ផ្នែក ទី៣

សៀវភៅត្រួតពិនិត្យសន្តិសុខព័ត៌មានការិយាល័យ

លទ្ធផលនៃការត្រួតពិនិត្យសន្តិសុខព័ត៌មាននៅការិយាល័យ

នៅ [ ]

NiDA

ការត្រួតពិនិត្យខាងក្រោមនេះ ត្រូវបានរៀបចំឡើងជាជំហានទីមួយនៃការគ្រប់គ្រងការិយាល័យសន្តិសុខព័ត៌មាន ដោយលោក/លោកស្រី

នៅម៉ោង

ប្រភេទនៃការគ្រប់គ្រង	ធាតុដែលត្រូវត្រួតពិនិត្យ	រូបថតទីតាំងទុកជា កស្តុតាង	ស្ថានភាពបច្ចុប្បន្ន (ត្រួតពិនិត្យលទ្ធផល)	វិធានការដែលត្រូវដាក់ចេញ	ការវិនិច្ឆ័យ
ការម៉ៅការងារអោយទៅប្រភពខាងក្រៅ	លក្ខណៈវិនិច្ឆ័យនៃការជ្រើសរើសអ្នក			ឯកសារ	
	អត្ថិភាពនៃខចែងអំពីកាតព្វកិច្ចមិនបញ្ចេញព័ត៌មានក្នុង កិច្ចសន្យា			ឯកសារ	
ព័ត៌មានឯកជន ឬទិន្នន័យផ្ទាល់ខ្លួន	សម្រាប់និយោជក ៖ អត្ថិភាពនៃខចែងអំពីកាតព្វកិច្ច មិនបញ្ចេញព័ត៌មាននៅក្នុងកិច្ចសន្យាការងារឬកិច្ច ព្រមព្រៀងដទៃទៀត			ឯកសារ	
	សម្រាប់និយោជិត ៖ អត្ថិភាពនៃខចែងអំពីកាតព្វកិច្ច មិនបញ្ចេញព័ត៌មាននៅក្នុងកិច្ចសន្យាការងារឬកិច្ច ព្រមព្រៀងដទៃទៀត			ឯកសារ	
	សម្រាប់ក្រុមហ៊ុន ៖ អត្ថិភាពនៃមាត្រាកិច្ចព្រមព្រៀង ឬកិច្ច សន្យាអំពីការការពារទិន្នន័យផ្ទាល់ខ្លួន ឬព័ត៌មានឯកជន			ឯកសារ	

ប្រភេទនៃការគ្រប់គ្រង	ធាតុដែលត្រូវត្រួតពិនិត្យ	រូបថតទីតាំងទុកជា កស្តុតាង	ស្ថានភាពបច្ចុប្បន្ន (ត្រួតពិនិត្យលទ្ធផល)	វិធានការដែលត្រូវដាក់ចេញ	ការវិនិច្ឆ័យ
អគារការិយាល័យ	ការអនុញ្ញាតអោយចូលក្នុងបន្ទប់ និងអត្តិភាព នៃកំណត់ត្រាអំពីការចូល/ចេញពីបន្ទប់	តម្រូវការដាច់ខាត		ការបង្កើតវិធាន	
	ការកំណត់ព្រំដែនទីធ្លាការិយាល័យ និងទីធ្លា ឆ្លងកាត់ទូទៅ			ក្តារកត់សម្គាល់	
	ប្រព័ន្ធសុវត្ថិភាពអគារ	តម្រូវការ		ការចាក់សោការពារកម្រិតខ្ពស់	
	ការងារបស់អ្នកខាងក្រៅ			ការបង្កើតវិធាន	
	ការការពារទិន្នន័យកិច្ចសន្យារបស់និយោជិក ។ល។			ការបង្កើតវិធាន	
	ការរក្សាទុកកំណត់ត្រាសម្រាប់ការប្រើប្រាស់សេវា អ្នកនាំសំបុត្រ	តម្រូវការ		ការបង្កើតវិធាន	

ប្រភេទនៃការគ្រប់គ្រង	ជាតុដែលត្រូវត្រួតពិនិត្យ	រូបថតទីតាំងទុកជា កស្តុតាង	ស្ថានភាពបច្ចុប្បន្ន (ត្រួតពិនិត្យលទ្ធផល)	វិធានការដែលត្រូវដាក់ចេញ	ការវិនិច្ឆ័យ
ម៉ាស៊ីនទូរសារ និងម៉ាស៊ីនបោះពុម្ព	កំណត់ត្រានៃការប្រើប្រាស់ផ្ទាល់ខ្លួនសម្រាប់ម៉ាស៊ីនទូរសារ			ការបង្កើតវិធាន	
	ការមិនយកចិត្តទុកដាក់ចំពោះឯកសារបោះពុម្ព/ ឯកសារទូរសារដោយមិនយកចិត្តទុកដាក់	តម្រូវការ		ការបង្កើតវិធាន	
	កំណត់ត្រានៃការធ្វើទូរសារ (ធ្វើ/ទទួល)			ការបង្កើតវិធាន	
	កំណត់ត្រានៃការធ្វើទូរសារឯកសារសម្ងាត់			ការបង្កើតវិធាន	
ទូដាក់អីវ៉ាន់/ ទូដាក់សៀវភៅ	ចំណាត់ថ្នាក់/ការបែងចែកប្រភេទព័ត៌មាន			ការបង្កើតវិធាន	
	ការការពារទិន្នន័យផ្ទាល់ខ្លួនដោយប្រើមុខងារចាក់សោ	តម្រូវការដោចំខាត		ការបង្កើតវិធាន និងការចាក់សោ	
	ការការពារឯកសារ	តម្រូវការដោចំខាត		ការបង្កើតវិធាន	
	រយៈពេលរក្សាទុកឯកសារ			ការបង្កើតវិធាន	
	កំណត់ត្រាឧបករណ៍រក្សាទុកទិន្នន័យដែលថែរក្សា ដោយមុខងារចាក់សោ			ការបង្កើតវិធាន និងការចាក់សោ	
	ការលុបអោយអស់ពីអេក្រង់បង្ហាញតាមរយៈ ការកំណត់មុខងារ screen saver ដោយមាន ដាក់ពាក្យសម្ងាត់	តម្រូវការ		ការបង្កើតវិធាន	
	អត្ថិភាពនៃលក្ខណៈវិនិច្ឆ័យគ្រប់គ្រងអត្ដលេខអ្នកប្រើប្រាស់ និងពាក្យសម្ងាត់			ការបង្កើតវិធាន	

ប្រភេទនៃការគ្រប់គ្រង	ធាតុដែលត្រូវត្រួតពិនិត្យ	រូបថតទីតាំងទុកជា កស្តុតាង	ស្ថានភាពបច្ចុប្បន្ន (ត្រួតពិនិត្យលទ្ធផល)	វិធានការដែលត្រូវដាក់ចេញ	ការវិនិច្ឆ័យ
កុំព្យូទ័រផ្ទាល់ខ្លួនលើតុ	ការកំណត់ពាក្យសម្ងាត់			ការបង្កើតវិធាន	
	ការប្រើប្រាស់អត្តលេខ និងពាក្យសម្ងាត់អ្នកប្រើប្រាស់			មិនប្រើ	
	ក្បាទុកទិន្នន័យផ្ទាល់ខ្លួន			ការបង្កើតវិធាន	
	ការប្រើប្រាស់អាសយដ្ឋានអ៊ីម៉ែលខុស និងការលួចប្រើអ៊ីម៉ែល			ការបង្កើតវិធាន	
	ការប្រើប្រាស់កម្មវិធីចាប់មេរោគ			ត្រូវអនុវត្ត	
	ការធ្វើបច្ចុប្បន្នភាពសុំណុំឯកសារគុំរូនៃកម្មវិធីខាងលើ			ត្រូវអនុវត្ត	
កុំព្យូទ័រជាប់តុ	ចាក់សោតុនៅពេលចេញទៅក្រៅ			ការបង្កើតវិធាន	
	លុបអោយអស់ពីលើអេក្រង់បង្ហាញកុំអោយមាន ព័ត៌មានសម្ងាត់ នៅពេល			ការបង្កើតវិធាន	
	ការលុបចោល/ការមិនយកចិត្តទុកដាក់ចំពោះព័ត៌មានផ្ទាល់ខ្លួន	តម្រូវការ		ការបង្កើតវិធាន	
LAN និងអ៊ីនធើណែត	ការការពារបណ្តាញ	តម្រូវការ		ការបង្កើតវិធាន	
	វិធានការសន្តិសុខនៃបរិក្ខារបណ្តាញ			ការបង្កើតវិធាន	
	ការផ្តាច់បណ្តាញខាងក្នុងពីបណ្តាញខាងក្រៅ			ការបង្កើតវិធាន	
	កំណត់ត្រានៃការចូលទៅប្រើប្រាស់			ការបង្កើតវិធាន	

ប្រភេទនៃការគ្រប់គ្រង	ធាតុដែលត្រូវត្រួតពិនិត្យ	រូបថតទីតាំងទុកជា កស្តុតាង	ស្ថានភាពបច្ចុប្បន្ន (ត្រួតពិនិត្យលទ្ធផល)	វិធានការដែលត្រូវដាក់ចេញ	ការវិនិច្ឆ័យ
កុំព្យូទ័រចល័ត ឬ កុំព្យូទ័រយួរដៃ	អនុញ្ញាតអោយយកកុំព្យូទ័រចល័តចេញ			ការបង្កើតវិធាន	
	ការរក្សាទុកទិន្នន័យផ្ទាល់ខ្លួន			ការបង្កើតវិធាន	
	ការថែរក្សាកុំព្យូទ័រផ្ទាល់ខ្លួននៅពេលយកចេញទៅក្រៅ	តម្រូវការ		ការបង្កើតវិធាន	
កុំព្យូទ័រមេ	ការចូលក្នុងបន្ទប់កុំព្យូទ័រមេ និងការចាក់សោបន្ទប់			ការបង្កើតវិធាន	
	ការអនុញ្ញាតអោយចូលក្នុងបន្ទប់កុំព្យូទ័			ការបង្កើតវិធាន	
	អត្ថិភាពនៃលក្ខណៈវិនិច្ឆ័យគ្រប់គ្រងអត្ដលេខ អ្នកប្រើប្រាស់ និងពាក្យសម្ងាត់			ការបង្កើតវិធាន	
	ការប្រើប្រាស់ការពង្រឹងប្រឆាំងនឹងការរំ			ការបង្កើតវិធាន	
	វិធានការសម្រាប់ពេលដាច់ចរន្តអគ្គិសនី			ការបង្កើតវិធាន	
	វិធានការការពារសម្រាប់ឧបករណ៍របស់កុំព្យូទ័រមេ	តម្រូវការ		ការបង្កើតវិធាន	
	ភាពជាប់លាប់នៃប្រតិបត្តិការកុំព្យូទ័រមេ			ការបង្កើតវិធាន	
	ឧបករណ៍ចម្លងឯកសារទុក			ការបង្កើតវិធាន	
	ការចម្លងទិន្នន័យទុក			ការបង្កើតវិធាន	
	ការការពារឧបករណ៍រក្សាទុកទិន្នន័យដែលបានថតចម្លង	តម្រូវការ		ការបង្កើតវិធាន	

ប្រភេទនៃការគ្រប់គ្រង	ធាតុដែលត្រូវត្រួតពិនិត្យ	រូបថតទីតាំងទុកជា កស្តុតាង	ស្ថានភាពបច្ចុប្បន្ន (ត្រួតពិនិត្យលទ្ធផល)	វិធានការដែលត្រូវដាក់ចេញ	ការវិនិច្ឆ័យ
	ការចូលទៅប្រើប្រាស់ព័ត៌មានផ្ទាល់ខ្លួន			ការបង្កើតវិធាន	
	ការចូលទៅប្រើប្រាស់សំណុំឯកសារ			ការបង្កើតវិធាន	
	ការអនុញ្ញាតអោយចូលទៅប្រើប្រាស់ទិន្នន័យ ផ្ទាល់ខ្លួន និងសំណុំឯកសារ			ការបង្កើតវិធាន	
	កំណត់ត្រានៃការចូលទៅប្រើប្រាស់ទិននន្ន័យផ្ទាល់ខ្លួន/ សំណុំឯកសារសម្ងាត់			ការបង្កើតវិធាន	
	ការការពារទិន្នន័យផ្ទាល់ខ្លួនពីការចូលទៅប្រើប្រាស់ដោយសេរី			ការបង្កើតវិធាន	
	ការផ្ទៀងផ្ទាត់មុខងារគ្រប់គ្រងការប្រើប្រាស់ទិន្នន័យផ្ទាល់ខ្លួន			ការបង្កើតវិធាន	
	វិធានការចូលទៅប្រើប្រាស់តាមរយៈកុំព្យូទ័រ ផ្សេងៗ			ការបង្កើតវិធាន	

ប្រភេទនៃការគ្រប់គ្រង	ធាតុដែលត្រូវត្រួតពិនិត្យ	រូបថតទីតាំងទុកដាក តស្តុតាង	ស្ថានភាពបច្ចុប្បន្ន (ត្រួតពិនិត្យលទ្ធផល)	វិធានការដែលត្រូវដាក់ចេញ	ការវិនិច្ឆ័យ
ការលុបចោលឬការបំផ្លាញ	ការប្រើប្រាស់ម៉ាស៊ីនកម្ទេចក្រដាស	តម្រូវការ		ការបង្កើតវិធាន	
	ការលុបចេញពីឧបករណ៍ក្បាទុកទិន្នន័យ			ទាំងស្រុង	
	ការលុបចេញពីកុំព្យូទ័រផ្ទាល់ខ្លួន			ការបញ្ជាក់អំពីការបំផ្លាញនិងការលុបចោលព័ត៌មាន ដែលក្បាទុកនៅក្នុងឧបករណ៍ក្បាទុកទិន្នន័យ	
លក្ខណៈពិសេសផ្សេងៗ	កំណត់សម្គាល់ ៖ ១. អំពី "ការវិនិច្ឆ័យ" G: ល្អ A: អាចទទួលយកបាន P: មិនល្អ - ត្រូវកែលម្អ ២. រូបថតទីតាំង តម្រូវការដាច់ខាត -- ចាំបាច់ត្រូវថតអោយបានច្រើនដងជាប់ៗគ្នា តម្រូវការ -- គួរថតអោយបានច្រើនដងជាប់ៗគ្នា ប្រសិនបើអាចធ្វើបាន				

ផ្នែក ទី៤

ឯកសារសម្រាប់ធ្វើបទបង្ហាញ

NiDA

JICA

លក្ខណៈវិនិច្ឆ័យ នៃនិយាម
សន្តិសុខព័ត៌មាន របស់រដ្ឋាភិបាល

Government Information Security Standard Criteria
(GISSC)

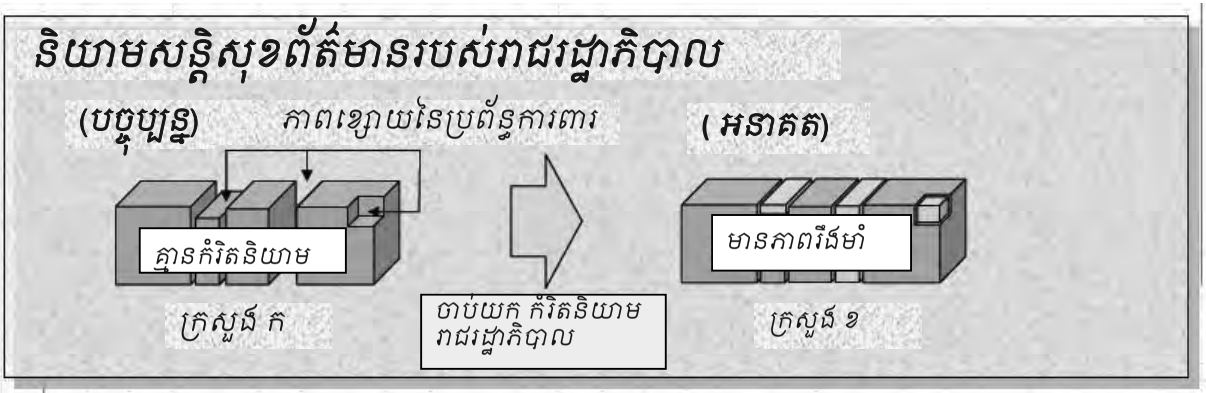
០១ - តុលា - ២០០៩

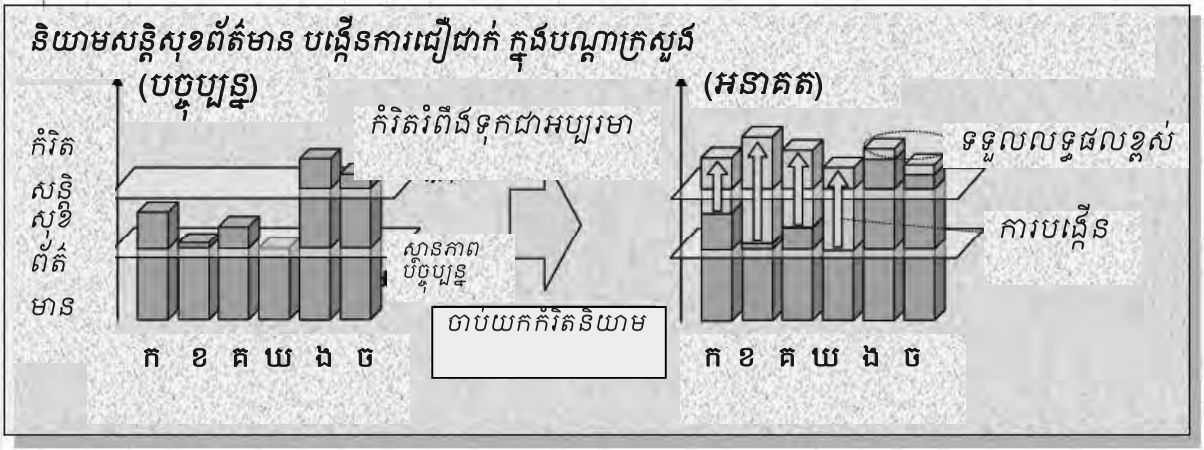
- ឯកឧត្តម **ជា ម៉ានិត** អគ្គលេខាធិការរង នៃ អគ្គលេខាធិការដ្ឋាន អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍វិស័យបច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា ប្រធានក្រុមការងារបច្ចេកទេសគ្រប់គ្រង កិច្ចការសន្តិសុខ បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន (iSMTT)
- លោក **ស៊ីណូរី គុរ៉ាដ៊ី** ជំនាញការ របស់ទីភ្នាក់ងារសហប្រតិបត្តិការអន្តរជាតិនៃប្រទេសជប៉ុន

ការកំណត់និយាមសន្តិសុខព័ត៌មានរបស់រដ្ឋាភិបាល (GISSC)
ខិចានចូចៅ

គោលជំហរ GISSC ក្នុងការរៀបចំឯកសារគ្រប់គ្រងសន្តិសុខព័ត៌មាន

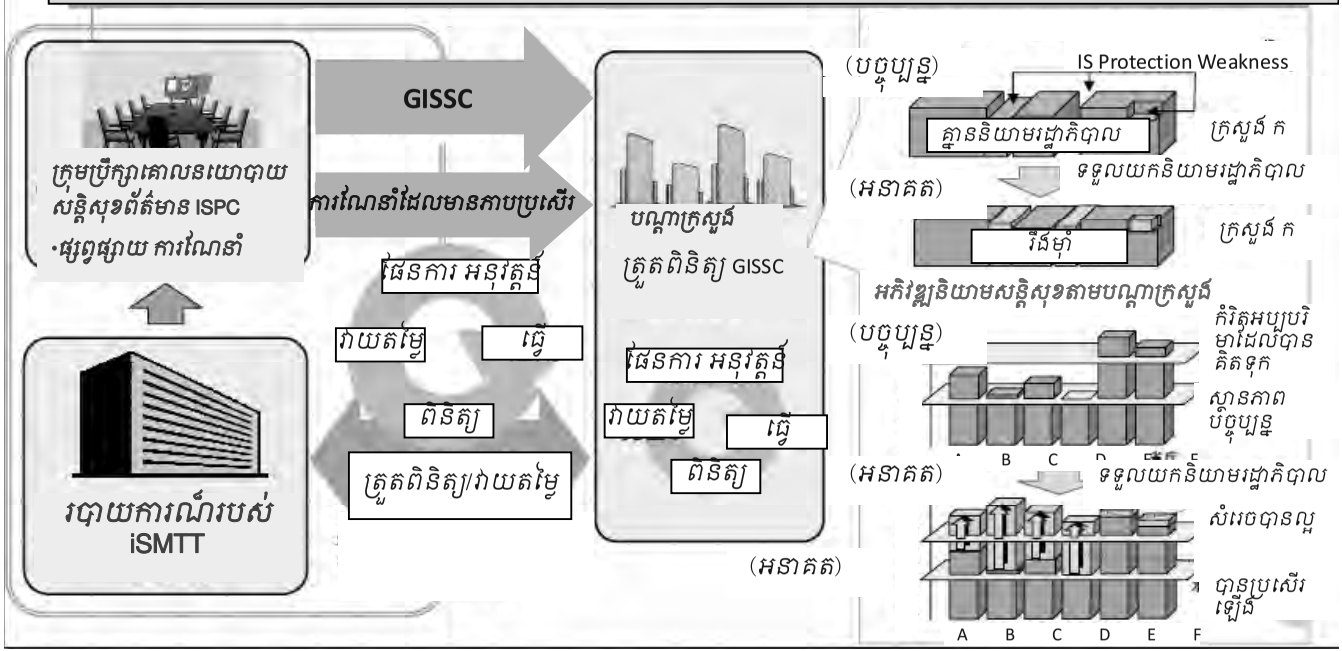
ជាវិធានមូលដ្ឋាន ដែលគ្រប់ក្រសួង-ស្ថាប័ន ត្រូវមានការទទួលខុសត្រូវ ក្នុងការរៀបចំ ផែនការ និងអនុវត្តនូវវិធានការសន្តិសុខព័ត៌មានដើម្បីជៀសវាងពីឧបទ្ទវហេតុណា មួយដែលអាចកើតឡើងក្នុងប្រព័ន្ធទំនាក់ទំនង និងព័ត៌មានរបស់ក្រសួង។ ដូច្នេះ ហើយរាជរដ្ឋាភិបាល នឹងផ្តល់នូវ គោលនយោបាយមូលដ្ឋានផង និង ផែនការរួម ដែលមានលក្ខណៈស្តង់ដាគំរូផង ធ្វើដូចនេះ ក្រសួង ស្ថាប័ន នៃរាជរដ្ឋាភិបាល អាចយកមក ធ្វើការអភិវឌ្ឍ និងធ្វើឲ្យការអនុវត្តសន្តិសុខព័ត៌មានរបស់ ពួកគេ កាន់តែប្រសើរឡើងយ៉ាងពិតប្រាកដ អាស្រ័យលើអាទិភាពរបស់គេ។


និយាមសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល
(បច្ចុប្បន្ន)
ភាពខ្សោយនៃប្រព័ន្ធការពារ
(អនាគត)
គ្មានកំរិតនិយាម
ក្រសួង ក
ចាប់យក កំរិតនិយាម
រាជរដ្ឋាភិបាល
មានភាពរឹងមាំ
ក្រសួង ខ

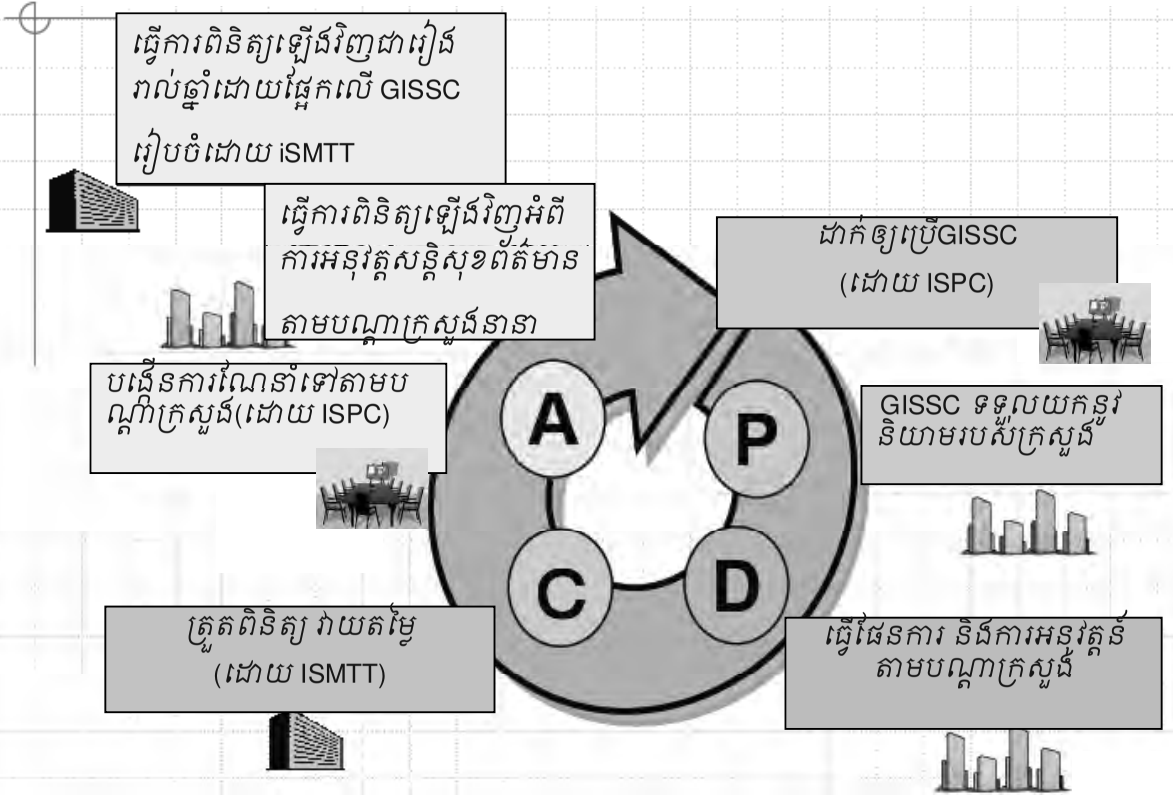

និយាមសន្តិសុខព័ត៌មាន បង្កើនការជឿជាក់ ក្នុងបណ្តាក្រសួង
(បច្ចុប្បន្ន)
(អនាគត)
កំរិតសន្តិសុខីព័ត៌មាន
កំរិតរំពឹងទុកជាអប្បរមា
ស្ថានភាពបច្ចុប្បន្ន
ទទួលលទ្ធផលខ្ពស់
ការបង្កើន
ចាប់យកកំរិតនិយាម
ក ខ គ ឃ ង ច
ក ខ គ ឃ ង ច

ការដាក់ឲ្យប្រើប្រាស់និយាមសន្តិសុខព័ត៌មានរាជរដ្ឋាភិបាល ជាបច្ចុប្បន្ន

- ក្រសួង និមួយៗត្រូវអនុវត្តផែនការទំនើប ដោយផ្អែកលើនិយាមសន្តិសុខព័ត៌មានគំរូរបស់រាជរដ្ឋាភិបាល(GISSC)
- ក្រុមការងារបច្ចេកទេសគ្រប់គ្រងកិច្ចការសន្តិសុខបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន(iSMTT) ធ្វើការត្រួតពិនិត្យ/ វាយតម្លៃអំពីប្រសិទ្ធភាពនៃការអនុវត្តន៍។ ក្រុមប្រឹក្សាជាតិនៃសន្តិសុខព័ត៌មាន(ISPC)ផ្សព្វផ្សាយនូវការណែនាំដែលមានភាពប្រសើរជាង យោងតាម របាយការណ៍របស់ iSMTT

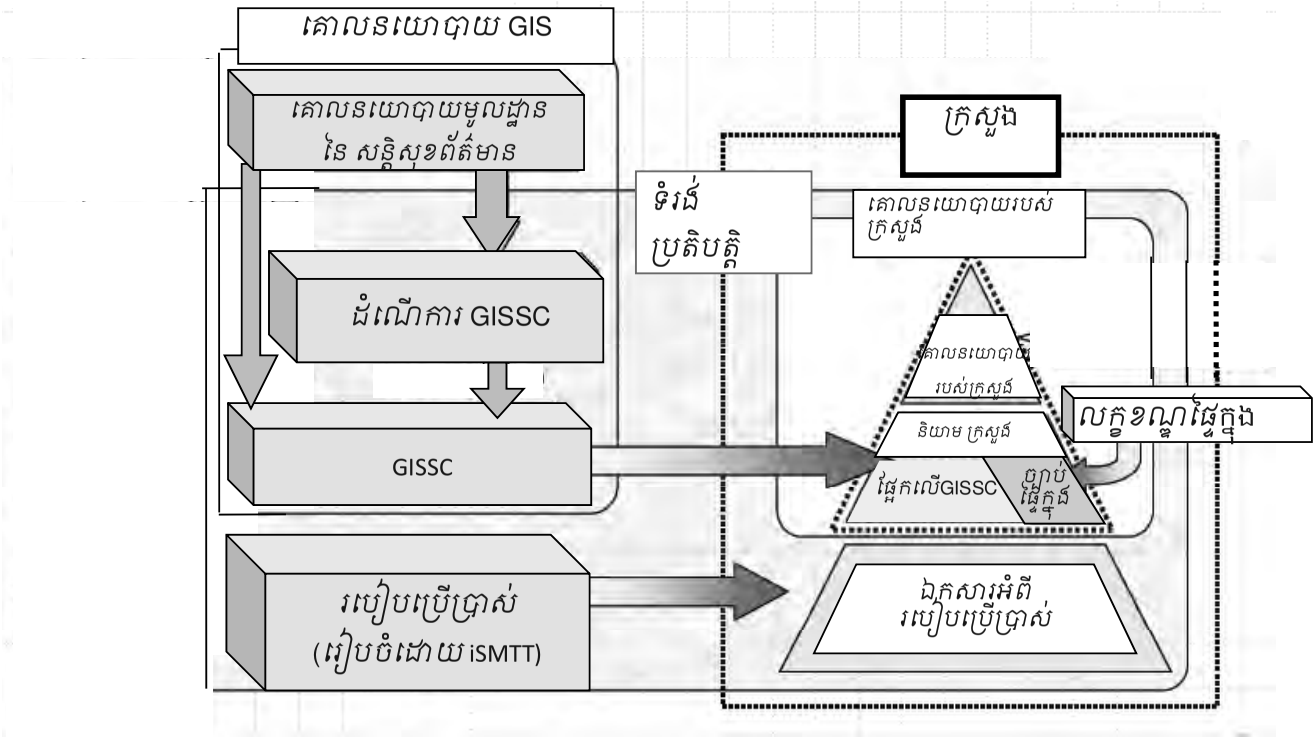


និតិវិធី (ផែនការ ធ្វើ ពិនិត្យ អនុវត្តន៍) PDCA

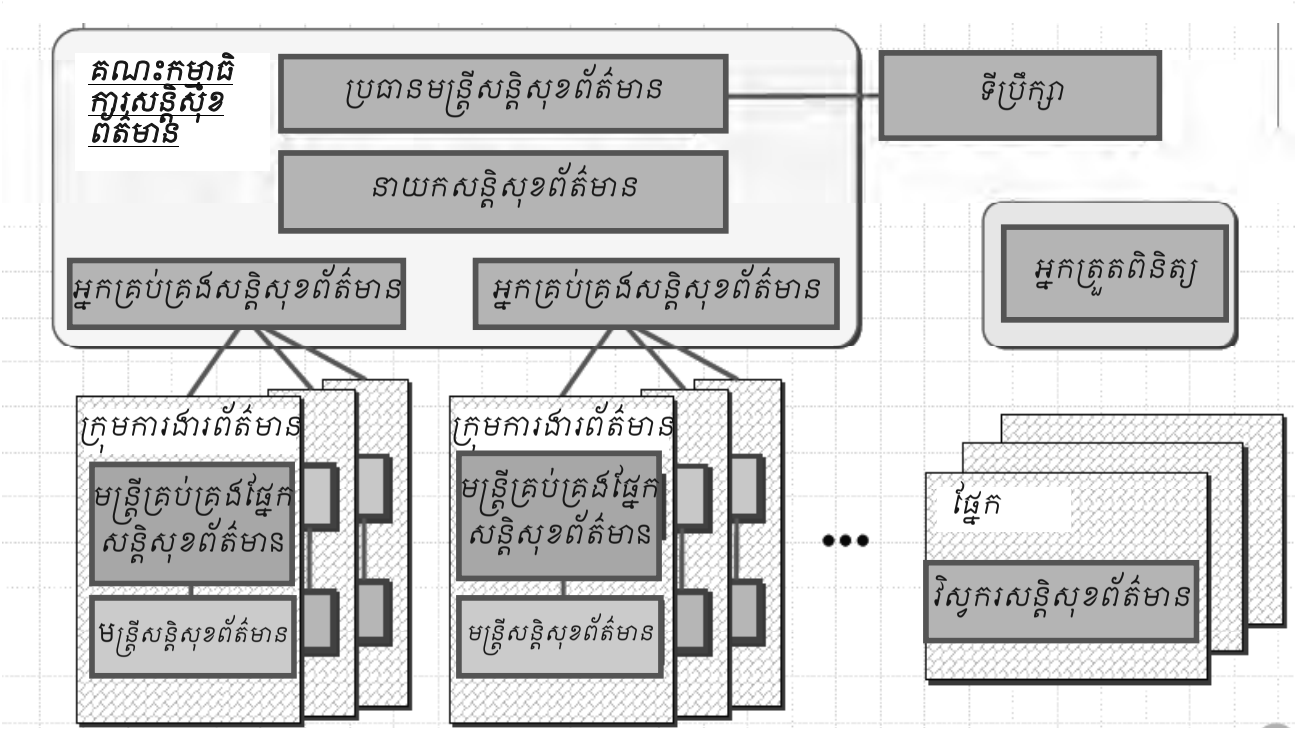


វិធានទូទៅ

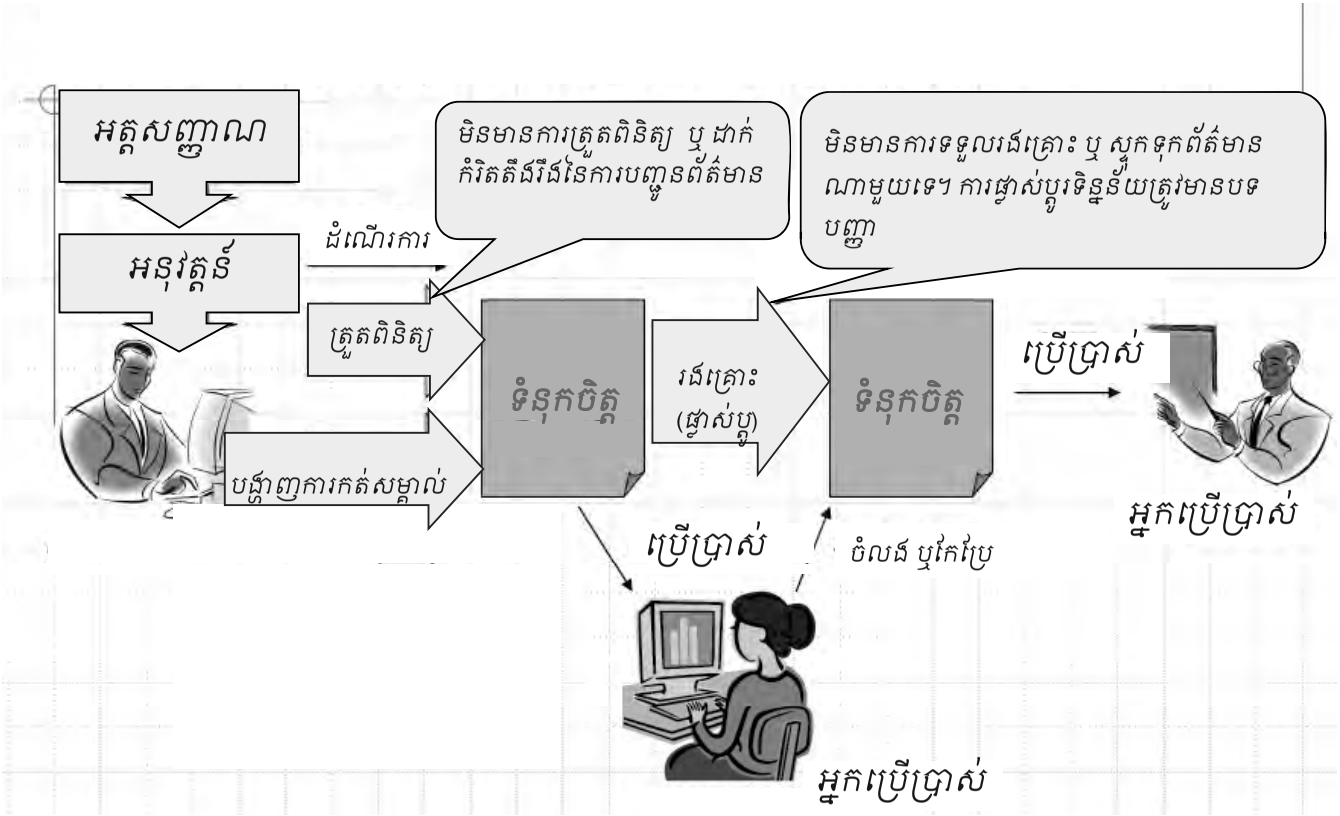
របៀបប្រើប្រាស់ GISSC



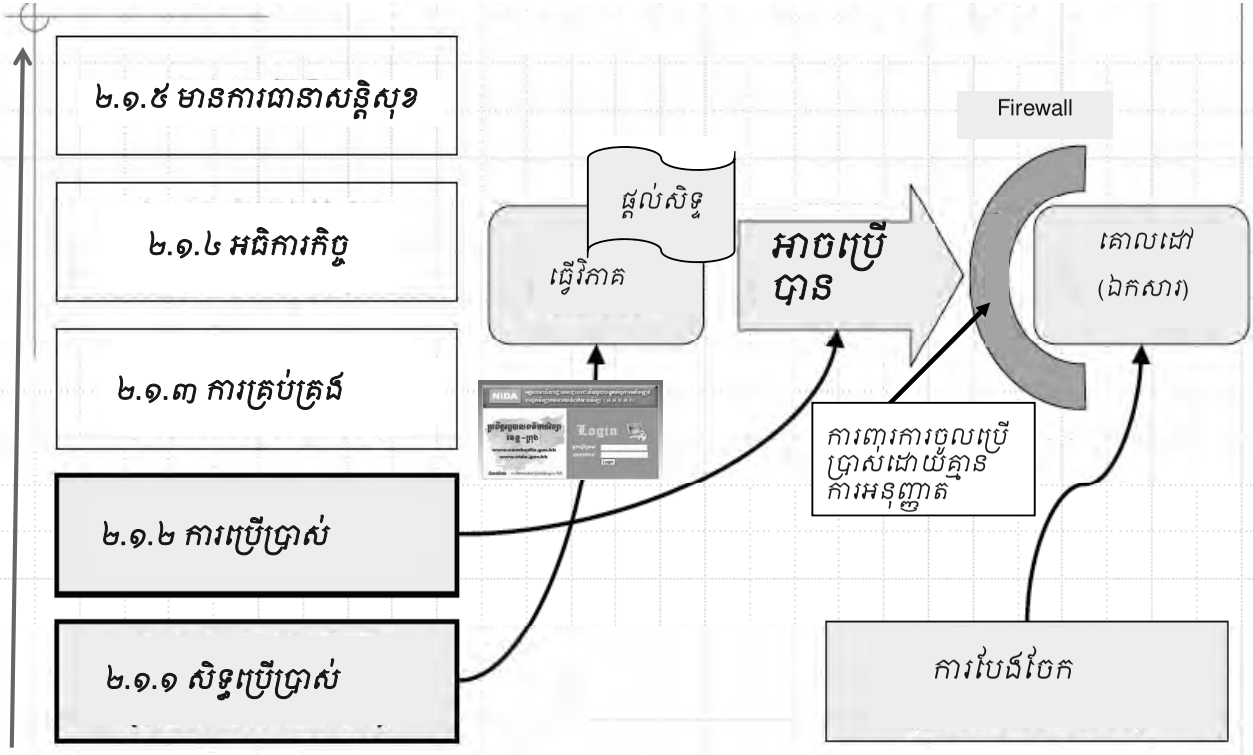
ការគ្រប់គ្រង និងភាពទទួលខុសត្រូវ



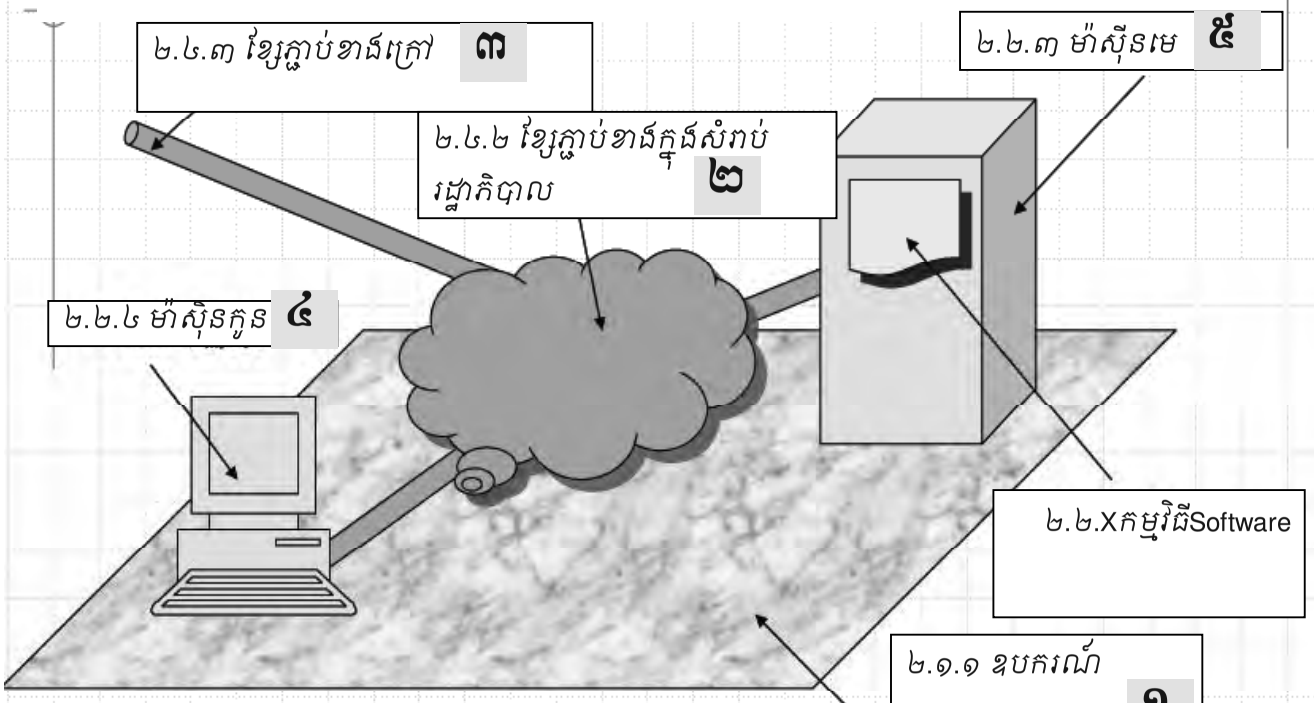
ការកំណត់ប្រភេទព័ត៌មាន



២.១ អនុវត្ត លើការកំណត់សន្តិសុខព័ត៌មាន តាមការចាំបាច់



ជាតុផ្សំទាំងប្រាំនៃ GISSC



ឯកឧត្តម ជា មានិត

manit_chea@nida.gov.kh
www.nida.gov.kh
HP : 089 68 61 68
Fax: 023 21 80 43

សូមអរគុណ

NiDA

JICA

គោលនយោបាយមូលដ្ឋាន នៃសន្តិសុខព័ត៌មាន របស់រដ្ឋាភិបាល

០១ - តុលា - ២០០៩

- ឯកឧត្តម **ជា មានិត** អគ្គលេខាធិការរង នៃ អគ្គលេខាធិការដ្ឋាន អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍វិស័យបច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា ប្រធានក្រុមការងារបច្ចេកទេសគ្រប់គ្រង កិច្ចការសន្តិសុខ បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន (iSMTT)
- លោក **ស៊ីណូរី គុរ៉ាដ៊ី** ជំនាញការ របស់ទីភ្នាក់ងារសហប្រតិបត្តិការអន្តរជាតិនៃប្រទេសជប៉ុន

ច្បាប់

NiDA

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានវិទ្យារបស់រាជរដ្ឋាភិបាល

jICA

១. ហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន (ICT) របស់រដ្ឋាភិបាល នៅក្នុងពិភពលោកនេះកំពុងជួបប្រទះនូវការគំរាមកំហែងផ្នែកសន្តិសុខព័ត៌មាន ដែលអាចបង្កនូវការខូចខាតធ្ងន់ធ្ងរដល់ទិន្នន័យព័ត៌មានវិទ្យា របស់រដ្ឋាភិបាល។ ខាងក្រោមនេះ ត្រូវបានចាត់ទុកថាជាឧក្រិដ្ឋជន អ៊ិនធឺណិត ៖

- Cyber Terrorist ជាជនដែលមានជំនាញ និងបណ្តាញចាត់តាំង ដែលអាចនឹងមានចេតនាផ្នែកនយោបាយ។
- Hacker ជាជនជំនាញ ដែលស្វែងរកការសប្បាយតាមរយៈការរំខានដល់សាធារណជន។
- Cyber Thieves, Fraud គោលបំណងរបស់ពួកគេ គឺដើម្បីរកលុយ។

ការធ្វើការវាយប្រហាហេដ្ឋារចនាសម្ព័ន្ធ ICT របស់រដ្ឋាភិបាល ដើម្បីកាត់ផ្តាច់សេវាតាមប្រព័ន្ធអ៊ិនធឺណិតរបស់រដ្ឋាភិបាល E-Government Service ដើម្បីលួចបំផ្លាញព័ត៌មានដែលមានតម្លៃ ឬមូលដ្ឋានទិន្នន័យសម្ងាត់របស់រដ្ឋ។

គោលដៅរបស់ពួកគេ គឺអាចសំដៅទៅលើហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មានជាតិ ដូចជាសេវាអ៊ិនធឺណិត ក្នុងគោលបំណងបង្កការរំខានដល់ជីវិតរស់នៅរបស់សាធារណៈជន។

២. រដ្ឋាភិបាលអាចជួបប្រទះនូវវិបត្តិ ប្រសិនបើព័ត៌មានសំខាន់ៗនៅក្នុងហេដ្ឋារចនាសម្ព័ន្ធរបស់រដ្ឋាភិបាលត្រូវបានពួកគេធ្វើឲ្យលេចឮទៅខាងក្រៅ ឬអាចផ្លាស់ប្តូរបាននោះ។

ដូច្នេះជាការសំខាន់បំផុត ដែលរដ្ឋាភិបាលត្រូវរៀបចំផែនការការពារសន្តិសុខព័ត៌មាន និងអនុវត្តនូវផែនការនោះ។

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានវិទ្យារបស់រាជរដ្ឋាភិបាល

- គោលនយោបាយជាមូលដ្ឋាន -

ដោយផ្អែកលើបរិយាកាសគំរាមកំហែងផ្នែកសន្តិសុខព័ត៌មាននាពេលបច្ចុប្បន្នរាជរដ្ឋាភិបាលនឹងណែនាំអោយមានការប្រើប្រាស់នូវដំណោះស្រាយដ៏ទូលំទូលាយនិងខ្លាំងក្លាសម្រាប់ការការពារសន្តិសុខព័ត៌មាន នៅតាមបណ្តា ក្រសួងនិងស្ថាប័នទាំងអស់ក្នុងកម្រិតដែលមាន គុណភាពរួម ។ ដើម្បីបង្កើតនូវដំណោះស្រាយរួមដ៏ខ្លាំងក្លានោះ លក្ខណៈ វិនិច្ឆ័យនិយាម សន្តិសុខ ព័ត៌មាន (គោលការណ៍ណែនាំ) ត្រូវបានបង្កើតឡើង ។ ក្រសួងនិងទីភ្នាក់ងារទាំងអស់ មានការកិច្ចទទួលខុសត្រូវក្នុងការបង្កើតដំណោះស្រាយ សន្តិសុខព័ត៌មាន សម្រាប់ប្រព័ន្ធICT របស់ខ្លួន ស្របទៅតាម គោលការណ៍ណែនាំនៃលក្ខណ វិនិច្ឆ័យ និយាម ។ ជាមួយគ្នានេះ ការថែរក្សាសេវាពរដ្ឋាភិបាលប្រឆាំងនឹងបញ្ហាជុំវិញការគំរាម កំហែងផ្នែកសន្តិសុខព័ត៌មានដែលប្រែប្រួលរៀងរាល់ថ្ងៃ អោយមានគុណភាពល្អនិងស្ថេរភាព ក៏ជាកត្តាមួយដ៏សំខាន់ផងដែរ ។ ដូច្នេះ លក្ខណវិនិច្ឆ័យនិយាម គួរត្រូវធ្វើការពិនិត្យឡើងវិញជារៀងរាល់ឆ្នាំ ។

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានវិទ្យារបស់រាជរដ្ឋាភិបាល

(១)ការបង្កើតលក្ខណៈវិនិច្ឆ័យនិយាមស្តីពីសន្តិសុខព័ត៌មានវិទ្យារបស់រាជរដ្ឋាភិបាល

រាល់ក្រសួងទាំងអស់ ត្រូវទទួលខុសត្រូវចំពោះការអភិវឌ្ឍប្រព័ន្ធ ICT របស់ខ្លួន ដែលរួមទាំងការអនុវត្តនូវ ដំណោះស្រាយការពារប្រព័ន្ធសន្តិសុខព័ត៌មាន ស្របតាមគោលការណ៍ណែនាំទូទៅរបស់រាជរដ្ឋាភិបាលផងដែរ ។ មជ្ឈមណ្ឌល គ្រប់គ្រងសន្តិសុខព័ត៌មាន ត្រូវមានការកិច្ចក្នុងការបង្កើត និងពង្រឹងការអនុវត្តគោលការណ៍ណែនាំ ទាំងនេះ ។ គោលការណ៍ណែនាំនេះ ត្រូវបានហៅថាជា លក្ខណៈវិនិច្ឆ័យនិយាមសន្តិសុខព័ត៌មានរបស់រាជរដ្ឋាភិបាល ដែល ត្រូវបានពិនិត្យឡើងវិញជារៀងរាល់ឆ្នាំ ដើម្បីសម្របទៅតាមការផ្លាស់ប្តូរឥតឈប់ឈរនៃការគំរាមកំហែងផ្នែកសន្តិសុខ ព័ត៌មាន។

លក្ខណៈវិនិច្ឆ័យនិយាមនេះ រួមបញ្ចូលនូវសកម្មភាពមួយចំនួនដូចខាងក្រោម ៖

- *រចនាសម្ព័ន្ធចាត់តាំង ទទួលខុសត្រូវផ្នែករដ្ឋបាល និងអធិការកិច្ច*
- *ការវាយតម្លៃទៅលើធនធានព័ត៌មាន*
- *ការពិចារណាអំពីការការពារសន្តិសុខព័ត៌មាន សម្រាប់ប្រព័ន្ធកម្មវិធីកុំព្យូទ័រគ្រប់ប្រភេទ*
- *ការពិចារណាអំពីការការពារសន្តិសុខព័ត៌មានសម្រាប់ម៉ាស៊ីនកុំព្យូទ័រមេ និងកុំព្យូទ័ររបស់អ្នកប្រើប្រាស់*
- *ការពិចារណាអំពីការការពារសន្តិសុខព័ត៌មានសម្រាប់ហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញទាំងអស់*
- *លក្ខខណ្ឌ ដែលតម្រូវឲ្យអនុវត្តចំពោះមុខងារសន្តិសុខព័ត៌មានទាំងអស់*
- *ការគ្រប់គ្រងលើការប្រើប្រាស់ ការផ្តល់សិទ្ធ ការបំលែងទិន្នន័យ រក្សាសុវត្ថិភាព ឧបករណ៍ និងសម្ភារៈសម្រាប់ប្រើប្រាស់អ៊ិនធឺណិត (ដូចជា បណ្តាញ ម៉ាស៊ីនមេ សារអេឡិចត្រូនិច DNS, Web, Firewall...)*

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានវិទ្យារបស់រាជរដ្ឋាភិបាល

(២) ការពិនិត្យឡើងវិញអំពីគោលនយោបាយសន្តិសុខព័ត៌មានរបស់ក្រសួង

- គ្រប់ក្រសួង ទាំងអស់ មានការកិច្ចទទួលខុសត្រូវក្នុងការអភិវឌ្ឍ និងថែរក្សាប្រព័ន្ធ ICT របស់ខ្លួនជាការចាំបាច់ និងត្រូវបង្កើតគោលនយោបាយ ផែនការសន្តិសុខព័ត៌មានរបស់ពួកគេ ស្របតាមគោល-ការណ៍ណែនាំរបស់ GISSC ។ ការអនុវត្តខ្ជាប់ខ្ជួននូវគោលនយោបាយ និងផែនការសន្តិសុខព័ត៌មាន គឺជាកត្តាដ៏សំខាន់ ។

(៣) ការធ្វើអធិការកិច្ចដោយខ្លួនឯង

- គ្រប់ក្រសួងទាំងអស់ ត្រូវបានតម្រូវអោយធ្វើការត្រួតពិនិត្យលើប្រព័ន្ធ ICT អោយបានទៀងទាត់ជារៀងរាល់ឆ្នាំស្របទៅតាម GISSC។ ប្រសិនបើរកឃើញចំណុចខ្វះខាតណាមួយនោះ ចូរធ្វើការកែប្រែ ។

(៤) ការអនុវត្តនូវវដ្ត "ផែនការ-ធ្វើ -ពិនិត្យ-អនុវត្តន៍" ឬ PDCA Cycle

- មជ្ឈមណ្ឌលគ្រប់គ្រងសន្តិសុខព័ត៌មានត្រូវពិនិត្យឡើងវិញនូវរបាយការណ៍អធិការកិច្ចរបស់ក្រសួង ដើម្បីពិនិត្យថាតើក្រសួងទាំងនោះ បានអនុវត្តខ្ជាប់ខ្ជួនតាមលក្ខណៈវិនិច្ឆ័យ GISSC ដែរឬទេ ។ ប្រសិនបើរកឃើញ ភាពមិនស៊ីសង្វាក់គ្នា ចាំបាច់ត្រូវផ្តល់ការណែនាំអោយធ្វើការ កែតម្រូវភ្លាម ។

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានវិទ្យារបស់រាជរដ្ឋាភិបាល

(៥)ការផ្សព្វផ្សាយ វិធីសាស្ត្របន្ថែម ដើម្បីគាំទ្រដល់ស្តេរកាពសន្តិសុខព័ត៌មាន

- ជាការចាំបាច់ណាស់ដែលតម្រូវឲ្យមានវិញ្ញាបនបត្របញ្ជាក់អំពីសន្តិសុខព័ត៌មាន រាល់ពេលដែលរដ្ឋាភិបាលបានជាវធនធាន ICT ដូចជា Router, Switch, Firewall ជួលអ្នកពិគ្រោះយោបល់ ឬបង្កើតកម្មវិធី ICT ។ ជាការចាំបាច់ដែលតម្រូវឲ្យផ្តល់ការត្រួតពិនិត្យលើ Software ដើម្បីរក្សារបានទៅ គោលនយោបាយសន្តិសុខព័ត៌មាន និង ដំណើរការគ្រប់គ្រងមានកំរិតដូចគ្នា ។

(៦) ការផ្សព្វផ្សាយសន្តិសុខព័ត៌មាន ដល់ក្នាក់ងារក្រៅរដ្ឋាភិបាល

- វាជាការចាំបាច់ណាស់ ដែលក្នាក់ងារក្រៅរដ្ឋាភិបាលទាំងអស់ត្រូវរក្សាកម្រិតនៃដំណើរ ការគ្រប់គ្រង សន្តិសុខព័ត៌មានស្របតាម GISSC ។

(៧) ផែនការសម្របសម្រួលនៅតាមបណ្តាមជ្ឈមណ្ឌលគ្រប់គ្រងសន្តិសុខព័ត៌មាន (IS) និងបណ្តាក្រសួងនានា គួរត្រូវបង្កើតឡើងនៅពេលជួបប្រទះចំណុចខ្វះខាតថ្មីក្នុងSoftware ។

- មជ្ឈមណ្ឌលគ្រប់គ្រងនេះ គួរតែមានការប្រាស្រ័យទាក់ទងល្អជាមួយបណ្តាក្រសួងទាំងអស់ ជាពិសេសជាមួយ បណ្តាក្រសួងដែលគ្រប់គ្រងលើហេដ្ឋារចនាសម្ព័ន្ធ ICT សំខាន់ៗ និងផ្ទាស់ប្តូរព័ត៌មានទាក់ទងទៅនឹងលទ្ធផលនៃការស្រាវជ្រាវ រកឃើញ និងការរិភាគអំពីចំណុចខ្វះខាតរបស់Software ។ នៅពេលដែលរកឃើញ គួរតែធ្វើការសិក្សា អំពី នីតិវិធីការពារ ហើយធ្វើជាសំណើទៅកាន់គ្រប់បណ្តាក្រសួងទាំងអស់ ។

លក្ខណៈវិនិច្ឆ័យនៃនិយាមសន្តិសុខព័ត៌មានវិទ្យារបស់រាជរដ្ឋាភិបាល

(៨) ផែនការអភិវឌ្ឍន៍ធនធានមនុស្សផ្នែកសន្តិសុខព័ត៌មាន

- *បច្ចុប្បន្នរដ្ឋាភិបាល មានចំនួនវិស្វករសន្តិសុខព័ត៌មានមិនទាន់គ្រប់គ្រាន់ព្រមទាំងកង្វះខាត ផ្នែក បច្ចេកទេស ដើម្បីអនុវត្តផែនការគ្រប់គ្រងសន្តិសុខ ព័ត៌មានតាមសេចក្តីត្រូវការនៅឡើយ។ មជ្ឈមណ្ឌលគ្រប់គ្រងនេះ គួររៀបចំផែនការសម្រាប់កម្មវិធីអប់រំធនធានចាំបាច់សំរាប់បម្រើការងារមជ្ឈមណ្ឌលគ្រប់គ្រងតម្រូវអោយមានធ្វើការផ្សព្វផ្សាយគោលការណ៍ណែនាំ ស្តីពី ការអភិវឌ្ឍ Software ទាក់ទងនឹងការការពារសន្តិសុខព័ត៌មានទៅតាមបណ្តាក្រសួងនានា ។*

(៩) ការបន្ថែមផែនការរយៈពេលមធ្យមនៅក្នុងរដ្ឋាភិបាល

- *មជ្ឈមណ្ឌលគ្រប់គ្រង គួររៀបចំបង្កើតក្រុមផ្សេងៗនៅក្នុងរដ្ឋាភិបាលដើម្បីធ្វើយតបទៅនឹងឧប្បត្តិហេតុសន្តិសុខព័ត៌មាន ដែលអាចកើតមានឡើងជាយថាហេតុ ។ វាចាំបាច់ណាស់ដែលត្រូវបង្កើត នូវគោលការណ៍ណែនាំរបស់ រដ្ឋាភិបាលស្តីពីលក្ខខណ្ឌតម្រូវរួមគ្នាផ្នែក សន្តិសុខព័ត៌មាន ។ បេសកកម្មមួយទៀតរបស់មជ្ឈមណ្ឌលគ្រប់គ្រង គឺរាល់សន្តិសុខ ព័ត៌មានដែលទាក់ទងនឹងកិច្ចសហប្រតិបត្តិការក្នុងក្របខណ្ឌរដ្ឋាភិបាល ។*

ឯកឧត្តម ជា មានិត

manit_chea@nida.gov.kh
www.nida.gov.kh
HP : 089 68 61 68
Fax: 023 21 80 43

សូមអរគុណ

NiDA

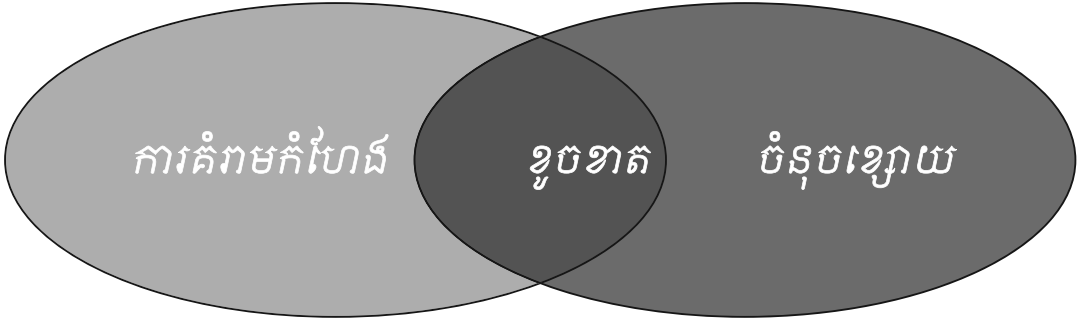
JICA

ការគំរាមកំហែងចំបងទាំង១០ ចំពោះសន្តិសុខព័ត៌មាន

๐๑ តុលា ๒๐๐๙

- ឯកឧត្តម **ជា មានិត** អគ្គលេខាធិការរង នៃ អគ្គលេខាធិការដ្ឋាន អាជ្ញាធរជាតិទទួលបន្ទុកកិច្ចការអភិវឌ្ឍន៍វិស័យបច្ចេកវិទ្យា គមនាគមន៍ ព័ត៌មានវិទ្យា ប្រធានក្រុមការងារបច្ចេកទេសគ្រប់គ្រង កិច្ចការសន្តិសុខ បច្ចេកវិទ្យា គមនាគមន៍ និងព័ត៌មាន (iSMTT)
- លោក **ស៊ីណូរី គុរ៉ាដឺ** ជំនាញការ របស់ទីភ្នាក់ងារសហប្រតិបត្តិការអន្តរជាតិនៃប្រទេសជប៉ុន

អ្វីទៅជាការគំរាមកំហែងសន្តិសុខព័ត៌មាន ហើយវាកើតឡើងដោយរបៀបណា?



ការគំរាមកំហែង X ចំនុចខ្សោយ = ខូចខាត

កុំព្យូទ័រឆ្លងមេរោគ X គ្មានកម្មវិធីកំចាត់មេរោគ= បាត់បង់ទិន្នន័យ

១.ការគំរាមកំហែងរបស់ DNS Poisoning

អ្នកប្រើប្រាស់

DNS Server

~~example.com.kh~~

example.com.kh

កែIP address

អ្នកវាយប្រហា

Example.com.kh
ដែលត្រឹមត្រូវ

abc@example.com.kh

Example.com.kh
ដែលបានកែ

បើព័ត៌មាននៅលើDNS Serverឬ Web page ត្រូវបានដាក់ជំនួយដោយព័ត៌មានក្លែងបន្ទំ អ្នកអាចនិងទៅកាន់ email ឬក៏website ក្លែងបន្ទំនោះបើទោះបីជាបញ្ចូល addressត្រឹមត្រូវក៏ដោយ

២.ការគំរាមកំហែងដែលស្គាល់គោលដៅវាយប្រហារច្បាស់

៣.ការធ្វើឲ្យលេចធ្មៃព័ត៌មានទៅខាងក្រៅ

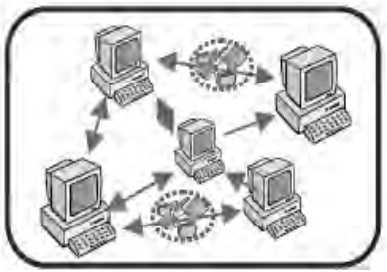
បាត់បង់ ឬត្រូវចោលួច

បាត់បង់ ឬត្រូវចោលួចនូវឯកសារ

មេរោគ

បញ្ជូនសារទៅខុសអាស័យដ្ឋាន

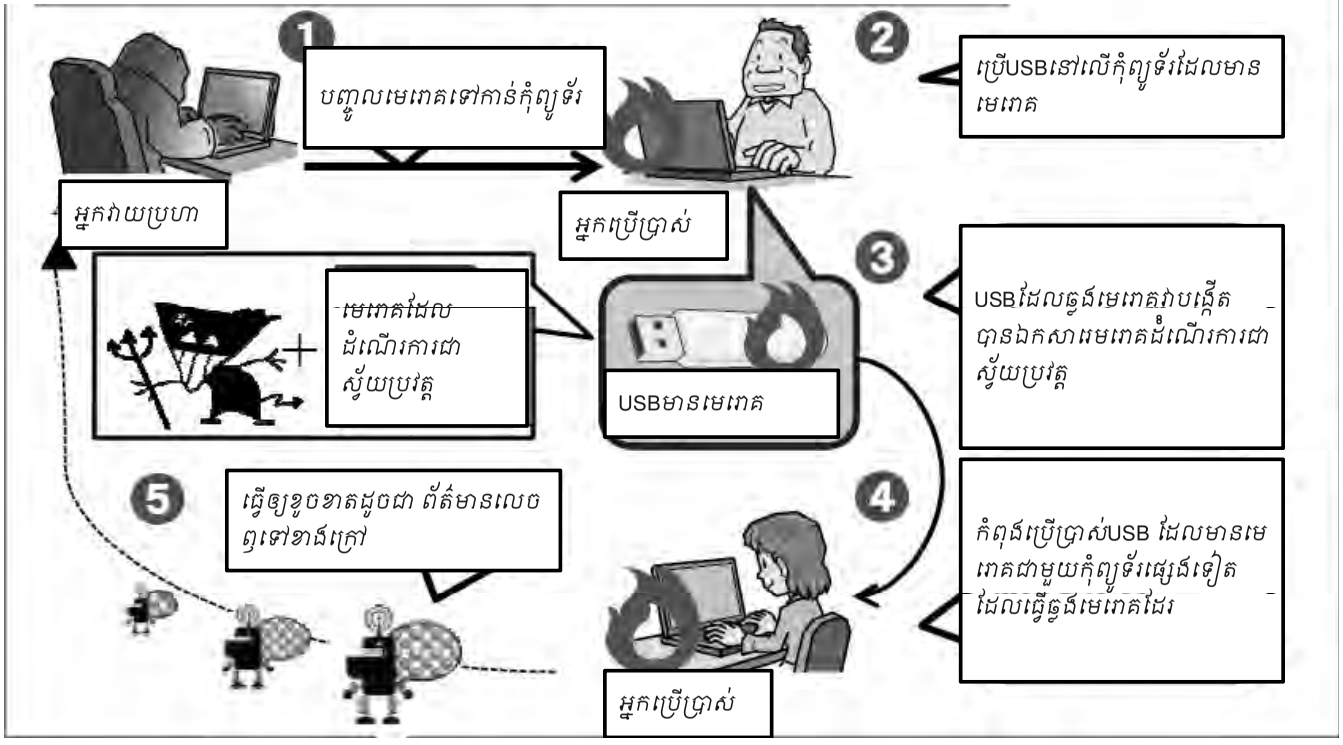
អ្នកបន្ទំនៅខាងក្នុង



កម្មវិធីលួចឯកសារ

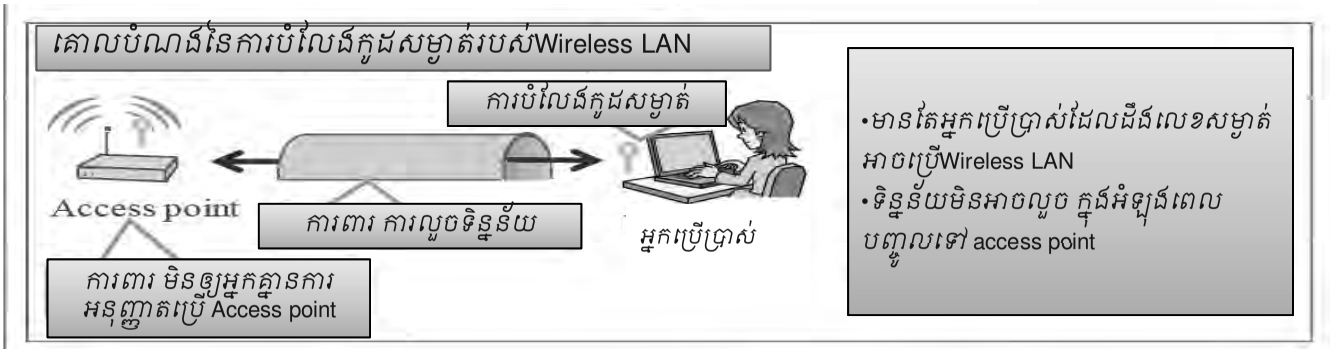
៤.របៀបផ្សេងៗដែលកុំព្យូទ័រឆ្លងមេរោគ

ឧទាហរណ៍នៃការឆ្លងមេរោគតាមរយៈការប្រើឧបករណ៍ផ្ទុកទិន្នន័យ(USB)

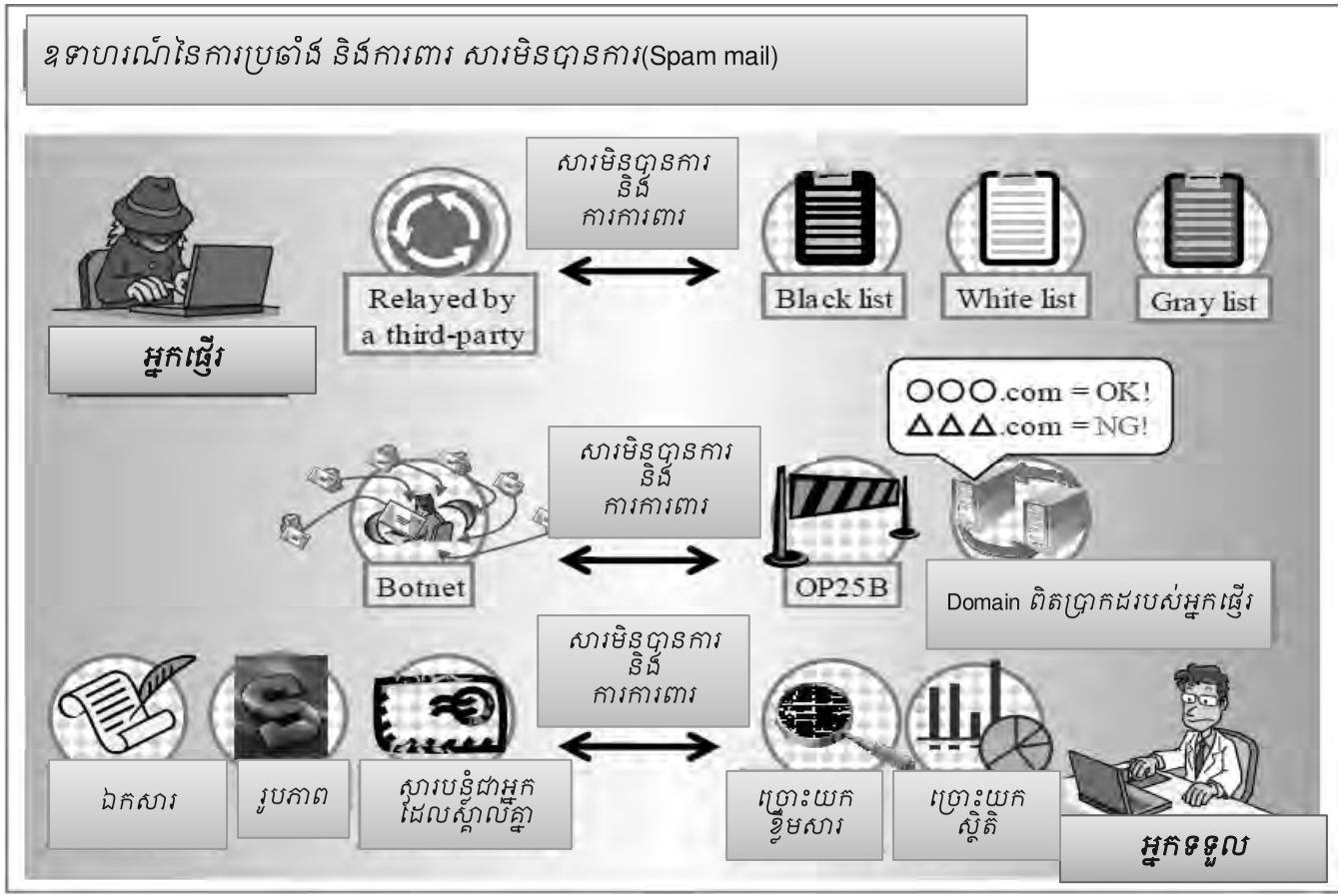


៥.ការគំរាមកំហែងកុំពុងតែកើនឡើងទៅលើចំនុចខ្សោយរបស់ Wireless LAN

ចំនុចខ្សោយនៃវិធីសាស្ត្របំលែងកូដសម្ងាត់របស់Wireless LAN

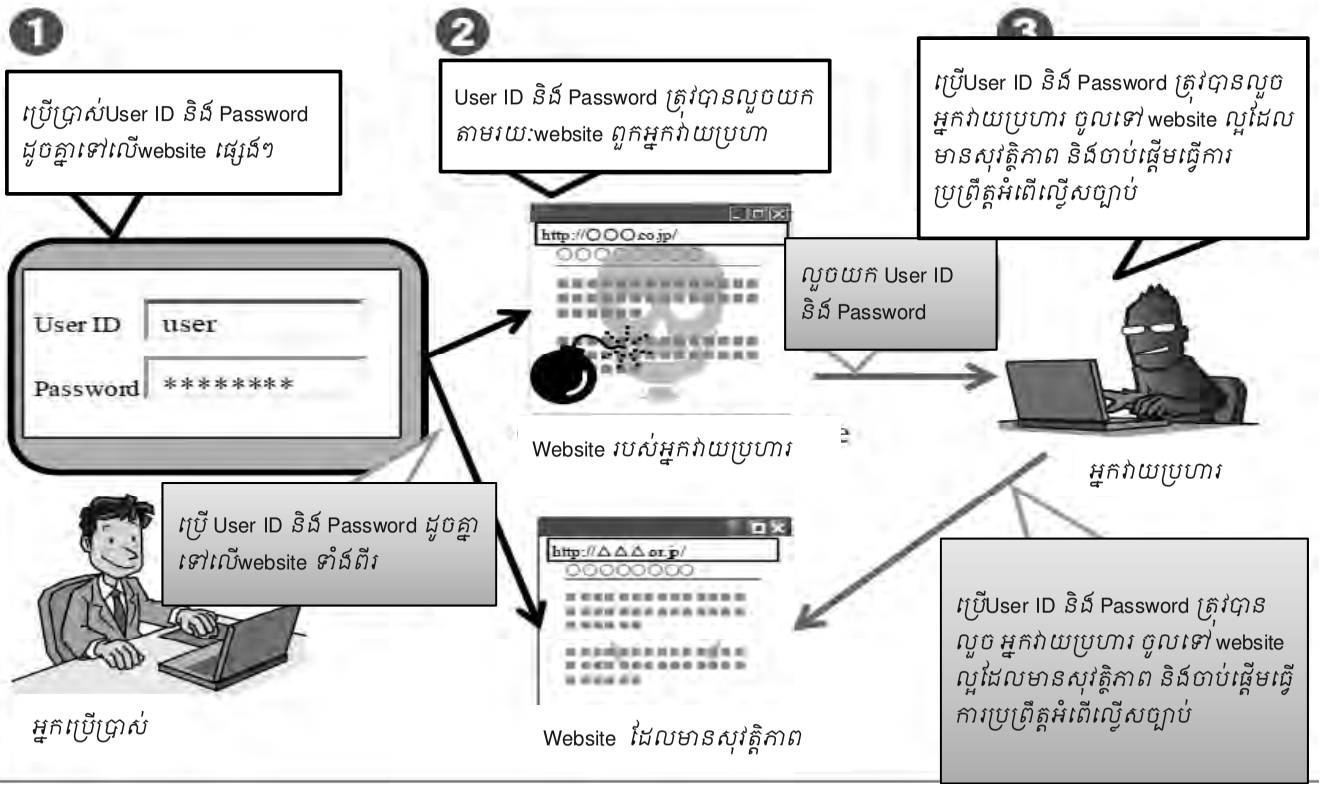


៦.ការកើនឡើងមិនឈប់ឈរនៃសារមិនបានការ(Spam mail)



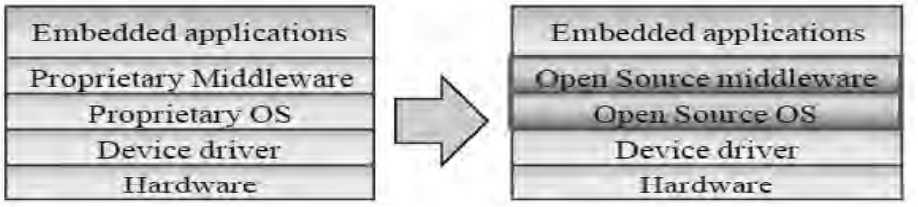
៧.ការគំរាមកំហែងកុំពុងកើនឡើងចំពោះការប្រើប្រាស់User ID និង Password ដូចគ្នា

ការគំរាមកំហែងកុំពុងកើនឡើងចំពោះការប្រើប្រាស់User ID និង Password ដូចគ្នាទៅលើwebsite ផ្សេងៗ



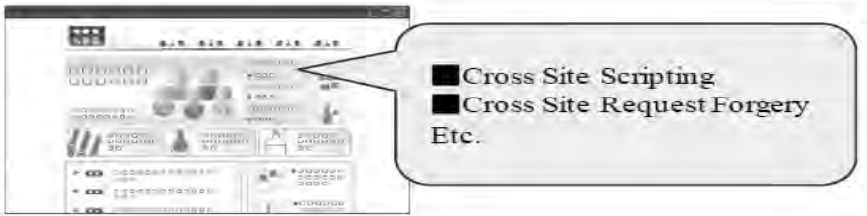
៨.ចំណុចខ្សោយក្នុងប្រព័ន្ធបង្កប់

ចំណុចខ្សោយក្នុងប្រព័ន្ធ និងឧបករណ៍



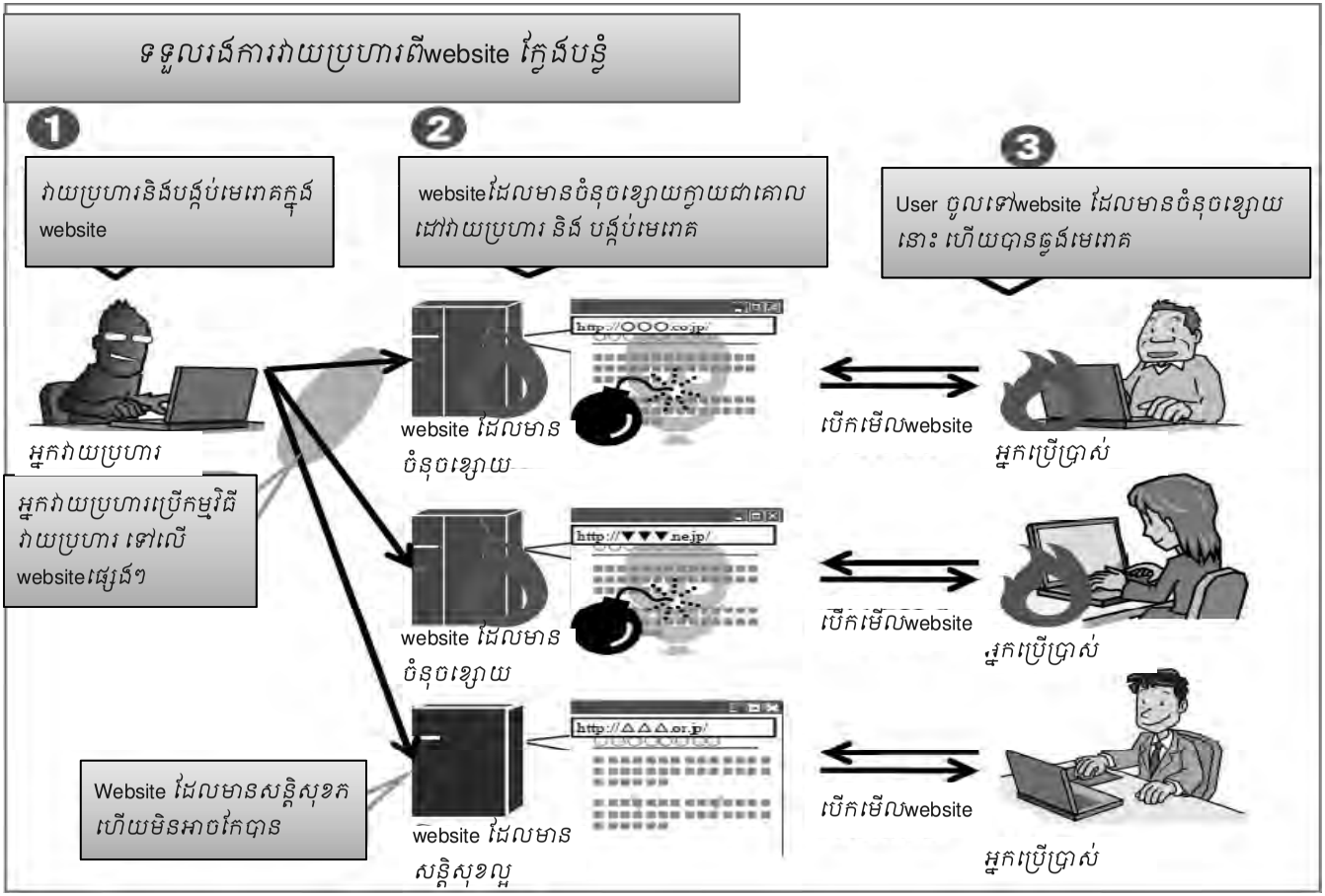
1. ប្រព័ន្ធដែលបង្កប់មានប្រើក្នុងកូដបើកចំហរ middleware និងប្រព័ន្ធប្រត្តិការ និងកុំព្យូទ័រ

2. ឧបករណ៍ និងប្រព័ន្ធបង្កប់ទាំងនេះ វាមានចំនុចខ្សោយដូចនិងកុំព្យូទ័រដែរ



3. ឧទហរណ៍Web Function ដែលមានប្រព័ន្ធបង្កប់ ត្រូវបានរកឃើញថាមានចំនុចខ្សោយដូចកុំព្យូទ័រដែរ

៩.ការវាយប្រហារតាមរយៈwebsite ត្រឹមត្រូវ



១០.លក្ខណៈនៃការវាយប្រហារ