ័យប្រវត្តិនៃទិន្នន័យ ព័ត៌មាន ឬឯកសារ រួមបញ្ចូលទាំងឧបករណ៍អេឡិចត្រូនិកសម្រាប់រក្សាទុកទិន្នន័យ ព័ត៌មាន ឬឯកសារនោះ។

២៤. ប្រព័ន្ធព័ត៌មាន(Information system) សំដៅដល់ប្រព័ន្ធសម្រាប់បង្កើត ផ្ញើ ទទួលរក្សាទុក ឬដំណើរការកំណត់ត្រាអេឡិចត្រូនិក។

២៥. អន្តរការី(Intermediary) សំដៅដល់បុគ្គលដែលផ្តល់សេវា ផ្ញើ ទទួល បញ្ជូន ឬរក្សាទុកជាបណ្តោះអាសន្នឬជាអចិន្ត្រៃយ៍នូវទំនាក់ទំនងអេឡិចត្រូនិកនោះ ឬផ្តល់សេវាផ្សេងទៀតដែលពាក់ព័ន្ធនឹងទំនាក់ទំនងអេឡិចត្រូនិក រួមបញ្ចូលនូវបុគ្គលដូចខាងក្រោម៖

១. បុគ្គលដែលតំណាងឱ្យអ្នកផ្ញើ អ្នកទទួល អ្នកបញ្ជូន ឬអ្នករក្សាទុក
២. បុគ្គលផ្តល់សេវាទូរគមនាគមន៍
៣. បុគ្គលផ្តល់សេវាបណ្តាញនានា
៤. បុគ្គលផ្តល់សេវាអ៊ុនធឺណិត
៥. បុគ្គលផ្តល់មធ្យោបាយស្វែងរកទិន្នន័យណាមួយតាមប្រព័ន្ធអេឡិចត្រូនិក
៦. បុគ្គលផ្តល់សេវាទូទាត់តាមអនឡាញ
៧. បុគ្គលផ្តល់សេវាដេញថ្លៃតាមអនឡាញ
៨. បុគ្គលផ្តល់សេវាទីផ្សារអនឡាញនិងសេវាពាណិជ្ជកម្មតាមបណ្តាញអ៊ុនធឺណិត។

២៦. បុគ្គលចេញបណ្ណ/កាតទូទាត់(Issuer) សំដៅដល់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុឬបុគ្គលណាម្នាក់ដែលបានចេញបណ្ណ/កាតទូទាត់ ដែលបានទទួលការអនុញ្ញាត។

២៧. កូដព្យាបាទ(Malicious code) សំដៅដល់កម្មវិធីឬតួនាទីលាក់មុខនៃកម្មវិធីដែលចម្លងមេរោគដល់ទិន្នន័យ ព័ត៌មាន ឬឯកសារ ដោយមានឬគ្មានបន្សល់ទុកស្លាកស្នាមសម្គាល់នៃមេរោគនោះក្នុងឯកសារអេឡិចត្រូនិកដែលបានឆ្លងមេរោគ ហើយមេរោគនោះអាចចម្លងបន្តក្នុងប្រព័ន្ធដោយឯកឯងឬដោយមានអន្តរាគមន៍ពីមនុស្ស។

២៨. អ្នកផ្ញើ(Originator) សំដៅដល់ភាគីឬអ្នកតំណាងដែលបានផ្តើមប្រតិបត្តិការបង្កើត រក្សាទុក ឬបញ្ជូនទិន្នន័យតាមមធ្យោបាយអេឡិចត្រូនិក ដោយមិនរាប់បញ្ចូលអន្តរការី។

២៩. បុគ្គលផ្តល់សេវាទូទាត់(Payment Service Provider) សំដៅដល់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ ឬបុគ្គលដទៃទៀតដែលបានទទួលការអនុញ្ញាតឬអាជ្ញាបណ្ណពីធនាគារជាតិនៃកម្ពុជា ឱ្យធ្វើប្រតិបត្តិការប្រព័ន្ធទូទាត់ ចេញផ្សាយឧបករណ៍ទូទាត់អេឡិចត្រូនិកឬមធ្យោបាយទូទាត់ ជាអេឡិចត្រូនិក ឬធ្វើប្រតិបត្តិការណាដែលត្រូវបានចាត់ទុកថាជាការផ្តល់ការទូទាត់សងប្រាក់ ជាអេឡិចត្រូនិកដល់សាធារណជន។

៣០. ទីតាំងអាជីវកម្ម(Place of business) សំដៅដល់៖

ក. ទីតាំងដែលអ្នកផ្ញើឬអ្នកទទួលបានចង្អុលបង្ហាញ លើកលែងតែភាគីណាមួយបានបង្ហាញថាអ្នកអះអាងនោះ ពុំមានទីតាំងអាជីវកម្មនៅទីនោះឡើយ។

ខ. ប្រសិនបើភាគីណាមួយមិនបានចង្អុលបង្ហាញទីកន្លែងអាជីវកម្មជាក់លាក់ណាមួយ ហើយភាគីនោះមានទីតាំងអាជីវកម្មច្រើនជាងមួយកន្លែង ទីតាំងអាជីវកម្មត្រូវកំណត់ថាជាទីកន្លែងដែលមានទំនាក់ទំនងជិតស្និទ្ធជាងគេទៅនឹងកិច្ចសន្យាដែលពាក់ព័ន្ធ ដោយត្រូវពិចារណាផងដែរអំពីកាល:ទេស:ដែលបានដឹងឬពិនិត្យដោយភាគីនៅពេលណាមួយមុនឬក្នុងពេលចុះកិច្ចសន្យា។

គ. សម្រាប់រូបវន្តបុគ្គលដែលពុំមានទីតាំងអាជីវកម្មទេនោះ ទីតាំងអាជីវកម្មសំដៅដល់ទីលំនៅអចិន្ត្រៃយ៍របស់បុគ្គលនោះ។

មិនត្រូវចាត់ទុកថាជាទីតាំងអាជីវកម្មរបស់ភាគីដោយគ្រាន់តែជា៖

- ទីតាំងដែលសម្ភារ:ឬឧបករណ៍បច្ចេកវិទ្យានៃប្រព័ន្ធព័ត៌មានត្រូវបានប្រើ
- អាសយដ្ឋានអេឡិចត្រូនិកឬឈ្មោះដែនកម្មសិទ្ធិ(Domain Name) ដែលភ្ជាប់ជាមួយនឹងទីតាំងរបស់ភាគី។

៣១. កំណត់ត្រា(Record) សំដៅដល់ព័ត៌មាន ទិន្នន័យ ឬឯកសារដែលត្រូវបានកត់ត្រាចូលរក្សាទុក ឬបញ្ចូលទៅក្នុងទម្រង់រូបី ឬដែលត្រូវបានរក្សាទុកក្នុងទម្រង់អេឡិចត្រូនិក ជាត្រដាសស្នាម ឬទម្រង់ប្រភេទផ្សេងទៀត ហើយដែលអាចទាញយកកំណត់ត្រានោះវិញបានក្នុងទម្រង់ជាក់ដែលអាចមើលបាន។

៣២. បុគ្គលផ្តល់សេវា(service provider) សំដៅដល់

(ក) បុគ្គលដែលផ្តល់សេវាព័ត៌មាននិងសេវាទំនាក់ទំនង រួមមាន ការធ្វើ ការទទួល ការរក្សាទុក ឬដំណើរការទំនាក់ទំនងអេឡិចត្រូនិក ឬការផ្តល់សេវាតាមប្រព័ន្ធអេឡិចត្រូនិកផ្សេងទៀត។

(ខ) បុគ្គលដែលជាម្ចាស់ បុគ្គលកាន់កាប់ បុគ្គលដំណើរការ បុគ្គលគ្រប់គ្រង ឬបុគ្គលត្រួតពិនិត្យបណ្តាញស្ទិចសាធារណៈ(Public Switched Network) ឬបុគ្គលដែលផ្តល់សេវាទូរគមនាគមន៍។ ឬ

(គ) បុគ្គលផ្សេងទៀតដែលប្រតិបត្តិឬរក្សាទុកទិន្នន័យបម្រើឱ្យសេវាទំនាក់ទំនងអេឡិចត្រូនិកនោះ ឬអ្នកប្រើប្រាស់សេវា។

៣៣. បុគ្គលផ្តល់នីតិវិធីសុវត្ថិភាព(Security procedure provider) សំដៅដល់បុគ្គលបង្កើត ឬផ្តល់នីតិវិធីសុវត្ថិភាព។

៣៤. នីតិវិធីសុវត្ថិភាព(Security Procedure) សំដៅដល់នីតិវិធីដែលកំណត់ដោយច្បាប់ ឬកិច្ចសន្យា ឬការសម្រេចដោយភាគីណាមួយ ហើយដែលត្រូវបានប្រើក្នុងគោលបំណង៖

(ក) ផ្ទៀងផ្ទាត់ថាហត្ថលេខា ទំនាក់ទំនង ឬប្រតិបត្តិការក្នុងប្រព័ន្ធអេឡិចត្រូនិក ពិតជារបស់បុគ្គលនោះ។

(ខ) រកឱ្យឃើញកំហុសឆ្គងឬការកែប្រែនៅក្នុងទំនាក់ទំនងឬក្នុងកន្លែងរក្សាទុកកំណត់ត្រាអេឡិចត្រូនិក ចាប់តាំងពីពេលជាក់ណាមួយ។

នីតិវិធីសុវត្ថិភាពខាងលើអាចតម្រូវឱ្យប្រើរូបមន្តអាល់ហ្គោរីត(algorithms)ឬកូដ ពាក្យឬលេខសម្រាប់ សម្គាល់អត្តសញ្ញាណ កូដនីយកម្ម សំណូរសម្ងាត់ ឬការទទួលស្គាល់នីតិវិធីណាមួយ ឬក៏ឧបករណ៍សុវត្ថិភាពស្រដៀងគ្នាផ្សេងទៀត។

៣៥. ព័ត៌មានឬកំណត់ត្រាជាលាយលក្ខណ៍អក្សរ(writing/written) សំដៅដល់ព័ត៌មានឬកំណត់ត្រាផ្សេងៗទៀតដែលត្រូវបានសរសេរ ចារឹក ឬបោះពុម្ពនៅលើក្រដាសឬសម្ភារៈផ្សេងៗទៀត។

៣៦. អ៊ីមែលឬសារអេឡិចត្រូនិក(E-mail or Electronic Message) សំដៅដល់សារឬព័ត៌មានដែលត្រូវបានបង្កើតឡើង ឬបញ្ជូន ឬទទួលបានពីប្រព័ន្ធអេឡិចត្រូនិក រួមទាំងឯកសារភ្ជាប់ក្នុងអត្ថបទ រូបភាព សំឡេង វីដេអូ និងកំណត់ត្រាអេឡិចត្រូនិកណាមួយផ្សេងទៀតដែលអាចបញ្ជូនជាមួយសារបាន។

៣៧. សន្តតិកម្ម(Will) សំដៅដល់ការផ្ទេរនូវសិទ្ធិនិងករណីកិច្ចរបស់មតកជនទៅឱ្យសន្តតិជនម្ចាក់ឬច្រើននាក់តាមឆន្ទៈឬតាមច្បាប់។

៣៨. ស្នើការ(Acceptance) សំដៅដល់ការសំដែងឆន្ទៈដែលបុគ្គលម្នាក់បានបញ្ចេញការយល់ព្រមរបស់ខ្លួនចំពោះសំណើដែលបុគ្គលដទៃបានស្នើមកខ្លួនដើម្បីបង្កើតកិច្ចសន្យា។



KINGDOM OF CAMBODIA

NATION RELIGION KING

LAW

ON

ELECTRONIC COMMERCE

ROYAL KRAM

NS/RKM/1119/017

WE

Preah Karuna Preah Bat Sâmdach Preah Bâromneath Norodom Sihamoni Saman Bhumichat Sasana Rakkhata Khattiya Khmeraratrat Putthintra Mohaksat Khemareacheana Samuhobhas Kampuchea Ekareacharath Bureanasanti Subheamagala Sirivibunla Khmera Sri Bireat

Preah Chao Krung Kampuchea Dhibodi

- Having seen the Constitution of the Kingdom of Cambodia;
- Having seen Royal Decree No. NS/ RKT/0918/925 dated 06 September 2018 on the appointment of the Royal Government of Cambodia
- Having seen Royal Kram No. NS/ RKT/0618/012 dated on 28 June 2018 promulgating the Law on the Organization and Functioning of the Council of Ministers;
- Having seen Royal Kram No. NS/ RKT/0196/16 promulgating the Law on the Establishment of the Ministry of Commerce;
- Having seen the Request of Samdech Akka Moha Sena Padei Techo Hun Sen, Prime Minister of the Kingdom of Cambodia

PROMULGATE

Law on Electronic Commerce which was enacted by the National Assembly on 8 October 2019 at its third plenary session off the sixth legislature, and entirely reviewed and approved by the Senate on its form and legal concept on 18 October 2019 at its extraordinary session of the fourth legislature, with the following content:

Chapter 1

General Provisions

Article 1: Purposes

The purposes of this law are as follows:

1. To govern electronic commerce in the Kingdom of Cambodia and with the international;
2. To create legal certainty in the civil and commercial transactions by electronic system;
3. To give confidence to the public in the usage of electronic communication.

Article 2: Goals

The goals of this law are as follows:

1. To determine the authenticity, perfection and reliability of an electronic form;
2. To promote the development of legal and business framework in order to conduct safe electronic commerce;
3. To prevent and enforce against acts which are harmful to data and information systems;
4. To eliminate obstacles which hinder electronic commerce and which created by the uncertainty of requirements of written documents and signature;
5. To facilitate electronic filing of documents with public institutions and promote an efficient delivery of services of public institutions through the use of reliable electronic records; and
6. To establish rules, regulations and standards regarding the authenticity and perfection of electronic records.

Article 3: Scope

This law shall apply to all activities, documents and civil and commercial transactions that are made via electronic system except for the activities, documents and transactions relating to:

1. Formation or enforcement of Power of Attorney;
2. Formation or execution of a testament, codicil or other matters relating to succession;
3. Any contract for sale, transfer or disposition of rights to immovable property or any interests in such property;
4. Transfer of immovable property or any interests relating to the immovable property; and
5. Any other exceptions as provided for by Sub-Decree.

Article 4: Definitions

All important terms use in this law are defined in the glossary found in the annex of this law.

Chapter 2

Validity of Electronic Communications

Article 5: Legal recognition of electronic communications

No one may refuse to recognize the validity, legal effect, admissibility or enforceability of an electronic communication solely on grounds that it is formed in electronic form or is in an electronic communication.

Article 6: In writing requirement

1. Where any provisions is required to provide an information in writing or recorded in writing, this requirement shall be deemed fulfilled if the information is made in an electronic form and can be accessed and retrieved for subsequent use.
2. Where the requirement in the provision of the paragraph (1) above applies, a legal requirement demanding any person to provide at the same time multiple copies of any information or matters to another person, the person subjected to such requirement may fulfil this requirement by only providing a single copy in electronic form.

Article 7: Signature requirements

1. Where any provision requires a signature of a person, such requirement shall be deemed fulfilled by an electronic signature if the electronic signature was created by means which:
    a. Can determine the identity of a person and indicate the approval of the person on information or record contained in the electronic communications.
    b. Can be trusted in accordance with the characteristics, the purpose and the circumstance for which the electronic communication was made or communicated.
2. Notwithstanding any provision that states a requirement for a signature or only states consequence for the absence of a signature, the provision of the paragraph (1) above shall also apply.

Article 8: Requirements to retain information in original form

A legal requirement to retain information that was not made electronic form may be fulfilled by the retention of such information in electronic form if:

1. Such electronic form is a reliable means to determine the completeness of the information; and
2. Such information is easily retrievable for subsequent use.

Article 9: Prescribed form

Where any provision requires that information be created in any prescribed form, such requirement shall be substituted by providing information in electronic form if the electronic form fulfils the following conditions:

1. Contains the same information or substantially the same information as prescribed form;
2. Is accessible, intelligible, and retrievable for subsequent use; and
3. Can be retained by the person who received the information.

Article 10: Record retention requirements

1. Where any provision requires that any specific document, record or information, such requirement shall be deemed fulfilled if the retention fulfils all conditions as follows:
   a. Information contained in such electronic communication is accessible and retrievable for subsequent use;
   b. Electronic communication is retained in original format in which it was created, sent or received, or in a format that can identify the accuracy of the information; and
   c. Such information is kept to allow any person can identify the origin and destination of such electronic communication, date and time when such electronic communication was sent or received.
2. Obligation to retain documents, records or information in accordance with paragraph (1) does not include any information for the sole purpose to send or receive messages.

Article 11: Evidentiary requirements

No provisions in relation to the application of rules of evidence may object to the admissibility of electronic communication as evidence only on the ground that:

1. The evidence is an electronic communication; or
2. The evidence is not in original form.

Article 12: Formation and validity of contracts

1. Offer, acceptance, and contract may be done in electronic means.
2. A contract in electronic form mentioned in the provision of the paragraph 1 above has validity, legal effect, and enforceability when the offer and acceptance coincide.

Article 13: Effect between parties

The originator and addressee of electronic communication shall not refuse the legal effect, validity or enforceability of theirs intent or declaration.

Article 14: Separate implementation by agreement of parties

1. By agreement, parties that participate in the generation, sending, receiving, storage or processing of electronic communication may disregard the provisions as stated in Chapter 2 of this law, except otherwise determined.
2. Notwithstanding the provisions as stated in Chapter 2, parties to the contract or transactions may:
   a. Refrain from using any electronic records, electronic communication or electronic

signature in the contract or any transaction as agreed between the parties; or

b. Set additional requirements in relation to form or authenticity of the contract or the transaction as agreed between the parties.

Chapter 3

Electronic Communications Process

Article 15: Time and place of dispatch and receipt of information in electronic communications

1. Information in an electronic communication is deemed dispatched when:
   a. The information leaves the information system that is under the control of the originator or of the party who sent it on behalf of the originator; or
   b. In case that the information is sent but it has not left the information system that is under the control of the originator or of the party who sent it on behalf of the originator, the information is deemed that it is dispatched when such information is received at any time.
2. Information in an electronic communication is deemed to be dispatched from the place of business of the originator, no matter where it is dispatched.
3. The time of receipt of an information is the time when the information becomes capable of being retrieved by the addressee at the electronic address designated by the addressee. The information is deemed to be received at the place where the addressee has its place of business.
4. If a specific electronic address has not been provided by the addressee, the time of receipt of an information is the time when the addressee becomes aware of the dispatch and retrievability at any electronic address and the information is deemed to be received at the place of business of the recipient.
5. If the electronic address is provided by the addressee, the information in the electronic communication is deemed to be received when it reaches the electronic address of the addressee, and is deemed to be received at the place where the addressee has its place of business.

Article 16: Offer for forming a contract

Any proposal to enter into a contract through an electronic communication which is not addressed to any other specific person is considered as an invitation to make an offer for forming a contract only. The proposal will be considered as an offer for creating a contract if the proposal clearly indicates the intention of the party that it shall be bound when there is an acceptance from the other party.

Article 17: Use of automated system for contract formation

A contract formed by the interaction of an automated system of a person with any natural person, or with the automated systems of another person, shall not be denied validity, legal effect, or enforceability of the contract on the ground that no natural person directly reviewed or intervened in the automated system or in forming the contract.

Article 18: Error of information input in electronic communication

Where a natural person makes an information input error in an electronic communication with the automated system of another party, and the automated system does not provide the person with an opportunity to correct the input error, that person, or the party on whose behalf that person was acting, has the right to make correction or withdraw the input error in case:

1. The person notifies the other party of the error as soon as possible after having learned of the error, and indicates that he had made an error in the electronic communication; and
2. The person has not benefitted in any way from the error, prior to notification to the other party, and has not caused any damages of interest to the other party or any third party.

The provision as stated in this Article shall not be applicable to the securities sector.

Chapter 4

Secure Electronic Records and Electronic Signatures

Article 19: Secure electronic record

An electronic record shall be considered as a secure electronic record, only if it is properly applied in accordance with the secure procedure which ensures that the electronic record has not been altered commencing from any specific point in time to the time of verification.

Article 20: Secure electronic signature

1. An electronic signature is secure only if it complies with the conditions below:
    a. Can be uniquely linked to only one signatory;
    b. Is capable of identifying the signatory;
    c. Is created by using means that is under the management of signatory;
    d. Confirm the date and time of the signature; and
    e. Confirm the original status of messages or the electronic record which is linked the signature.
2. The provision of the paragraph (1) above shall not limit the ability of any person in an electronic communication to:
    a. Establish/set additional conditions in relation to the reliability of electronic signature; or
    b. Adduce evidence of non-reliability of an electronic signature.

Article 21: Presumptions relating to secure electronic records and signatures

1. Unless there is evidence to the contrary, in any proceedings involving a secure electronic record, the secure electronic record is presumed as an electronic record which has not been altered since a specific point in time.
2. Unless there is evidence to the contrary, in any proceedings involving a secure electronic signature, a secure electronic signature is presumed as follows:
    a. The electronic signature is the signature of the related person; and
    b. The electronic signature was affixed by a person with the intention of signing or

approving the electronic record.

3. In the absence of a secure electronic record or a secure electronic signature, nothing in any provisions of the Chapter 4 shall create any presumption relating to the authenticity or accuracy of the electronic record or electronic signature.

Article 22: Use of stolen identity

All person shall not use the identity, record, electronic signature, electronic address, secret code, or feature of other persons in bad faith or without permission in a commercial or non-commercial transaction via electronic system.

Article 23: Competent institution to manage the security procedures

1. The Ministry of Posts and Telecommunications shall be the competent institution to manage security procedures for the electronic record and the electronic signature.

2. The management of the secure procedures for the electronic record and the electronic signature shall be determined by regulations.

Chapter 5

Intermediaries and Electronic Commerce Service Providers

Article 24: Liability of intermediaries and electronic commerce service providers

1. An intermediary or an electronic commerce service provider shall not be subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of service provision of the intermediary and the electronic commerce service provider, if the intermediary and electronic commerce service provider was not the sender/originator of the record and in the case that:

   a. The intermediary or electronic commerce service provider has no actual knowledge that the information gives rise to civil or criminal liability;

   b. The intermediary or electronic commerce service provider is not aware of any facts or circumstances which they ought to know reasonably give rise to a likelihood of civil or criminal liability in respect of the information; or

   c. The intermediary or electronic commerce service provider becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known and take action in accordance with the procedure set out in Article 25 in relation to unlawful information and defamation in below.

2. An intermediary or electronic commerce service provider shall not be required to monitor any electronic record processed by the electronic system which is under his management whether its processing would constitute or give rise to an offence or give rise to civil liability unless otherwise provide/determine.

3. Provision of this article shall not apply to an intermediary or electronic commerce service

provider to be free from:

a. Any obligation established pursuant to a law or legal norms /regulations;

b. Any obligation to comply with an order or direction of a court or other competent authority; or

c. Any contractual obligation.

Article 25: Liability for information or event

1. If an intermediary or an electronic commerce service provider is aware that that the information in an electronic record gives rise to civil or criminal liability, the intermediary or the electronic commerce service provider shall immediately take measure as bellow:

   a. Remove the information from any information system within the intermediary's or the electronic commerce service provider's control and cease to provide services in respect of that information;

   b. Preserve the information as evidence and notify the Ministry of Posts and Telecommunications or relevant competent institutions about the facts and the identity of the suspected person.

2. In the event that an intermediary and an electronic commerce service provider is aware of any facts or circumstances which may lead to the civil or criminal liability, the intermediary and the electronic commerce service provider shall preserve the information evidence and notify the Ministry of Posts and Telecommunications or relevant competent ministries-institutions.

3. When it is acknowledged or notified in respect of any information of electronic record which may be subject to civil or criminal liability, the Ministry of Posts and Telecommunications and relevant competent ministries-institutions may give an instruction to the intermediary or electronic commerce service provider to perform any operation as follows:

   a. Remove the electronic record from the system which is under its control;

   b. Suspend or cease to provide services to the person; or

   c. Suspend or cease to provide services in respect of that electronic record.

4. An intermediary or an electronic commerce service provider is not liable on civil liability, whether in contract, outside of contract or in accordance with the law in respect of an activity performed in good faith as directed by the Ministry of Posts and Telecommunications or relevant competent ministries-institutions.

5. Any person who lodges a notification of unlawful activity with an intermediary or an electronic commerce service provider bout illegal activity knowing that the notification is false or misleading shall be subject to civil or criminal liability in respect of such offense.

Article 26: Provision of issuance of a permission letter or a license

1. An intermediary and an electronic commerce service provider shall request for a permission letter or a license from the Ministry of Commerce and the Ministry of Posts and Telecommunications.
2. The Ministry of Commerce provides a permission letter or a license including:
   a. A permission letter to operate an electronic business for a natural person.
   b. A license to allow the operation of electronic commerce service provision for a legal person.
3. The Ministry of Posts and Telecommunications shall provide an online service certificate.
4. The exception, the determination of type for license, the formalities, and the procedure of providing a permission or license shall be determined by a sub-decree.

Article 27: Professional code of conduct and regulations on intermediaries and electronic commerce service providers

1. An intermediary or an electronic commerce service provider shall comply with the approved professional code of conduct and regulations relating to electronic commerce determined by inter-ministerial Prakas between the Ministry of Commerce and the Ministry of Posts and Telecommunications.
2. The professional code of conduct referred to the provisions in paragraph (1) shall be determined and prepared by the Ministry of Commerce and the Ministry of Posts and Telecommunications in cooperation with the relevant competent ministries-institutions and related parties.

Article 28: Tax obligation, incentives and preferences

An intermediary and an electronic commerce service provider shall be subject to the common legislation of the applicable tax regime and shall receive the incentives and preferences in accordance with the laws and regulations in force.

Chapter 6

Consumer Protection

Article 29: Minimum information in electronic commerce

1. A person using electronic communications to sell goods or services to consumer shall provide accurate, clear and intelligible information and must have at least the following information:
   a. Name or legal name of the person, the registered business address and an electronic means for contact or a telephone number;
   b. Form of prompt, easy and effective communication between consumers and the

seller;

c. Terms, conditions and costs of goods or services associated with a commercial transaction, particularly the terms and conditions, and methods of payment, and details related to withdrawal or cancellation of the purchase order, termination, return and exchange of goods, and refund; and

d. Actual goods and services offered for sale.

2. The information provided in the provisions of the paragraph (1) above shall be sufficient to enable consumers to make a decision about the commercial transaction and to retain the information.

3. The provisions of this Article shall not apply to the securities and insurance sector.

Article 30: Unsolicited communications

Any person, whether or not having a place of business inside or outside the Kingdom of Cambodia, who sends unsolicited commercial communications to consumers based in or out of the Kingdom of Cambodia through an electronic media or through an intermediary or a telecommunication service provider shall provide the consumer with a clearly specified and easily activated option to reject the unsolicited commercial communication.

Article 31: Formation of Counterfeit Electronic System and Malicious Code

1. Any person shall not create an electronic system for the purpose of counterfeiting or causing a confusion in order to take advantage, or in the purpose of attracting to have a usage or an operation, and lead to have an injury/damage to the person who used it or to the third party.

2. Any person shall not create, provide, enable, distribute, or send the virus-code in the bad-faith purpose through electronic means in to electronic instrument or system of other persons.

Article 32: Data protection

1. Any person that holds personal information in electronic form shall use all means to ensure that the information is protected by such security safeguards as it is reasonable in every circumstances to avoid the loss, access, use, modification, leak or disclosure of those information, except with the permission of the owner of the information or any other party authorized by law.

2. Any person shall not interfere in the electronic system, access, retrieve, copy, extract, leak, delete or modify data, which is under the retention of any other person in bad-faith or without permission.

Article 33: Implementation of provisions related to consumer protection

Any person using electronic communications for commercial activities with consumers shall comply with all other provisions and regulations related to consumer protection.

Chapter 7

Government Activities and Transactions via Electronic System

Article 34: Acceptance of electronic communications by state institutions

1. Ministries or institutions of the government may use the following actions and transaction in electronic form:
    a. The filing of documents or the fulfilment of requirements for document creation or retention;
    b. Issuance of any license or permission letter;
    c. Provision for the method and manner of payment; or
    d. Other authorized activities as determined by the state ministries-institutions.
2. In any case where the state ministries-institutions decides to use electronic communications in any activities or transaction as stated in the provisions of the paragraph (1) above, such ministry or institution/agency may specify:
    a. The manner and form in which such electronic communication information shall be filed, created, retained or published;
    b. The type and form of signature required when there is a requirement for a signature in the electronic communication;
    c. The manner and form in which such signature shall be affixed to the electronic communication;
    d. Control processes and procedures as appropriate to ensure accuracy, security and confidentiality of electronic communications or payments; and
    e. Any other conditions required to be equivalent as documents or electronic payment with that documents or payment in written format.

Chapter 8

Electronic Evidences

Article 35: General admissibility of electronic evidence

Nothing in the provisions of rules on any evidence shall apply to deny the general admissibility of an electronic record as evidence on the sole ground that it is an electronic record, even if the evidence is not in its original form.

Article 36: Perfection of the electronic system

1. In any legal proceeding, the validity of electronic evidence may be satisfied on proof of the perfection of the electronic system in or by which the data was recorded or stored.
2. In the absence of evidence to the contrary, the electronic system in which used for recording and storing for electronic recording is presumed perfection in any legal proceeding shall be in according with one of the following conditions:

a. Where evidence is adduced that supports a fact finding/confirming that the electronic system or other similar instrument was operating properly is when the electronic recording is presumably recorded and stored or when it is used as evidence or in the event that the electronic system or other similar instrument was not operating properly or not working at all but the perfection of the electronic record was not affected by such circumstances, and there are no other reasonable grounds to doubt the perfection of the record;

b. Where it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it as evidence in accordance with legal procedures; or

c. Where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to use/introduce the electronic record as evidence in the proceedings in accordance with legal procedures.

Article 37: Perfection of information

1. In the absence of evidence to the contrary, an electronic record made or stored in an electronic system is presumed to be proven that it has a perfection in any legal proceeding if the electronic record:

   a. Has remained complete and unaltered, apart from the addition of any endorsement; or any immaterial change which arises in the normal course of communication, storage or display;

   b. Has been certified or has been signed in an electronic format, by a method provided by a duly licensed security procedure provider;

   c. Has its perfection and content certified by competent ministries or institutions;

   d. Has been recorded in a storage device, or any other electronic means that does not allow alteration of the electronic records;

   e. Has been examined and its perfection confirmed by an expert appointed by the Court;

   f. When there is evidence supporting a fact finding/confirming that at all material times the electronic system or other similar instrument was operating properly during/at important times, or if not, that in any respect in which it was not operating properly or out of operation, the perfection of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the perfection of the record; or

   g. When there is evidence proving that the electronic record was recorded or stored by a party participating in the legal proceedings who is adverse in interest to the party seeking to use the electronic record;

2. When there is evidence proving that the electronic record was recorded or stored as usual and for the purpose of ordinary course of business by a natural person who is not a party to the legal proceedings, and such natural person did not record or store it under the control of the party seeking to use the record.

3. Where a report contained in an electronic record produced by an electronic system does not constitute hearsay, such report shall be admissible if the conditions specified in the provisions of the paragraph (2) related to the electronic record are met.

Article 38: Printouts

Any printouts with the original content from the electronic records can be used as evidence in legal proceedings.

Article 39: Burden of prove the authenticity of electronic evidence

1. The person requesting to introduce an electronic record in any legal proceeding shall be responsible for showing its authenticity with evidence to support the electronic record to be introduced.
2. In the case where there is any provisions which protects the vulnerable persons, including consumers and children, and which establishes the burden of introducing evidence that provides more benefits to those individuals than this law does, the provisions shall prevail over this Article.

Article 40: Standards of recording or preserving of electronic records

For the purpose of determining, under any other provisions, as to whether or not an electronic record is admissible, evidence may be presented based on standard, procedure, usage or practice on how an electronic record is to be recorded or preserved by taking into consideration the type of business, the nature and the purpose of the electronic record.

Article 41: Issuance of an authenticity certificate

1. Any person wishing to prove the authenticity of an electronic record as evidence, he/she can request for the evidence from the expert with respect to the authenticity of the electronic record in the form of a certificate.
2. The authenticity certificate under the provision of paragraph 1 above shall be issued by:
    a. Competent ministries - institutions or a person responsible in relation to the operation or management of a specified security procedure provider or a security procedure provider recognized by the Court; or
    b. An expert appointed or recognized by the Court.
3. A person who has the authority to issue the authenticity certificate as mentioned in the provision of paragraph 2 above shall not falsify or issue a false or unreal authenticity certificate of a record or electronic evidence.

Article 42: Other Procedures for the Production of Electronic Evidence

In addition to the means of proof referred to in this law, electronic evidence may be produced by means of alternative techniques and procedures, such as certification by a notary or competence institutions, recording on non-rewritable electronic medium, and electronic system forensics result in the course of judicial discovery.

Article 43: Violation of Coding

Any person shall not encode in electronic communications via electronic system which is an evidence that could lead to an accusation or encode the data or evidence in electronic system in relation to an offense.

Article 44: Admissibility of Electronic Records from Foreign Countries

Electronic evidence confirmed by competent ministries or institutions of foreign states shall be admissible as evidence if the perfection/integrity of the electronic system which records or stores the electronic record comply with the accuracy standards provided for in Chapter 8 of the law.

Article 45: Admissibility of Electronic Information from Foreign Countries

In order to determine as to whether or not the information in the electronic form is admissible or admissible to a certain degree, it is not necessary to determine the place where such information was produced or used or where the place of business was established overseas as long as such electronic record can accessible and retrievable in the jurisdiction of the Kingdom of Cambodia.

Chapter 9
Electronic Payments and/or Electronic Funds Transfers

Article 46: Electronic Payment Transaction

1. Any person operating a payment system, providing a payment service, issuing an electronic payment instrument or providing an electronic means of payment, or conducting any other operations to the public considered to be an electronic payment and shall obtain prior authorization or license from the National Bank of Cambodia.

2. The National Bank of Cambodia shall be the competent authority to formulate regulations relating to electronic payment.

Article 47: Responsibilities of Payment Service Providers

1. Payment service providers shall not provide the customers with an unsolicited payment instruments except in case of card expiration or replacement.

2. Before executing an electronic fund transfer, the payment service providers shall clearly identify the customers' identity and re-authenticate the electronic fund transfer. The payment service providers shall be held liable in the following cases:

    a. Execution of a transaction without authorization of the customers;

    b. Execution of a fund transfer after receiving report of forgery, loss, or theft of the electronic fund transfer instruments;

    c. Execution of a transaction despite the notification from the customers as defined in Article 48 below;

    d. Failure to comply with the instruction of the customers or an execution which is not in compliance with the customer's instruction; or

    e. Technical malfunction, an error in operating the technical system, or a flaw in the electronic fund transfer instruments.

3. The payment service providers shall not be held liable in case of force majeure event or customers' defaults.

4. In the case where the payment service providers are to be held liable, the service providers shall reimburse to the customer no later than 30 (thirty) days from the date of receiving the notification of the customer as defined in Article 48 of this law the transaction fee, charges, and a fine for late payment resulting from this transaction, without accounting for damages which may be suffered by the customer.

5. Any person shall not, without authorization, issue a card or transform the card into another form different from that of the original in bad faith for forgery or cheating purposes, which could cause damage/injury to another person.

Article 48: Responsibilities of Customers

1. Customers shall notify the payment service providers of any unauthorized, mistaken or wrongful transaction of their own account.
2. Customers shall notify the payment service providers or the establishment authorized by the payment service providers of any loss or theft of electronic transfer instrument or electronic fund transfer method or theft of data, which can be used with the payment instrument. Such notification shall be made in writing or by any electronic means which is acceptable to the payment service providers, and shall notify as soon as possible not exceeding 2 (two) days after the theft or loss of electronic transfer instrument is discovered.
3. In case where there is sufficient evidence proving that the loss or damage is caused by customer's default, the payment service provider shall have rights to demand the customer to be fully responsible for such loss or damage.
4. If there is no evidence to prove the customer's default, the payment service provider shall be fully and unconditionally responsible for such loss or damage.

Chapter 10
Competency, complaint and Procedures for a Fine

Article 49: Competency

A written warning, cease of business activities or transaction, suspension, revocation or cancellation of an authorization or license and imposition of a fine shall fall within the competency of the Ministry of Commerce and the Ministry of Posts and Telecommunications.

In case where a person refuses to comply with above measures, the Ministry of Commerce and the Ministry of Posts and Telecommunications may refer the case to the competent court.

Article 50: Procedures for a Complaint

1. Those who are not satisfied with the written warning, cease of business activities or business transaction, suspension, revocation or cancellation of the authorization or license and a fine by the Ministry of Commerce and the Ministry of Posts and Telecommunications shall be entitled to lodge their complaint with the Minister of Commerce and the Minister of Posts and Telecommunications.
2. The Minister of Commerce and the Minister of Posts and Telecommunications shall make

decision within 30 (thirty) days at the latest.

3. Any person who are not satisfied with the decision of the Minister of Commerce and the Minister of Posts and Telecommunications shall have the rights to lodge their complaint to the competent court of the Kingdom of Cambodia within 30 (thirty) days at the latest from the date of receipt of the notification of the decision.

Article 51: Procedure for Imposing a Fine

Procedure for imposing a fine, payment of a fine, management of fining receipt and disposition of the proceeds derived from such fines as prescribed in the provisions of this law shall be determined by an inter-ministerial Prakas between the Minister of Economy and Finance, the Minister of Commerce and the Minister of Posts and Telecommunications.

Chapter 11
Penalties

Article 52: Sanction

Sanctions in this law shall include a written warning, cease of business activities or business transactions, suspension, revocation or cancellation of the authorization or license, penalty, imprisonment and a (monetary) fine.

Article 53: Offence for Identity Theft

To be punishable by an imprisonment from 6 (six) months to 3 (three) years and a fine from 1,000,000 (one million) Riel to 6,000,000 (six million) Riel for those who act in violation of the provision in Article 22.

Article 54: Offence for Failure to Report of an Information or a Fact

To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for the intermediary and the electronic commerce service providers who act in violation of the provisions of paragraph 1 and paragraph 2 of Article 25.

Article 55: Provision of False Information

To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for those who commit act as prescribed in the provision of paragraph 5 of Article 25.

Article 56: Executing of an Unauthorized Transaction

To cease business activities or business transaction and be subjected to a monetary fine not exceeding 10,000,000 (ten million) Riel for those who act in violation of the provision of paragraph 1 of Article 26.

If any person used to be subjected to the measure prescribed in paragraph 1 already, and the same offence has been committed, he/she shall be punishable by an imprisonment from 1 (one) year to 3 (three) years and a fine from 2,000,000 (two million) Riel to 6,000,000 (six million) Riel.

Article 57: Offence for Failure to Comply with the Provision Regarding Minimum Information in Electronic Commerce

To be subjected to a written warning for those who act in violation of the provisions in paragraph 1 and paragraph 2 of Article 29.

Where the written warning was once given, but the same offence as prescribed in paragraph 1 above has been committed, the license or the authorization of the electronic commerce provider shall be suspended or revoked.

Article 58: Offence for Sending an Unsolicited Business Communication

To be subject to a written warning for those who act in violation of the provisions of Article 30.

Where the written warning was once given, but the same offence has been committed as set forth in paragraph 1 above, the licensed or authorized of an intermediary or the electronic commerce service provider shall be suspended or revoked or disable the media or closed down the electronic medium of the originator.

Article 59: Offence for Electronic System Forgery and Malicious Code

To be punishable by an imprisonment from 6 (six) months to 3 (three) years and a fine from 1,000,000 (one million) Riel to 6,000,000 (six million) Riel for those who act in violation of the provisions of Article 31.

Article 60: Offence for Failure to Comply with Data Protection Obligations

To be punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riel to 4,000,000 (four million) Riel for those who store information in an electronic form for a personal purpose, which is contrary to the provision of paragraph 1 of Article 32.

To be punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riel to 4,000,000 (four million) Riel for those who act in violation of the provision of paragraph 2 of Article 32.

Article 61: Offence for Violation of Authenticity Issuance

To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for those who act in violation of the provision of paragraph 3 of Article 41.

Article 62: Offence for Coding Violation

To be punishable by an imprisonment from 1 (one) year to 3 (three) years and a fine from 2,000,000 (two million) Riel to 6,000,000 (six million) Riel for those who act in violation of the provision of Article 43.

Article 63: Offence for an Electronic Payment Transaction

To be punishable by an imprisonment from 1 (one) year to 5 (five) years and a fine from 1,000,000 (one million) Riel to 10,000,000 (ten million) Riel for those who act in violation of the provision of paragraph 1 of Article 46.

Article 64: Offence for Electronic Payment Instrument Forgery

To be punishable by an imprisonment from 1 (one) year to 3 (three) years and a fine from 2,000,000 (two million) Riel to 6,000,000 (six million) Riel for those who act in violation of the provision of paragraph 5 of Article 47.

Article 65: Criminal Responsibility of a Legal Entity

1. A legal entity may be pronounced to be criminally responsible in accordance with the conditions prescribed in Article 42 (criminal responsibility of a legal entity) of the Criminal Codes for offences set forth in Article 53 to Article 54, paragraph 2 of Article 56, and Article 59 to Article 64 of this law.
2. A legal entity shall be fined twice as much, plus one or more additional penalties as follows:

    a. Dissolution in accordance with the formalities determined in Article 170 (Dissolution and Liquidation of a Legal Entity) of the Criminal Code.

    b. Placement under the court surveillance according to the modalities determined by Article 171 (Placement under the Court Surveillance) of the Criminal Code.

    c. Prohibition from conducting one or more activities according to the modalities determined by Article 172 (Prohibition from Operating Activities) of the Criminal Code;

    d. Posting the decision on punishment in accordance with the formalities determined by Article 180 (Posting of a Decision) of the Criminal Code;

    e. Publication of the decision on punishment on newspapers or broadcasting on all means of audio-visual communications according to the modalities prescribed in Article 181 (Broadcasting the Decision by all Means of Audi-Visual Communications) of the Criminal Code.

Chapter 12
Final Provision

Article 66: Abrogation
All provisions contrary to this Law shall be abrogated.

Article 67: Application of this law
Once in force, this law shall be applied after 6 (six) months publication or dissemination.

PRL. 1911.1654

Saturday, 6th day of the waxing,
Month of katdeuk, Year of Pig, B.E. 2563
Done at the Royal Palace, 2 November 2019

NORODOM SIHAMNI

Having made the request to His Majesty the King
For Signature
Prime Minister

Samdech Akka Moha Sena Padei Techo HUN SEN

Having informed Samdech Akka Moha Sena Padei Techo
Prime Minister
Minister of Commerce

PAN SORASAK

Annex
Definition

The key terms used in this law shall be defined as follows:

1. **"Access"** means accessing into a computer program, a computer system, a system or an electronic network in order to communicate, transmit, store, or download data, information, or other documents contained in the electronic system by any means.
2. **"Addressee"** means a person who is intended by the originator to receive an electronic communication except an intermediary with respect to the electronic communication.
3. **"Automated system"** means a computer program, computer system, electronic system or network or other electronic means, which are used to notify or responded automatically without an intervention of any natural person.
4. **"Card"** means a card/bank card, credit/debit card, smart card, card/payment card, although in an electronic form, which bears the value and has the function for making payment.
5. **"Contaminant"** means electronic programs which are designed to:
    (a) Modify, destroy, record, transmit data or programs contained in an electronic system; or
    (b) Interfere by any means in the normal operation of an electronic system or electronic network;
6. **"Cardholder"** means the person who has named on the card and receive benefit from such a card.
7. **"Communication"** means any statement, declaration, demand, notice, request, offer or acceptance that the parties are required to make or choose to make in connection with the formation or performance of a contract.
8. **"Counterfeit card"** means any cards/payment cards which is made by fictitious, altered and false representation, depiction, or cards/payment cards which is comprised of any component of the card that is illegal.
9. **"Data"** refers to a group of numbers, characters, symbols, message, images, sound, video, information or electronic program which are prepared in a form suitable for use in database or an electronic system.
10. **"Electronic"** refers to technology having electrical, digital, magnetic, optical, biometric, electrochemical, wireless, electromagnetic, or other technologies of similar functions.
11. **"Electronic Address"** means any number or addressee which is used for sending or receiving notifications, documents, information or electronic communication.
12. **"Authenticity"** refers to an accuracy and credibility of electronic communications.
13. **"Electronic commerce"** refers to activities involving purchase, sale, rental, exchange of goods or services, including business activities and civil as well as activities and various transactions by the state through electronic system.
14. **"Electronic Payment Instrument"** means any cards/payment cards or any payment instruments which is in an electronic form and has function to make a cash payment.

15. **"Electronic communication"** means information which is communicated, processed, recorded, displayed, created, stored, received or transmitted by electronic means.
16. **"Electronic device"** means any devices designed to manage, control, and operate through electronic system.
17. **"Electronic evidence"** means any information, data or documents which are created, stored, sent or received in electronic format or electronic communication for being used to prove facts in legal proceedings, and such information, data or documents shall be authentic in accordance with the e-Commerce Law.
18. **"Electronic form"** refers to form of information, data or document which are created, sent/transmitted, received or stored in electronic system.
19. **"Electronic fund transfer"** means any transaction which is conducted through an electronic fund transfer counter or via any movable electronic devices or via electronic devices of similar functions in order to instruct banking and financial institutions to debit or credit an account.
20. **"Electronic record"** refers to a record which is made, communicated, received, stored or processed in an electronic system or which is for transmission from one electronic system to another.
21. **"Electronic commerce service provider"** means a person who uses electronic means to supply goods and/or services except for insurance establishments.
22. **"Electronic signature"** means any signatures which are created through electronic means for using to identify the signatory, including digital signature, biometric signature and other signatures.
23. **"Electronic system"** refers to an electronic device or a group of devices interconnected or inter-related via an electronic program, which may perform automatic processing of data, information or documents, including electronic devices for the storage of such data, information or documents.
24. **"Information system"** refers to a system for generating, sending, receiving, storing or otherwise processing electronic records.
25. **"Intermediary"** refers to a person who providing services, sending, receiving, transmitting or storing services, either on a temporary or permanent basis, of the electronic communication or provides other services relating to the electronic communication, including the following persons:
    1. A person representing the sender, receiver, transmitter, or the custodian;
    2. Telecommunication service providers;
    3. Network service providers;
    4. Internet service providers;
    5. Search engines providers;
    6. Online payment service providers;
    7. Online auction service providers;
    8. Online marketplaces service providers and internet commerce service provider.

26. **"Issuer"** refers to banking and financial institutions or any person who obtained approval to issues a payment card.

27. **"Malicious code"** refers to a program or a hidden function of a program that infects data, information or documents by or without leaving any trace/mark of the virus in the infected electronic file, and the virus is capable of spreading over the system with or without human intervention.

28. **"Originator"** refers to a party or a representative who initiates the operation to create, store or transmit data via electronic means, excluding the intermediary.

29. **"Payment Service Provider"** refers to banking and financial institutions or any other person who is authorized by or obtained the license from the National Bank of Cambodia to operate the payment system, issue electronic payment instrument or electronic means of payment or to conduct any operations considered to be an electronic payment to the public.

30. **"Place of business"** refers to:

    (a) A place indicated by the sender or addressee, unless there is a party who claims otherwise that the sender or addressee does not have the place of business in the area where they claim to be.

    (b) If any party has not specifically indicated his place of business, and such party has more than one place of business, the place of business shall be then the one which has the closest relationship with the contract involved, taking into consideration the circumstances known to or examined by the party any time before or during the time of executing the contract.

    (c) For a natural person who has no place of business, the place of business shall be their permanent address.

    The followings shall not be a place of business of a party:

    - A place where the technology materials or equipment of the information system are used;
    - Electronic address or domain name which is attached to the location of a party.

31. **"Record"** refers to information, data or documents which is recorded, stored or otherwise inserted in a tangible form or stored in an electronic, paper-based or other forms and is retrievable in visible form.

32. **"Service provider"** refers to:

    (a) A person who provides an information and communication services including sending, receiving, storing or processing the electronic communication or providing of services through other electronic systems;

    (b) A person who owns, possesses, operates, manages or controls a public switched network or a person who provides telecommunication services; or

    (c) Any other person who processes or stores data for the use of electronic telecommunication service-oriented or users of such service.

33. **"Security procedure provider"** refers to a person who develops or provides the security procedures.

34. **"Security procedure"** refers to a procedure which is established by law or a contract or a decision of any party, and is applied for the purpose of:

    (a) Verifying that the signature, communication or transaction in the electronic system is belong to particular person, or

    (b) Detecting error or alteration in the communication, or in the place where the electronic record is stored from any specific period of time.

The above security procedure may require the use of algorithms formula or codes, identifying words or numbers, coding, answerback (secret question) or acknowledgment of any procedures, or similar security devices.

35. **"Writing/written"** refers to any information or other records which is written, inscribed or printed on paper or other materials.

36. **"Email or Electronic Message"** refers to message or information which is created or sent or received from electronic system, indulging attachments in texts, image, sound, video, and any electronic record which can be transmitted with the message.

37. **"Succession"** or **"Will"** refers to the assignment of right and duties of the decedent to one or more successors at will or by law.

38. **"Acceptance"** refers to an expression of will in which a person has expressed his consent to an offer made by other persons in order to form a contract.