



# இலங்கையின் தகவல் மற்றும் சைபர் பாதுகாப்பு உபாயங்கள் 2018 - 2023



## முகவுரை

உலகெங்கிலும் டிஜிட்டல் தொழில்நுட்பமானது ஒரு சக்திமிக்க பொருளாதார கருவியாக மாறியுள்ளது. இது பொது மக்களின் வாழ்கை தரத்தை மேம்படுத்தியுள்ளது. தொழில் துறை மற்றும் பொதுமக்கள் ஆகியோரை இணைக்கும் கருவியாக இது மாறியுள்ளது. அத்துடன் தகவல் மற்றும் சேவைகளை பெற்றுக்கொள்ளும் ஊடகமாகவும் இருக்கின்றது. இன்று சமூகங்கள் டிஜிட்டல் தொழில்நுட்பத்தை சார்ந்து இருக்கின்றன.

டிஜிட்டல் தொழில் நுட்பமானது பல எண்ணற்ற நன்மைகளை கொண்டு வருவதுடன் பல இணைய அச்சுறுத்தல்களையும் கொண்டு வருகின்றது. 2015 ஆண்டு உலகளவில் பதிவு செய்யப்பட்ட இணைய பாதுகாப்பு நிகழ்வுகளின் எண்ணிக்கை, 59.06 மில்லியன்கள் ஆகும் என மதிப்பிடப்பட்டுள்ளது. ஒரு ஆய்வின்படி 2019 ம் ஆண்டு ஆகும் போது 2.1 டிரில்யன் டொலர் இதற்றாக செலவிடப்படும் என மதிப்பிடப்பட்டுள்ளது. 2015 ஆண்டுடன் ஒப்பிடுகின்ற போது இது நான்கு மடங்கு அதிகமாகும் 2010 ம் ஆண்டு தொடக்கம் 2017 வரை இது கணிசமான அளவு அதிகரித்துள்ளதை நாம் அவதானிக்கலாம்.

இந்த சூழலில் இலங்கையில் முதல் தகவல் சைபர் பாதுகாப்பு மூலோபாயத்தை அறிமுகப்படுத்தி நாட்டை சைபர் ஆபத்துக்களில் இருந்து பாதுகாப்புடன் வைத்திருப்பதற்கு சைபர் பாதுகாப்பு திட்டம் அமுல் படுத்தப்படுகின்றது. இந்த திட்டமானது எதிர்வரும் 2018 தொடக்கம் 2023 வரை ஐந்து ஆண்டுகளுக்கு அமுல்படுத்தப்படுகின்றது. இதன் நம்பகமான இணைய

பாதுகாப்பு சூழலை ஏற்படுத்தி டிஜிட்டல் பாதுகாப்பின் நன்மைகளை பொது மக்களுக்கு வழங்குவதே ஆகும்.. இந்த செயற்பாடுகள் முக்கியமான 5 பிரிவுகளை கொண்டு இருக்கும்

1. தேசிய தகவல்கள் மற்றும் இணைய பாதுகாப்பு மூலோபாயம் தொடர்பான விடயங்களை அமுல்படுத்துவதற்கு அரசாங்கத்தின் மூலமான செயற்திட்டம் ஒன்றை உருவாக்குதல்.
2. சட்டங்களையும் கொள்கைகளையும் உருவாக்கி தரமானதும் ஒழுங்குபடுத்தப்பட்டதுமான சூழலை உருவாக்கி சைபர் தாக்குதல்களில் இருந்த பொது மக்களையும் நிறுவனங்களையும் பாதுகாப்பதே எங்களது நோக்கமாகும்.
3. இணைய தாக்குதலில் இருந்து பாதுகாப்பதற்காவும் அதனை தடுப்பதற்காகவும் சரியான முறையில் செயற்படுவதற்காகவும் தேர்ச்சிமிக்க மற்றும் திறமைமிக்க தொழில் படை ஒன்றை உருவாக்குதல்.
4. அரசாங்கத்துடனும் அதனுடன் இணைந்த அதிகார மையங்களுடனும் இணைந்து அரசாங்க செயல்முறைகளில் டிஜிட்டல் தொழில் நுட்பத்தை புகுத்தி அதில் பொருத்தமான சைபர் பாதுகாப்பு நடவடிக்கைகளை செயற்படுத்துவதாகும்.
5. இலங்கை மக்களுக்கு இணையம் தொடர்பான குற்றச் செயல்கள் மற்றும் அது வலுவூட்டல் செயற்பாடுகள் தொடர்பான விழிப்புணர்வு செயற்திட்டங்களை உருவாக்குதல்.
6. அரசாங்க - தனியார் துறை மற்றும் உள்ளூர் - சர்வதேச மட்டங்களில் இணைந்து செயற்பட்டு இணைய பாதுகாப்பு தொடர்பான ஆரோக்கியமான சூழலை ஏற்படுத்தல்

## தற்போதை நிலமை தொடர்பான பகுப்பாய்வு அறிக்கை

இந்தப் பகுதியானது முழுமையாக தகவல் தொழில்நுட்பம் தொடர்பான நாங்கள் மேற்கொண்டுள்ள தயார்படுத்தல் தொடர்பான நடவடிக்கைகளையும் அரசாங்கம் இது தொடர்பாக மேற்கொண்டுள்ள ஆரம்ப கட்ட நடவடிக்கைகள் தொடர்பாகவும். இணைய தள பாதுகாப்பு தொடர்பாக இலங்கையில் எடுக்கப்பட்டுள்ள பாதுகாப்பு நடவடிக்கைகள் தொடர்பாகவும் விளக்கமளிக்கின்றது.

## தகவல் தொழில்நுட்பம் தொடர்பான எங்களது தயார்படுத்தல்.

இலங்கையில் தகவல் தொழில்நுட்பம் தொடர்பான அறிவு 28.3% மாகவும் டிஜிட்டல் தொடர்பான கல்வி அறிவு 38.7% மாகவுமு: கானப்படுகின்ற அதே வேளை நிரந்தர தொலை பேசி வசதிகள் ஒவ்வொரு 100 பேருக்கும் 12.49% மாகவும் கையடக்க தொலை பேசி ஒவ்வொரு 100 பேருக்கும் 103.16 மாகவும் புரோண்ட பேன்ட் இணைப்பு ஒவ்வொரு 100 பேருக்கும் 10.45 மாக கானப்படுகின்றது. இணைய தள வசதியுள்ளவர்கள் 23.5% மாகவும் இணைய தள வசதியை பாவிக்கின்றவர்களின் எண்ணிக்கை 21.3% மாகவும் மின்னஞ்சலை பயன்படுத்துகின்றவர்களின் விகிதம் 11% மாகவும் கானப்படுகின்றது. துகவல் தொழில்நுட்ப பயன்பாடுகள் தொடர்பாக நகர்புரங்களுக்கும் கிராமபுரம் மற்றும் தோட்ட புரங்களுக்கிடையில் பாரிய வேறுபாடுதன்மை கானப்படுகின்றது.

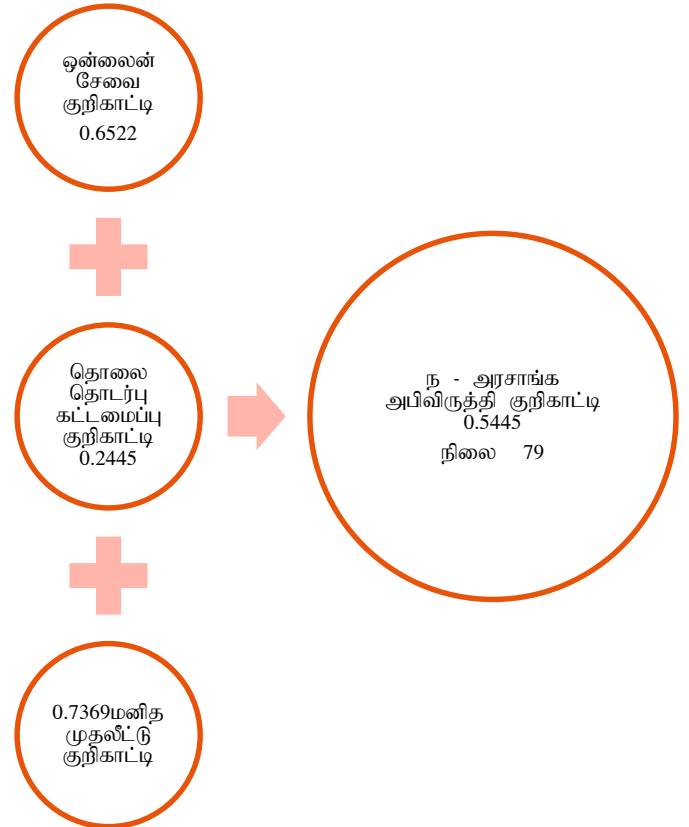
சில குறிப்புகள்<sup>3,4</sup>

<b>விட்டிடல் கணனி வைத்திருப்பவர்கள்</b> * 23.5% நகரம்: 39.9% கிராமபுரம்: 21% தோட்டபுரம் 5.1%	<b>தொலை பேசி பாவனையாளர் ஒவ்வொரு 100 பேருக்கும்</b> 12.49 (நிலையான) 103.1 (எடுத்து செல்லக்கூடிய)	<b>புரோடபேண்ட் பாவனையாளர்கள் ஒவ்வொரு 100 பேருக்கும்</b> நிலையான 2.65 வயர்-அற்ற 7.8
<b>இணைய பாவனை</b> 21.3% மின்னஞ்சல் பாவனை 11%	<b>(அ) .கணனி அறிவு 28.3%</b> (நகரம் 41.1% 26.5% தோட்டபுரம் 9.5%) <b>(ஆ) டிஜிட்டல் அறிவு 38.7%</b> (நகரம் 54.5% கிராமம் 36.4% தோட்டம் 16.4%)	
<b>இணைய பாவனைக்கான உபகரணங்கள்</b> மடி கணனி 38.1% ஸ்மார்ட் போன் 56.9% டெப்லட் 2.1% கை பேசி 2.9%		

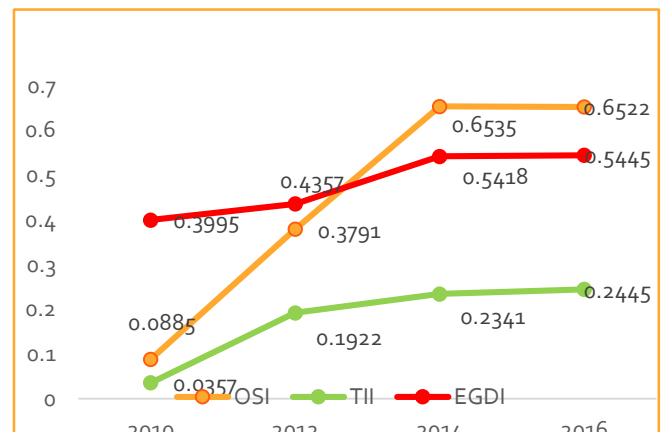
## டிஜிட்டல் அரசாங்கம் தொடர்பில் எங்களது முன்னேற்றம்.

டிஜிட்டல் அரசாங்கம் தொடர்பான ஐக்கிய நாடுகள் சபையின் குறிகாட்டிக்கு அமைவாக (EGDI) 190 நாடுகளில் இலங்கை 79 வது இடத்தினை பெற்றுள்ளது. (அ) ஒன் லைன் சேவை குறிகாட்டியின் அடிப்படையில் நாம் 0.6522 புள்ளிகளை பெற்றுள்ளோம். (OSI) டிஜிட்டல் தொழில் நுட்பத்தை அரசாங்க செயற்பாடுகளில் எவ்வாறு பயன்படுத்தப்படுகின்றது என்பது

தொடர்பாக அதில் கவணம் செலுத்தப்பட்டுள்ளது. (ஆ) தொலை தொடர்பு கட்டமைப்பு குறிகாட்டியில் நாங்கள் 0.2445 புள்ளிகளை பெற்றுள்ளோம் இதில் முழுமையான தொலை தொடர்பு கட்டமைப்பு வசதிகள் தொடர்பாகவும் இணைய வசதிகள் மற்றும் இணையதள பயன்பாடு போன்ற விடயங்களில் கவணம் செலுத்தப்பட்டுள்ளது(வுஐஐ). (இ) மனித முதலீட்டு குறிகாட்டி (HCI) இது முழுமையாக பாடசாலை கல்வியையும் எழுத்தறிவு வீதத்தினையும் குறித்து காட்டுகின்றது. மனித முதலீட்டு குறிகாட்டியில் நாங்கள் உலகளில் சராசரியான பெறுமானத்தை பெற்றுள்ளோம் ஆனால் தொலை தொடர்பு கட்டமைப்பு வசதிகளில் நாம் குறைவான அடைவு மட்டத்தை பெற்றுள்ளோம்.



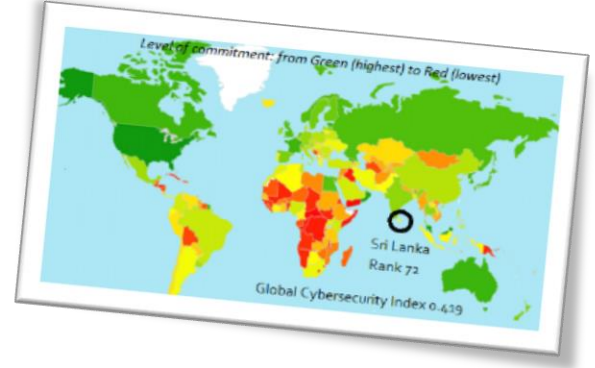
டிஜிட்டல் அரசாங்கம் தொடர்பான அபிவிருத்தி முன்னேற்றம்.



## சைபர் பாதுகாப்பு தண்மை

### சைபர் பாதுகாப்பு குறிகாட்டியில் நமது நிலை

தகவல் தொழில்நுட்ப பகுதியில் இருக்கின்ற (ITU) 193 நாடுகளில் பூலோக சைபர் பாதுகாப்பு குறிகாட்டி (GCI) மதிப்பீட்டுக்கு அமைவாக இலங்கை 72 வது இடத்தில் இருக்கின்றது. 2016 ம் ஆண்டு சைபர் பாதுகாப்பு தொடர்பாகவும் நாடுகள் அதற்காக மேற்கொண்ட பங்களிப்புகள் தொடர்பாகவும் பின்வரும் 5 வித்தியாசமான கோணத்தில் ஆய்வு மேற்கொண்டது. குறிப்பாக (அ) சட்டம் (ஆ) தொழில்நுட்பம் (இ) திறன் விருத்தி (ஈ) அமைப்பு உருவாக்கம் (உ) கூட்டுறவு போன்ற கோணங்களில் ஆராய்சியை மேற்கொண்டது. ஆதன்படி இலங்கை தொடங்கப்பட்டுள்ள மற்று



### அரச பங்களிப்பு குறிகாட்டியில் எமது செயல்திறன்

2017 இல் எங்கள் செயல் திறன்

#### ய. சட்டம் : நாங்கள் தொடங்குகின்றோம்

சைபர் குற்றச்செயல்கள் தொடர்பாகவும் சைபர் பாதுகாப்பு தொடர்பாகவும் சட்டங்களை இயற்றுவதற்கும் அது தொடர்பான சட்ட ரீதியான பயிற்சிகளை நடாத்துவதற்கும் நாங்கள் நடவடிக்கைகள் மேற்கொண்டுள்ளோம்.

#### டி. தொழில் நுட்பம்: நாங்கள் முதிர்ச்சியடைகின்றோம்

சைபர் பாதுகாப்பு தொடர்பாகவும் அது தொடர்பான பிரச்சினைகளை கையாள்வதற்கும் தொழில்நுட்ப நிறுவனங்களை நாடி அது தொடர்பான சிறந்த வேலைத்திட்டம் ஒன்றை முன்வைப்பதற்கு நாங்கள் நடவடிக்கைகள் மேற்கொண்டுள்ளோம்.

#### உ. திறன்கள் அபிவிருத்தி செய்வதில் நாங்கள் முதிர்ச்சி பெற்றுள்ளோம்.

ஆய்வு மற்றும் மேம்படுத்தல், கல்வி மற்றும் பயிற்சியளித்தல் நிகழ்ச்சி திட்டங்கள், தொழில் தகமை சான்றிதழ்கள் வழங்கல் போன்ற சேவைகளை அரசாங்க துறைக்கு வழங்குகின்ற அளவினை பொருத்து இது அளவிடப்படுகின்றது.

#### எ. அமைப்பின் அடிப்படையில்: நாங்கள் முதிர்ச்சியடைந்துள்ளோம்.

நிறுவன ரீதியான கொள்கை உருவாக்கம் சைபர் பாதுகாப்புக்கான உத்திகளை கையாள்வதில் விடயங்களை ஒருங்கிணைத்தல் போன்ற விடயங்களில் நாங்கள் தேசிய ரீதியில் அபிவிருத்தி யடைந்துள்ளோம்.

#### ந. ஒத்துழைப்பு : நாங்கள் தொடங்கியுள்ளோம்.

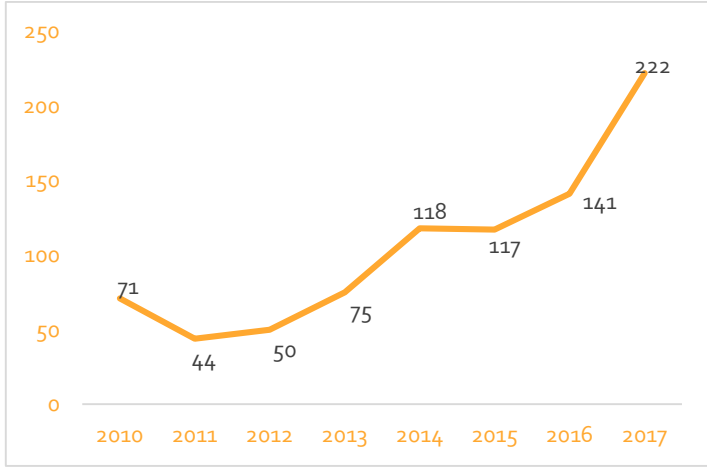
கூட்டுறவு இணையத்தில் தகவல்களை பரிமாறிக்கொள்ளல் போன்ற செயற்பாடுகளின் அடிப்படையில் அளவிடப்படுகின்றது. இருக்கின்றது அத்துடன் பெரும்பாலும் நாங்கள் இந்த விடயத்தில் முதிர்ச்சியடைந்து வருகின்ற நிலையில் இருக்கின்றோம்

மதிப்பீட்டு எடுகோள்கள்	மதிப்பீட்டு உடப எடுகோள்கள்	எமது நிலை
அ. சட்டம்	சைபர் குற்ற செயல் தொடர்பான சட்டம்	தொடக்கம்
	சைபர் பாதுகாப்பு சட்டம் இயற்றல்.	தொடக்கம்
	சைபர் பாதுகாப்பு பயிற்சி	முண்ணனி
ஆ. தொழில்நுட்பம்	தேசிய ஊறுகவு, 'ஊறுகவு', 'ஊறுகவு	முண்ணனி
	ஆ. ரசாங்க ஊறுகவு, 'ஊறுகவு	முண்ணனி
	துறைரீதியான ஊறுகவு, 'ஊறுகவு, 'ஊறுகவு	முண்ணனி
	நிறுவனங்களின் தரம்	தொடக்கம்
	தொழில் திறன்	தொடக்கம்
	ஒன்லைன் பிள்ளை பாதுகாப்பு	தொடக்கம்
	இ. திறன் விரத்தி	தரப்படுத்தல் நிறுவனங்கள்
ஈ. அமைப்பு	சைபர் பாதுகாப்பின் சிறந்த செயற்பாடு	முண்ணனி
	சு மற்றும் னு நிகழ்ச்சி திட்டம்.	முதிர்ச்சி
	பொது விழிப்புணர்வு பிரச்சாரம்.	முண்ணனி
	தொழில் பயிற்சி பாட நெறிகள்	முண்ணனி
	கல்வி நிகழ்ச்சி திட்டங்கள்	முதிர்ச்சி
	ஊக்குவிப்பு பொறிமுறை	தொடக்கம்
	வீட்டை அடிப்படையாக கொண்ட தொழில்.	தொடக்கம்
	உபாயங்கள்.	தொடக்கம்
	பொறுப்பு முகவர்கள்	முதிர்ச்சி
	ஐசபர் பாதுகாப்பு மெடறிக்	தொடக்கம்
உ. ஒத்துழைப்பு	இரு தரப்பு ஒப்பந்தம்	தொடக்கம்
	புல தரப்பு ஒப்பந்தங்கள்	தொடக்கம்
	கர்வதேச பங்குபற்றல்கள்	தொடக்கம்
	துனியார் அரசாங்க பங்குடமை	முதிர்ச்சி
	கூட்டு செயற்பாட்டை ஒருங்கிணைத்தல்.	தொடக்கம்

**பதிவு செய்யப்பட்ட சம்பவங்கள்**

கடந்த பல வருடங்களாக ஊடுகவு'ஊஊ சைபர் பாதுகாப்புதொடர்பாக பல்வேறு சம்பவங்களை பதிவு செய்துள்ளது. 2010 ஆண்டு தொடக்கம் 2017 வரை காலப்பகுதியில் 71 இருந்து 222 ஆக இத்தகைய சம்பவங்கள் பதிவு செய்யப்பட்டுள்ளது. நிறைய சம்பவங்கள் சமூக ஊடகங்கள் தொடர்பான விடயங்களே பதிவு செய்யப்பட்டுள்ளன. இது ஒரு வேகமான அதிகரிப்பை காட்டுகின்றது. 2010 ஆண்டு 80 சம்பவங்களும் 2017 ம் ஆண்டு 3685 சம்பவங்களும் பதிவு செய்யப்பட்டுள்ளன.

சைபர் பாதுகாப்பு தொடர்பான சம்பவங்கள் வளர்ச்சி



சம்பவங்களின் தண்மை	2012	2013	2014	2015	2016	2017
பிழிங்	08	08	12	14	23	42
தனிப்பட்ட விடயங்கள் துஷ்பிரயோகம்	08	08	08	21	32	29
ஸ்கேம்	06	18	12	18	12	32
மெலிசியஸ் மென்பொருள்ரென்சம் மென்பொருள்	02	02	03	12	21	39
நிதி மோசடி	-	-	-	10	16	35
வலை தளங்களின் சமரசம்	15	16	56	20	10	25
மின்னஞ்சல் சமரசம்	06	08	10	16	16	14
புலமை சொத்து மீறல்	03	03	03	03	07	06
அதிகாரமின்றி அடைய முற்படுத்தல்.	01	11	08	-	-	-
ஹாழ்ஹு. ஹாழ்ஹு	01	01	06	03	04	-

சமூக ஊடக சம்பவங்கள்	1100	1200	2250	2850	2200	3685
சமூக வலய ஊடகம் தொடர்பான உண்மைகள் (2017)						

**4.2 மில்லியன்கள்**

மொத்த இணைய பாவனையாளர்களில் 63% மானவர்கள் முகநூல் பாவனையாளர்கள்

இலங்கை கணனி அவசர தயார் குழுவிட்கு அறிவிக்கப்பட்ட தரவுகள் 2017

3685 சமூக ஊடகங்கள் தொடர்பாக பதிவு செய்யப்பட்ட சம்பவங்கள்

2018 பேக் சமூக ஊடக கணக்கு 829 ஹக்கிங் சமூக ஊடக கணக்கு

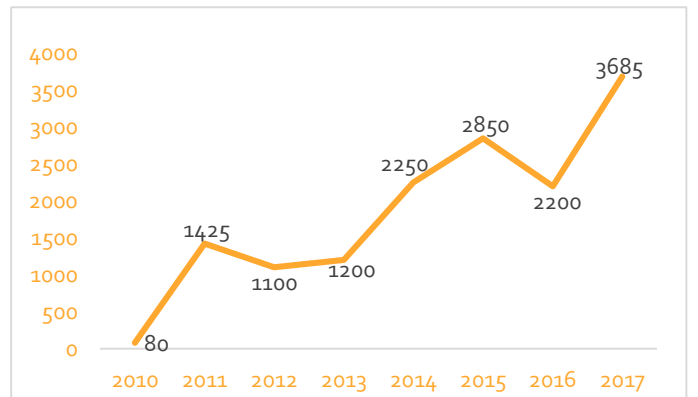
416 சம்பவங்கள் புகைப்பட துஷ்பிரயோகம் சம்பந்தமானது.

57 கொடுமைப்படுத்தல் மற்றும் பயமுறுத்தல் 54 சம்பவங்கள் தொலை பேசி இலக்கத்தை தவறாக பயன்படுத்தல் தொடர்பானது

17 சம்பவங்கள் புகைப்படங்கள் மற்றும் வீடியோக்கள் தொடர்பானது 7 சம்பவங்கள் பதிப்புரிமை மீறல் சம்பந்தமான

ஏனையவை 287

சமூக வலய ஊடகம் தொடர்பான நிகழ்வுகளில் வளர்ச்சி





## எங்களது மூலோபாயம்

வினைத்திறன் மிக்கதும் நம்பகமானதுமான சைபர் பாதுகாப்பு சூழலை உருவாக்கி இலங்கை பிரஜைகள் அனைவருக்கும் டிஜிட்டல் வசதிகளை பெற்றக்கொடுப்பதே எமது நோக்காகும்.



## பிரதானமான ஆறு மூலோபாய பகுதிகள்

1. **ஆட்சி கட்டமைப்பு ஒன்றை உருவாக்குதல்**  
தேசிய தகவல்கள் மற்றும் சைபர் பாதுகாப்பை அமுல்படுத்துவதற்காக சிறந்த ஆட்சி கட்டமைப்பு ஒன்றை உருவாக்குதல்.
2. **சட்டம், கொள்கை மற்றும் நியமங்கள் என்பவற்றை நிறுவுதல் அமுல்படுத்தல்**  
இணைய பாவனையாளர்களை சைபர் தாக்குதல்களில் இருந்து தனிநபர்களையும் அமைப்புக்களையும் பாதுகாத்தலும் அதற்காக சட்டம் மற்றும் ஒழுங்கு முறையை உருவாக்கம் செய்தலும்.
3. **தகுதியான பணியாளர்களின் அபிவிருத்த**  
தகுதியான வினைத்திறன் மிக்க பணியாளர்களை உருவாக்கி இணையதள தாக்குதல்களுக்கு பதிலளித்தலும் பாதுகாத்தலும்.
4. **டிஜிட்டல் அரசாங்க முறையும் உட்கட்டமைப்பும்.**  
டிஜிட்டல் அரசாங்க முறை நடைமுறைப்படுத்தப்பட்டு இயக்கப்படும் என்பதை உறுதிப்படுத்துவதற்காக பொது துறை நிறுவனங்களுடன் இணைந்து பணியாற்றுவதல் இணைய பாதுகாப்பினை ஏற்படுத்திப் பின்னடைவுகளில் இருந்து பாதுகாத்தல்.
5. **பொது மக்களுக்கு விழிப்புணர்வு மற்றும் வலுவூட்டல் செயற்பாடுகளை செய்தல்**  
இலங்கை மக்கள் சைபர் தாக்குதல்களில் இருந்து தங்கள் சொத்துக்கள் ஆவணங்கள் மற்றும் அடையாளங்களை பாதுகாத்து கொள்வதற்காக திறமை மிக்கவர்களாக மாற்ற வேண்டும்.
6. **பொது - தனியார் உள்ளூர் சர்வதேச கூட்டுறவை மேம்படுத்துதல்.** மேம்படுத்துதல். மற்றும் ஒரு வலுவான இணைய பாதுகாப்பு சூழலை ஏற்படுத்துதல்.

## உந்தல் இலக்கம் 1: ஆட்சி கட்டமைப்பு ஒன்றை உருவாக்குதல்.

### எங்கள் விபூகம்

2006 ம் ஆண்டு இலங்கை அரசாங்கம் இலங்கையில் CERT நிறுவனத்தை நிறுவியது. இதன் மூலமாக கணினிக்கு ஏற்படும் அச்சுறுத்தல்கள் கணினி அமைப்புக்குள் வலையமைப்புக்குள் என்பனவற்றில் ஏற்படும் பாதிப்புக்கள் தொடர்பாக பாதுகாத்தல் மற்றும் அத்தகைய பாதிப்புக்களினால் இருந்து பாதுகாக்கும் தொழில்நுட்ப ஆலோசனைகளை வழங்குதல் என்பனவாகும் CERT அமைப்பு தகவல் தொழில்நுட்ப முகவரினால் நிறுவப்பட்டது தற்போது இந்த நிறுவனம் தொலை தொடர்பு மற்றும் டிஜிட்டல் கட்டமைப்பு அமைச்சினால் நிர்வகிக்கப்படுகின்றது.

சைபர் பாதுகாப்பு தொடர்பில் ஒரு சிக்கலான சூழல் உருவாகியுள்ளது. இலங்கை அரசாங்கமானது இந்த பிரச்சினைகளை அடையாளம் கண்டு தேசிய தகவல் மற்றும் சைபர் பாதுகாப்பு உபாயங்கள் என்பனவற்றை அறிமுகப்படுத்தியுள்ளது. இதன் மூலமாக இது தொடர்பாக எழுகின்ற பிரச்சினைகளை சமாளிக்கக்கூடியதாக இருக்கின்றது. உயர்மட்டத்திலான மேலிருந்து கீழ் நோக்கிய தகவல் மற்றும் சைபர் பாதுகாப்பு திட்டத்தினை உருவாக்குதல் அத்துடன் இந்த இலக்கினை அடைவதற்கு குறித்த கால எல்லையும் அரசாங்கத்தினால் தீர்மானிக்கப்பட்டுள்ளது.

இந்த உபாயங்களை செயற்படுத்துவதற்காக தேசிய சைபர் பாதுகாப்பு முகவர் அமைப்பு ஒன்று ஏற்படுத்தப்படும். அத்துடன் அந்த முகவர் அமைப்பு இந்த முகவர் அமைப்பு இந்த விடயம் தொடர்பான கொள்கைகளை உருவாக்குதல் இந்த விடயங்கள் தொடர்பாக பொதுமக்களுக்கு கல்வி அறிவூட்டும் செயற்பாடுகளில் ஈடுபடுதல் போன்ற செயற்பாடுகளை செய்வதுடன் துறை சார்ந்த தொழில் படையை உருவாக்கி. இந்த தொழில் துறையை அபிவிருத்தி செய்வதாகும். அத்துடன் இந்த முகவர் சகல நடவடிக்கைகளையும் கண்காணித்து வழிநடாத்தும் பொறுப்பினையும் கொண்டிருக்கும்.



### எங்களது ஆரம்பம்

#### 1.1. தேசிய தகவல் மற்றும் சைபர் பாதுகாப்பு முகவர் இலங்கை என்ற நிலையத்தை நிறுவல்

ஐஊஊஊ இதை நிலையமானது இலங்கையில் சைபர் பாதுகாப்பு தொடர்பான விடயங்களை கையாளும் மிக உயர்ந்த அதிகாரம் பெற்ற நிறுவனமாக இருக்கும். இந்த நிறுவனமானது சைபர் பாதுகாப்பு தொடர்பான விடயங்களை மேற்பார்வை செய்து சைபர் பாதுகாப்பு உபாயங்களை உருவாக்கி அதனை செயற்படுத்துகின்ற அதிகாரம் பெற்ற நிறுவனமாக விளங்கும்.

- 1.1.1. இந்த முகவர் நிலையமானது பாதுகாப்பு, நிதி, நிதி, தகவல் தொழில்நுட்பம் மற்றும் தொலை தொடர்புகள், பொது நிர்வாகம் போன்ற அமைச்சகங்களுடன் இணைந்த ஒரு உயர்மட்ட நிர்வாக குழுவினால் நிர்வகிக்கப்படும் அத்துடன் இந்த முகவர் அமைப்பின் பிரதிநிதிகள் தேசிய பாதுகாப்பு சபையிலும் அங்கம் வகிப்பார்கள்.
- 1.1.2. சைபர் பாதுகாப்பு தொடர்பான விடயங்களை கையாளும் பிரதானமான முகவர் நிலையமாக இது அமைந்திருக்கும். ஐசபர் பாதுகாப்பு தொடர்பாக மூல உபாயங்களை உருவாக்கி அதனை செயற்படுத்தும்.

- 1.1.3. சைபர் பாதுகாப்பு தொடர்பான சட்டங்களை உருவாக்கி டிஜிட்டல் குற்ற தடுப்புக்களையும் அது தொடர்பான தடவியல் புலனாய்வுகளையும் மேற்கொள்ளும்

- 1.1.4. இந்த துறையில் ஆற்றலை மேம்படுத்துவதற்காக ஊருசவு நிறுவனம் வசதிகளை செய்து கொடுக்கும் ஊருசவு ஊன நிறுவனம் இதன் செயற்பாடுகளை ஒருங்கிணைக்கும் ஊருசவு அத்துடன் இந்த நிறுவனம் சம்பவங்களையும் தகவல்களையும் பகிர்ந்துகொள்ளும் அத்துடன் ஏனைய பாதுகாப்பு விடயங்கள் தொடர்பாக சிறந்த செயற்பாடுகளை மேற்கொள்ளும்.

“எங்கள் விபூகம். சைபர் பாதுகாப்பு மற்றும் தகவல் விபூகங்களை வகுத்து அதனை செயற்படுத்தக்கூடிய சக்திமிக்கதும் அதனை மேற்பார்வை செய்யக்கூடியதுமான சைபர் அச்சுறுத்தலுக்குகெதிராக செயற்படக்கூடிய தாக்கீதிக் கட்டமைப்பை உருவாக்குவதே எமது நோக்கமாகும்.

1.1.5. அமைச்சுக்கள் அதிகார சபைகள், கூட்டுத்தாபனங்கள் போன்ற அரசாங்க அமைப்புகளுக்கு தொழில்நுட்ப ஆலோசனைகளை வழங்குதல்.

1.1.6. திமர் சைபர் அச்சுறுத்தல் தொடர்பான விடயங்களை இலங்கை மக்களுக்கு எச்சரிக்கை விடுத்தல்..

1.1.7. தகவல் பாதுகாப்பு தொடர்பான இணைந்த சேவைகளை வழங்கும் நிறுவனங்களுக்கு சான்றிதழ்களை கொடுத்து அவர்களின் சேவைகளை உறுதிப்படுத்தல்.

## 1.2. தேசிய சைபர் பாதுகாப்பு முகவர் நிறுவனத்தின் கீழ் இருக்கின்ற நிறுவனங்கள்

6.1. இலங்கை தேசிய சைபர் பாதுகாப்பு நிறுவனத்தின் கீழ் சைபர் அவசர அறிவிப்பு நிறுவனம் செயற்படுகின்றது ஊறுசுவுஊஊ இந்த நிறுவனம் பாவனையாளர்களை சைபர் அச்சுறுத்தலில் இருந்து பாதுகாக்கின்றது. அத்துடன் அரசு நிறுவனங்களையும் தனியார் நிறுவனங்களையும் சைபர் பாதுகாப்பு தொடர்பான தேவையான தகவல்களை வழங்கி பாதுகாக்கின்றது கணனி அவசர பாதுகாப்பு சேவையையும் வழங்குகின்றது.

## 6.2. அரசாங்க அமைப்புகள் சமூக குழுக்கள் மற்றும் அரசாள்பற்ற நிறுவனங்களின் உதவியை பெறுதல்.

6.2.1. சமூக மேம்பாடு மற்றும் நலன்புரி அமைச்சு, பெண்கள் மற்றும் குழந்தைகள் விவகார அமைச்சு, சிறுவர் பாதுகாப்பு அதிகார சபை சட்டமற்றும் ஒழுங்கு அமைச்சு ஆகியவை உள்ளடங்கிய அரசாங்க நிறுவனங்களுடன் இணைந்து இது தொடர்பாக கிராம சமுதாயத்தில் விழிப்புணர்வு செயற்திட்டம் ஒன்றை நடாத்துதல். சமூகத்தில் அதிகம் பாதிப்படையும் மக்களுக்கு இணைய பாதுகாப்பு தொடர்பான அறிவுரைகளை வழங்குதல்.

1.2.1. தேசிய ஒருங்கிணைந்த சூழல் மற்றும் கணனி முறை பகுப்பாய்வு அமைப்பு நிறுவப்படவிருக்கின்றது இதில் 22 X 7 சைபர் பாதுகாப்பு அழைப்பு நிலையம் அமைக்கப்படவுள்ளது. இந்த அமைப்பு அமைக்கப்படுவதன் பிரதான நோக்கம் அரசாங்க நிறுவனங்கள் மற்றும் தனியார் நிறுவனங்கள் பொது மக்கள் ஆகியோரை சைபர் தாக்குதலில் இருந்து பாதுகாப்பதாகும்.

1.2.2. தேசிய ஒருங்கிணைந்த சூழல் மற்றும் கணனி முறை பகுப்பாய்வு அமைப்பானது தேசிய சைபர் முன்னெச்சரிக்கை முறை ஒன்றை அமுல்படுத்த இருக்கின்றது இது இணைய சேவையை வழங்குகின்ற நிறுவனங்களுக்கு உதவும் வகையில். அமைக்கப்படவுள்ளதுடன் சரியான நேரத்தில் மக்களுக்கு தகவல்களை வழங்கி பொது மக்களின் கணனிகளை சைபர் தாக்குதல்களில் இருந்து பாதுகாத்து பெர்து மக்களுக்கு இது தொடர்பான அறிவை வழங்குவதாகும்.

1.2.3. தேசிய ஒருங்கிணைந்த சூழல் மற்றும் கணனி முறை பகுப்பாய்வு அமைப்பு டிஜிட்டல் தடவியல் ஆய்வகத்தை நிறுவுவதற்கு ஆலோசித்துள்ளது. இதில் கணனி தடவியல், வீடியோ

1.2.4. தடவியல், கையடக்க தொலை பேசி தடவியல் போன்ற பிரிவுகளை அமைத்து அந்த தடவியல்களின் அடிப்படையில் பரிசோதனை செய்து புலனாய்வுகளை மேற்கொள்வதற்கு திட்டமிட்டுள்ளது.

1.2.5. தேசிய ஒருங்கிணைந்த சூழல் மற்றும் கணனி முறை பகுப்பாய்வு அமைப்பு (NCSOC) தேசிய சைபர் பாதுகாப்பு இயக்க நிலையம் ஒன்றை செயற்படுத்த இருக்கின்றது அரசாங்கம் டிஜிட்டல் முறையை செயற்படுத்துகின்ற போது ஏற்படும் அச்சுறுத்தல்கள் மற்றும் பதற்றமான தகவல் கட்டமைப்பு மற்று அவசர நிலைமகளின் போது தனியார் துறைக்கு உதவுதல் போன்ற சேவைகளை இதன் மூலமாக வழங்குவதற்கும் அதனை கண்காணிப்பு செய்யும் நடவடிக்கைகளையும் மேற்கொள்ளும்.

1.2.6. ஜேஊரூயு தேசிய ஒருங்கிணைந்த சூழல் மற்றும் கணனி முறை பகுப்பாய்வு அமைப்பு (NCA) தேசிய சான்றிதழ் அதிகார சபை ஒன்றை நிறுவ இருக்கின்றது இது சான்றிதழ் சேவை வழங்கும் அமைப்பு என அழைக்கப்படும்.

1.2.7. ஜேஊரூயு தேசிய ஒருங்கிணைந்த கணனி சூழல் மற்றும் பகுப்பாய்வு அமைப்பு ஒரு ஆய்வு பகுதியை நிர்மாணிப்பதற்கு திட்டமிட்டுள்ளது. போன்ற விடயங்களில் ஆய்வுகளை மேற்கொள்ள இருக்கின்றது.

1.2.8. இதன் மூலமாக டிஜிட்டல் விடயங்களை விருத்தி செய்து அதனை ஒருங்கிணைத்து தொடர தேர்ச்சியான ஊக்க செயற்பாடுகளை வழங்கி மூலோபாய கொள்கை ஆய்வு, தகவல் பாதுகாப்பு ஆய்வு, சைபர் பாதுகாப்பு தொழில்நுட்பம் போன்ற விடயங்களில் ஆய்வுகளை மேற்கொள்ள இருக்கின்றது.

1.3. கண்காணிப்பு மற்றும் மதிப்பீட்டு கட்டமைப்பு விரிவான அடிப்படையில் கண்காணிப்பு மற்றும் மதிப்பீட்டு நடவடிக்கைகளை மேற்கொள்வதற்கான கட்டமைப்பு ஒன்றை நிர்மாணிப்பதற்கும் தீர்மானித்துள்ளதுடன். உபாயங்களை செயற்படுத்துகின்ற போது பெறப்படும் விளைவுகள் தொடர்பாக அளவீடுகளையும் மதிப்பீடுகளையும் மேற்கொள்ளும்.

## உந்தல் இலக்கம் 2 : சட்டம், கொள்கைகள் மற்றும் தரநிலைகள்.

### எங்களது மூலோபாயங்கள்

இலங்கையில் தனிநபர்களுக்கும் நிறுவனங்களுக்கும் எதிராக இணைய தளங்கள் தொடர்பான குற்றச் செயல்கள் நாளுக்கு நாள் அதிகரித்து வருவதை அறிக்கைகள் காட்டுகின்றன. இதில் கடன் அட்டை மோசடிகள், பழிவாங்கும் நடவடிக்கைகள், புலமை சொத்துக்கள் திருட்டு ஆபாச படங்கள். வலைதளங்களை மறைத்தல், அங்கீகரிக்கப்படாத தரவுகளின் செயலாக்கம் நிதி தரவுகளை ஹேக்கிங் செய்தல், போன்ற முறை கேடான செயல்கள் நடைபெறுகின்றன. இத்தகைய சைபர் குற்றச்செயல்களில் ஈடுபடும் நிறுவனங்களுக்கும் தனிநபர்களுக்கும் எதிராக போராடி பொருத்தமான தரவு டிஜிட்டல் முறைகளை ஏற்படுத்தவும். தனியுரிமை மற்றும் சைபர் வெளிப்பாட்டு சுதந்திரத்தை பாதுகாக்கவும். பொருத்தமான சட்டங்களையும் கொள்கைகளையும் உருவாக்கி அமுல்படுத்த வேண்டியதுடன் அதனை தரநிலை உருவாக்கம் செய்ய வேண்டும்.

இலங்கை அரசாங்கமானது இந்த விடயம் தொடர்பாக பல்வேறு நடவடிக்கைகளை மேற்கொண்டுள்ளது. அவையாவன ஐ.என்.டி. 27000 அடிப்படையாக கொண்ட பாதுகாப்பு கொள்கை (2009) தரவுகள் பகிர்ந்து கொள்ளும் கொள்கை, சட்ட இலக்கம். 19 இன் 2006இ இலத்திரனியல் பரிவர்த்தனை சட்டம். சட்ட இலக்கம் 30 இன் 2006இ உதிரிப்பாகங்கள் மோசடி சட்டம். புலமை சொத்து சட்டம். சட்ட இலக்கம் 24 இன் 2007 குற்றவியல் சட்டம். போன்ற சட்டங்களை இயற்றியுள்ளது. அத்துடன். சைபர் குற்றவியல் தொடர்பான மகா நாட்டில் கலந்து கொண்ட முதல் தெற்காசிய நாடு என்ற பெருமையும் நமது நாட்டுக்கு உண்டு. அதற்கு மேலாக கணனி குற்ற பிரிவு என்ற தனியான குற்ற பிரிவு குற்ற புலயாய்வு திணைக்களத்தில் ஏற்படுத்தப்பட்டுள்ளது அதன் அடிப்படையில் இலங்கை பொலிஸ் திணைக்களம் நடவடிக்கைகளை மேற்கொண்டுள்ளது.

மேலும் சைபர் குற்றங்கள் தொடர்பான விடயங்களை கட்டுப்படுத்துவதற்கு ஒழுங்கு முறையான கட்டமைப்பை பலப்படுத்துவதன் மூலமாகவும். நடைமுறைப்படுத்தப்படுகின்ற கொள்கைகள் மற்றும் சட்டங்களின் குறைபாடுகளை கண்டறிந்து புதிய சட்டங்களையும் புதிய கொள்கைகளையும் உருவாக்கி அதனை நடைமுறைப்படுத்தி தனிநபர்களையும் நிறுவனங்களையும் சைபர் தாக்குதல்களில் இருந்து பாதுகாக்க வேண்டும்.

“மூலோபாயம் சரியான ஒழுங்கு முறையான தனி நபர்களையும் நிறுவனங்களையும் சைபர் தாக்குதலளில் இருந்து பாதுகாப்பதாகும் அத்துடன் சரியான பொருத்தமான சட்டங்களை இயற்றி அதனை பொது மக்கள் மத்தியில் அறிமுகப்படுத்தி சட்ட ரீதியாக அவர்களுக்கு உதவுவதுடன் சரியான தரநிலைநிபந்தனை கொள்கைகளை உருவாக்குவதாகும். ”



### எங்களது ஆரம்பம்

#### புதிய பாதுகாப்பு சட்டத்தை அறிமுகப்படுத்தல்

2.1.1. அரசாங்கம் தேசிய ஒருங்கிணைந்த சைபர் பாதுகாப்பு முகவர் ஜே.ஐ.ஐ.சி. நிறுவனத்தை அமைப்பதற்காக புதிய சட்டம் ஒன்றை அறிமுகப்படுத்தியுள்ளது. நாட்டில் அதிகரித்து வரும் சைபர் அச்சுறுத்தல்களை சமாளிப்பதற்கும் அதனை வெளிப்படுத்துவதற்கும் அதிகாரம் மிக்க ஸ்தாபனத்தை உருவாக்குவதே அதன் நோக்கமாகும்.

2.1.2. புதிய சட்டமானது சைபர் குற்றச்செயல்களை தடுப்பதற்கும், அதனை முகாமைத்துவப்படுத்துவதற்கும் ஏற்படுத்தப்பட்டுள்ளது. நடைமுறையில் இருக்கின்ற சட்டமானது சட்ட இலக்கம் 24 இன் 2007 ஆனது நவீன காலத்தில் நடைபெறுகின்ற கணனி குற்றச் செயல்களை தடுப்பதற்கு போதுமானதாக இல்லை



தரவு பாதுகாப்பு மற்றும் தனியுரிமை சட்டங்கள் மற்றும் தரவு பகிர்வு கொள்கை.

தற்போது வாடிக்கையாளர்களின் தரவுகளை திருடுகின்ற குற்றச்செயல்கள் அதிகரித்து காணப்படுகின்றது எனினும் வாடிக்கையாளர்களின் தரவுகளை பாதுகாப்பதற்கான பொருத்தமான சட்டங்களை இலங்கை கொண்டிருக்கவில்லை. எனவே அரசாங்கமானது தனிப்பட்டவர்களினதும் நிறுவனங்களினதும் தரவுகளை பாதுகாப்பதற்கான புதிய சட்டங்களை இயற்றி அதனை அவர்கள் சேகரித்து பயன்படுத்தக்கூடிய தரவு தனியுரிமை பாதுகாப்பு சட்டத்தை அறிமுகப்படுத்துவோம்.

2.2.1 அரசாங்கத்தின் இந்த நடவடிக்கையின் மூலமாக பொதுமக்களினதும் நிறுவனங்களினதும் தரவுகளை பாதுகாக்கின்றது. அத்துடன் இவர்களின் தனியுரிமை மீறல்களை தடுக்கின்றது. அத்துடன் தனியார் நிறுவனங்கள் தங்களது தரவுகளை போதுமான பாதுகாப்பு நிலையில் வைத்து தனியுரிமை மீறல்களில் இருந்து அவற்றை பாதுகாக்கின்றன.

2.2.2 அரசாங்க நிறுவனங்களுக்கான தரவு பகிர்வு கொள்கையை நாங்கள் அறிமுகப்படுத்துவோம்.

### 2.3 அடிப்படை தரநிலை பாதுகாப்பு

தகவல் அமைப்பு மற்றும் வன்பொருள் மற்றும் மென்பொருள் பயன்பாடுகளுக்கான அடிப்படை தகவல்கள் மற்றும் சைபர் பாதுகாப்பு தரங்களை உருவாக்குவதற்காக இலங்கை தர நிர்ணய சபைக்கு உதவுவோம்.

### 2.4 சிக்கலான உட்கட்டமைப்பு பாதுகாப்பு கொள்கை

உட்கட்டமைப்பு பாதுகாப்பு கொள்கையை நாம் அறிமுகப்படுத்தகின்றோம். இதன் மூலமாக சிக்கலான உட்கட்டமைப்பு விடயங்களை கண்டறிந்து அதற்கு தேவையான பாதுகாப்பு நடவடிக்கைகளையும் தேவையான ஆலோசனைகளையும் வழங்குவதோடு உட்கட்டமைப்புக்களையும் பாதுகாப்பதற்கு தேவையான வசதிகளையும் வழங்குகின்றது.

### 2.5 தகவல் பாதுகாப்பு கொள்கை

நிறுவனங்களின் தகவல் அமைப்பு முறை அவற்றின் தரம் என்பனவற்றுக்கு அமைவாக பாதுகாப்பு கொள்கைகளை உருவாக்கி இந்த நிறுவனங்களுக்கு உதவுவதற்கு நாங்கள் தயாராக இருக்கின்றோம். ஒவ்வொரு நிறுவனங்களினதும் பாதுகாப்பு கொள்கையானது சர்வதேச தரத்துடன் ஒழுங்கமைக்கப்பட்டிருக்க வேண்டும்.

## உந்தல் இலக்கம் 3: தகுதியான பணியாளர் தொகுதியை விருத்தி செய்தல்

### எங்கள் மூலோபாயம்

சைபர் தாக்குதலின் காரணமாக தகவல்கள் பரிமாற்று சேவையில் பாரிய இடையூறுகள் ஏற்படுகின்றன. அத்துடன் இதன் மூலமாக ஏற்படுகின்ற பாதிப்புக்களும் அதிகரித்து வருகின்றன. இந்த சூழலில் தகவல் மற்றும் சைபர் பாதுகாப்பு விடயத்தை செயற்படுத்தி அதனை பாதுகாத்தல், தடுத்தல், சரியான பதிலடி கொடுத்தல் போன்ற விடயங்களை செயற்படுத்துவதற்கு செயற்பாடுகளை செய்வதற்கும் இத்துறையில் அறிவு கர்மைமிக்கதும் தொழில் திறமைமிக்க தொழிற்படை ஒன்றை உருவாக்குவது அவசியமாகின்றது. 2016

2016 ம் ஆண்டு . ஐரோப்பிய நிறுவனத்தினால் நேர்கொள்ளப்பட்ட ஆய்வுகளின்படி சுமார் 2 மில்லியன் இணைய பாதுகாப்பு நிபுணர்கள் பற்றாக்குறையாக காணப்பட்டார்கள். GCI நிறுவனத்தின் கருத்துப்படி வளர்ந்துவரும் நாடுகளின் இணைய அச்சுறுத்தலை தடுப்பதற்காகவும் அதனை எதிர்த்து போராடுவதற்கும் ஒட்டு மொத்தமாக மனித வளத்தை அதிகரிப்பதில் இலங்கை அரசாங்கம் அதிக முயற்சி எடுக்க வேண்டும் என குறிப்பிடப்பட்டுள்ளது. இன்று இலங்கையில் சைபர் பாதுகாப்பு நிபுணர்களின் பற்றாக்குறை அதிகமாக காணப்படுகின்றது நமது நாட்டின் சூழலில் திறம்பட வேலை செய்ய தேவையான தொழில்நுட்ப திறன் கொண்ட அனுபவம் மிக்க தொழில் வல்லுனர்களை உருவாக்க வேண்டும்.

“இணையத்தள நிபுணர்களின் தேவைக்கும் வினியோகத்திற்கும் பாரிய இடைவெளி காணப்படுகின்றது. இந்த இடை வெளிகளை தொடர்ச்சியாக மதிப்பீடு செய்வதன் மூலமாக சைபர் பாதுகாப்பு நிபுணர்களின் தேவைக்கு ஏற்ப நிரம்பல் செய்யலாம். மற்றும் இணைய பாதுகாப்பு அறிவை வளர்த்து கொள்வதற்காக அது தொடர்பான கற்றல் வாய்ப்புக்களை அதிகரிப்பதுடன் எதிர்கால சைபர் பாதுகாப்பு செயற்பாடுகளில் ஈடுபடுவதற்கு இளைஞர் அணி ஒன்றையும் திரட்டுதல் வேண்டும்.



## எங்களது ஆரம்பம்

### 3.1. தொழில் நிபுணர்களின் கேள்வி மற்றும் நிரம்பல் அளவை மதிப்பீடு செய்தல்.

சைபர் பாதுகாப்பு மற்றும் தகவல் தொழில்நுட்ப நிபுணர்களின் கேள்வி நிரம்பல் தொடர்பான ஆய்வினை நாங்கள் நடாத்திட்டுள்ளோம். அத்தகைய பகுப்பாய்வானது ஜேஊரெயு நிறுவனத்துக்கு அவசியமாக இருப்பதோடு அந்த நிறுவனம் இந்த விடயம் தொடர்பாக கொள்கைகளை வகுப்பதற்கும். பொருத்தமான விபூகங்களை செயற்படுத்துவதற்கும் கேள்விக்கும் நிரம்பலுக்கும் இடையிலான இடைவெளியை கண்டறிவதற்கும் அவசியமாக இருக்கும்.

### 3.2. தேர்ச்சி மிக்க செயற்பாட்டு கட்டமைப்பு

நாம் ஒரு தேசிய தகவல் மற்றும் சைபர் பாதுகாப்பு தொடர்பான தேர்ச்சி மிக்க செயற் கட்டமைப்பு ஒன்றை உருவாக்குவோம். அதன் மூலமாக அரசாங்க மற்றும் தனியார் நிறுவனங்கள் வினைத்திறன் மிக்க சைபர் சுற்றாடலில் செயற்படுவதற்கான வேலை கட்டமைப்பு ஒன்றை விருத்தி செய்வோம் அத்துடன் இந்த கட்டமைப்பு செயற்திட்டத்தில் அரசாங்கம் மற்றும் தனியார் நிறுவனங்கள் கவணத்திற் கொள்ளப்படும்

3.2.2 நாங்கள் தகவல் மற்றும் சைபர் பாதுகாப்பு துறையில் தேசிய தொழில் தகுதி தரத்தை மேம்படுத்துவதற்கு (NVQ) முன்றாம் நிலை தொழிற் கல்வி ஆணைக்குழுவுடன் இணைந்து பணியாற்றுவதற்கு முடிவு செய்துள்ளோம். முன்மொழியப்பட்ட தேசிய தகவல் மற்றும் சைபர் பாதுகாப்பு கட்டமைப்பு தொடர்பாக சர்வதேச தரநிலை அமைப்புக்களால் வரையறுக்கப்பட்ட தொழில் முறை தகுதி நிலையுடன் இணைந்த வகையில் இருக்க வேண்டும்.

### 3.3. பொது துறை ஊழியர்களுக்கான திறன் மேம்படுத்தல் மற்றும் திறன் மீளாய்வு செய்யும் சந்தர்ப்பங்களை வழங்குதல்.

தகவல் தொழில்நுட்ப சேவையில் ஓவ்வொரு தரத்தில் இருக்கும் ஊழியர்களுக்கும் தேசிய தொழில் சான்றிதழ் ஏடு வழங்கப்படும் மற்றும் சேவையில் இருப்பவர்களும் தகவல் தொழில்நுட்ப சேவைக்கு இணைத்துக்கொள்ளப்படுவார்கள்.

தேசிய தொழில் சான்றிதழ் தரத்துக்கு அமைவாக (NVQ) விசேடமான பயிற்சி நெறிகளை முககியமான விடயங்களை கையாளும் முகவர் அமைப்புக்கு வழங்குவதற்கு தீர்மானித்துள்ளோம். நமது சமுதாயத்தில் இருக்கும் மிகவும் பாதிக்கப்பட்ட மக்களுக்காக சட்டத்தை அமுல்படுத்துகின்ற முகவர்களுக்கும் முப்படைகளின் இருக்கும் புலனாய்வு பிரிவினருக்கும் நாங்கள் இது தொடர்பாக பயிற்சியளிப்பதற்கு திட்டமிட்டுள்ளோம்.

3.3.1. தகவல் மற்றும் சைபர் பாதுகாப்பு செயற் கட்டமைப்பின் மூலமாக அரசாங்க நிறுவனங்களில் இருக்கின்ற அடிமட்ட ஊழியர்களுக்கும் சைபர் பாதுகாப்பு தொடர்பான பயிற்சி நெறிகளை வழங்குவதற்கு தீர்மானித்துள்ளோம்.

3.3.2. அரச ஊழியர்களுக்கு இந்த துறையில் சிறப்பு பட்டப்படிப்புக்களை மேற்கொள்வதற்கும் பட்ட பின்படிப்புக்களை மேற்கொள்வதற்கும் மற்றும் இந்த துறையில் தொழிற் தகமை பயிற்சிகளை மேற்கொள்வதற்கும் நாங்கள் புலமை பரிசீலகளை வழங்குவதற்கு தீர்மானித்துள்ளோம்.

3.3.3. பொது சேவைக்காக நடாத்தப்படுகின்ற வினைத்திறன் பரீட்சைகளில் சைபர் பாதுகாப்பு தொடர்பான விடயங்களையும் சேர்த்துக்கொள்ள தீர்மானித்துள்ளோம்.

### 3.4. முன்றாம் நிலை மற்றும் தொழிற்கல்வி திட்டங்களை விரிவுப்படுத்தல்

- 3.4.1. உள்நாட்டு பல்கலைக்கழகங்களுக்கும், தொழிற்கு பயிற்சி நிறுவனங்களுக்கும், தனியார் துறை மூலமாக கல்வி சேவையை வழங்குவதற்கும்கூட தொழிற்கு துறையை மையப்படுத்தி டிப்ளோமா பாடநெறிகளை வழங்குவதற்கும் மற்றும் பட்ட பின்பு பாடநெறிகளை வழங்குவதற்கும், பாட வழங்குவதற்கு சந்தர்ப்பத்தை ஏற்படுத்தி கொடுக்க தீர்மானித்துள்ளோம் உயர்தரமான சைபர் பாதுகாப்பு திறனை பெற்றுக்கொள்வதற்கு சைபர் பாதுகாப்பு தொடர்பாக செயல் முறை பயிற்சிகளையும் கோட்பாட்டு பயிற்சிகளையும் வழங்குவதற்கு தீர்மானித்துள்ளோம்.
- 3.4.2. தனியார் தொழில் நிறுவனங்களுக்கு இந்த துறையில் தொழில் ரீதியான தகமைகளை பெற்றுக்கொள்வதற்கு நாங்கள் உதவுவோம்.

### 3.5. நாடு முழுவதிலும் பயிற்சி கட்டமைப்புக்களை உருவாக்கல்

- 3.5.1. பொது துறை மற்றும் தனியார் துறையின் பங்களிப்புடன் தகவல் மற்றும் சைபர் பாதுகாப்பு தொடர்பான விடயங்களில் அவர்களுக்கு பயிற்சியளித்து இந்த கட்டமைப்பை விருத்தி செய்வதற்கு உதவுவோம்.
- 3.5.2. அரசாங்க பயிற்சி நிறுவனங்களுக்கு (இலங்கை நிருவாக அபிவிருத்தி நிறுவனம் மற்றும் உள்ளூராட்சி நிறுவனங்கள் என்பனவற்றுக்கு தகவல் தொழில்நுட்பம் சைபர் பாதுகாப்பு தொடர்பான விடயங்களில் அரசாங்க ஊழியர்களுக்கு பயிற்சியளிக்க உதவுவோம்.

### 3.6. மின் - கற்றல் தொகுதிகள் (மொடியூல்கள்)

புதிதாக தொலை தொடர்பு கற்றல் மையங்களை நிறுவுவதற்கு ஊக்கமளிப்போம் அத்துடன் அரசாங்க ஊழியர்களின் கற்றல் செயற்பாடுகளை ஊக்குவிப்பதற்காக தகவல் தொழில்நுட்பம் மற்றும் சைபர் பாதுகாப்பு போன்ற விடயங்களில் கற்றல் மொடியூல்களை வடிவமைத்து வழங்குவோம்.

### 3.7. சர்வதேச மாநாடுகளில் கலந்து கொள்வதற்கான அரசு ஊழியர்களுக்கான வாய்ப்புக்கள்.

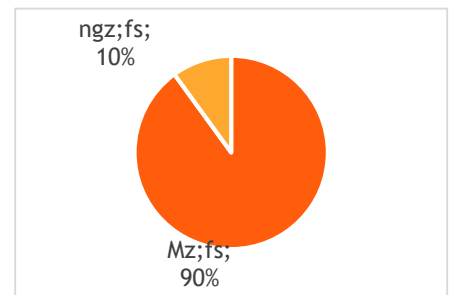
சர்வதேச ரீதியாக தகவல் தொழில் நுட்ப மாநாடுகளில் பங்குபற்றி பங்களிப்பு செய்தல் மற்றும் ஏனைய செயற்பாட்டாளர்களுடன் ஆழமான தொடர்புகளை பேணி எமது நிலையை நிலைநிறுத்தல் என்பன முக்கியமான

விடயங்களாகும். இத்தகைய சர்வதேச மாநாடுகளில் கலந்துகொள்வதின் நோக்கம் தகவல் தொழில்நுட்பம் மற்றும் சைபர் பாதுகாப்பு தொடர்பான அறிவை பெற்றுக்கொள்வது மட்டுமல்ல உலக முழுவதிலும் உள்ள இணைய பாதுகாப்பு தொடர்பான நிபுணர்களுடன் தொடர்பினை ஏற்படுத்தி கொள்வதற்கும் நாங்கள் உதவுகின்றோம். சர்வதேச தொடர்புகளை வெளிநாட்டு வள திணைக்களத்துடன் இணைந்து பொது சேவையில் இருக்கும் தகவல் பாதுகாப்பு உத்தியோகத்தரகர்களுக்கும் இந்த வாய்ப்புக்களை தருவதற்கு நாங்கள் உத்தேசித்துள்ளோம்.

### 3.8. எதிர்கால செயற்பாடுகளுக்கான வழிகள்

- 3.8.1. எதிர் காலத்தில் பாதுகாப்பு தொடர்பான விடயத்திலும் தகவல் தொழில்நுட்ப துறையிலும் ஒரு நிபுணத்துவம் மிக்க அணியினரை உருவாக்குவதற்காக பாடசாலை பாடவிதானத்தில் சைபர் பாதுகாப்பு மற்றும் தகவல் தொழில்நுட்பம் போன்ற துறைகளை சேர்த்து கொள்வதற்கு நாங்கள் பங்களிப்பினையும் சிபாரிசுகளையும் செய்வோம்.
- 3.8.2. க.பொ.த (c) பூர்த்தி செய்து வெளியேறும் மணவர்களுக்கு இந்த துறையில் எத்தகைய வேலை வாய்ப்புக்கள் இருக்கின்றது என்ற வழிப்புணர்வு கூட்டங்களை நடாத்துவோம் இதற்காக நாடு முழுவதிலும் தொழில் வழி காட்டி பயிற்சி நெறிகளை நடாத்துவதற்கு நாங்கள் திட்டமிட்டுள்ளோம்.
- 3.8.3. பெண்களுக்கு சைபர் பாதுகாப்பு துறையில் நிறைய வேலைவாய்ப்புக்கள் இருக்கின்றன உலகலாவிய ரீதியில் இதற்கான பெண்களின் பங்களிப்பு 11% மாகவே இருக்கின்றது இது உலக தொழிற்படையின் எண்ணிக்கையோடு ஒப்பிடுகின்ற போது இது மிகவும் தாழ் மட்டமாகும்.

பெண்கள் இணைய பாதுகாப்பு தொழில்களின் (ஆசியா பசிபிக் பிராந்தியம்) <sup>10</sup>



இந்த துறையில் பெண்களின் பங்களிப்பு குறைவாக கானப்படுகின்றமையால் அது தொடர்பான வழிப்புணர்வு கூட்டங்களை நடாத்தி பெண்களுக்கு இதில் ஆர்வத்தை ஏற்படுத்துவதற்கு உத்தேசிக்கப்பட்டுள்ளது அத்துடன் பாடசாலை மட்டத்திலும் இதற்கான செயற்பாடுகளை மேற்கொள்வதற்கு திட்டமிடப்பட்டுள்ளது.

## உந்தல் 4: டிஜிட்டல் அரசாங்க உள்ளக கட்டமைப்பு

### எங்களது மூலோபாயம்

டிஜிட்டல் அரசாங்க முன்முயற்சிகள் பொது மக்களுக்கு சிறந்த பயனை தந்துள்ளது. அத்தகைய சேவைகள் சைபர் தாக்குதலினால் அதிகளவில் பாதிக்கப்பட்டுள்ளது. மற்றவர் தாக்குதல்கள் மற்றும் சட்டவிரோதமாக இணைய தளத்தில் உள்நுழைதல் போன்ற சம்பவங்களும் சேவைகளை இயங்கிவிடாமல் தடுத்தல் போன்ற நடவடிக்கைகளும் மேற்கொள்ளப்பட்டுள்ளன. அரசாங்க சேவைகள் மீதான சைபர் தாக்குதல்கள் பொது சேவை வழங்களுக்கு கணிசமான பாதிப்பினை ஏற்படுத்துகின்றது. இதன் மூலமாக பொது மக்களின் நம்பிக்கை இழக்கப்படுகின்றது. அரசாங்கம் தகவல்களை பாதுகாப்பாக வைத்திருக்கவிட்டால் பொது மக்கள் அதன் மீதான நம்பிக்கையை இழந்துவிடுவார்கள். எனவே டிஜிட்டல் அரசாங்கமுறையில் தகவல்களை கவணமாகவும் பாதுகாப்பாகவும் வைத்திருக்க வேண்டியது அவசியமாகும்.

டிஜிட்டல் அரசாங்க அமைப்பு மற்றும் அதன் கட்டமைப்பில் உள்ள பலவினங்களையும் பாமிப்பக்களையும் கண்ட பிடித்த அடையாளம் காணப்பட்ட பலவினங்களை கறைப்பதற்காக பொரத்தமான பாதகாப்ப நடவடிக்கைகளை எடப்பதற்க மன்னரிமை கொடக்கப்படம். இஅத்தடன் தகவல் மற்றும் சைபர் பாதகாப்ப தொடரில் எழுகின்ற பிரச்சினைகளை கண்டறிவதற்கம் அத தொடர்பான மதிப்பிடடைநடாத்தவதற்கம் பங்கதார்களக்க உதவவொம்.

“எங்களின் மூலோபாயம் அரசாங்க துறையில் அனைத்து மட்டங்களிலும் டிஜிட்டல் முஜற மற்றும் டிஜிட்டல் ககட்டமைப்பு என்பன சைபர் தாக்குதலினால் பாதிக்கப்படுகின்றது இதனை சமாளிப்பதற்கு பொருத்தமான நிறுவன மட்டத்தில் உபாயங்களை அமுல்படுத்தி மற்றும் சரியான பாதுகாப்பு கொள்கைகளை நடைமுறைப்படுத்தி இந்த பாதிப்புக்கள் தொடர்பாக அரசாங்க மட்டத்தில் இருக்கின்ற அனைவருக்கும் விழிப்புணர்வு செயற்திட்டங்களை முன்னெடுக்க வேண்டும்.”



### எங்களது ஆரம்பம்

#### 4.1. தகவல் மற்றும் சைபர் பாதுகாப்பு அபாய மதிப்பிட

4.1.1. அரசாங்கத்தறையில் தனியார் தறையில் மெற்கொள்வொம் அபாயகரமான தகவல் தகவல் மறைகளை கையாளகின்ற நிறுவனங்கள் தொடர்பாக நாங்கள் மதிப்பிட ஒன்றை மெற்கொள்வொம்.அத தொடர்பான அத்தகைய அபாயகரமான தகவல் மறைகளை கையாளகின்ற நிறுவனங்கள் தொடர்பில் தகவல்களை திரட்டி அவற்றக்க உதவவதற்கான செயற்பாடகளை மெற்கொள்வொம்.



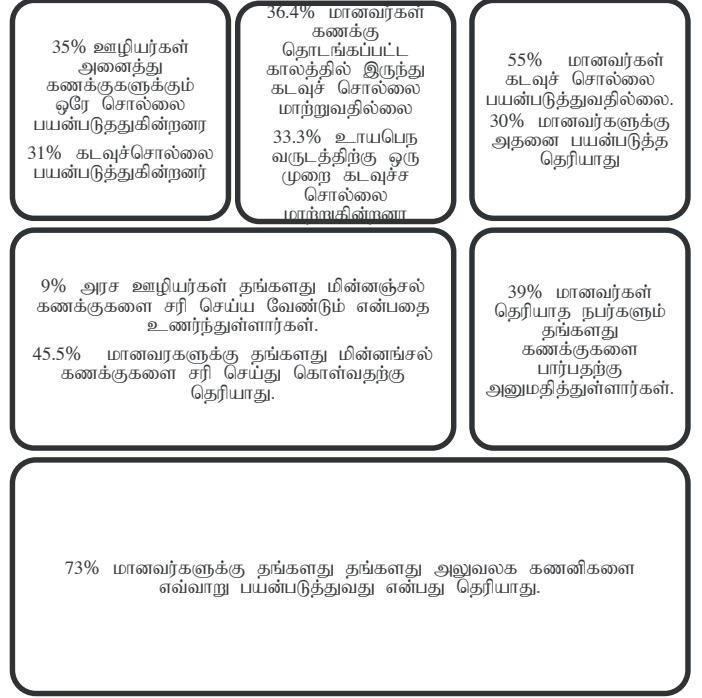
#### 4.2. டிஜிட்டல் அரசாங்க கட்டமைப்பு பாதகாப்பு முறை

தேசிய ஒருங்கிணைந்த சைபர் பாதகாப்பு முகவர் நிறுவனத்தின் (NICS) மூலமாக டிஜிட்டல் அரசாங்கத்தின் உள்கட்டமைப்பில் பாதிப்பினை ஏற்படுத்தக்கின்ற விடயங்கள் தொடர்பாக எழுகின்ற அபாயங்கள் மற்றும் பயமுறுத்தல்கள் தொடர்பான விடயங்களை கையாள்வதற்காக தனியான பிரிவு ஒன்றை அமைப்பதற்கு தீர்மானித்துள்ளோம். இந்த அமைப்பு குறிப்பிட்ட நிறுவனங்களுடன் இணைந்த பாதிப்பை ஏற்படுத்தக்கின்ற விடயங்களை பகப்பாய்வு செய்து போதிய தடுப்புகள் நடவடிக்கைகளையும் எச்சரிக்கைகளையும் கொடுத்தற்கு பொறுப்பாக இருக்கும். இந்த அமைப்பின் மூலமாக பல வகையான பயிற்சிகளை ஒருங்கிணைப்போம் இந்த பயிற்சிகள் மூலமாக எழுப்பி பாதிப்புக்களை அடையாளம் கண்டு அதற்கான தீர்வினை வழங்குவோம்.

#### 4.3. டிஜிட்டல் அரசாங்க உள்கட்டமைப்பு பாதுகாப்பு அலகு

- 4.3.1. தகவல் மற்றும் சைபர் பாதகாப்பு பற்றி இலங்கை அதிகாரிகள் மத்தியில் விழிப்பணர்வு ஏற்படுத்தலாம் என நம்பப்படுகின்றது. எனவே டிஜிட்டல் சற்றாடலில் செயையாற்றுவதற்காக அரசாங்க அதிகாரிகளை தயார்நிலைப்படுத்துவதற்காக பொதுத்துறை உழியர்களிடம் அவ்வப்போது சைபர் மற்றும் தகவல் தொழில்நட்பம் தொடர்பான ஆய்வுகள் மேற்கொள்ளப்படுகின்றன
- 4.3.2. அரசாங்க உழியர்கள் சைபர் பாதகாப்பு மற்றும் தகவல் தொழில்நட்ப அரசாங்க சூழலில் பணியாற்றுவதற்கு தேவையான சூழலை ஏற்படுத்தி அதற்கு தேவையான திறன்களையும் பாதுகாப்பினையும் ஏற்படுத்தி கொடுப்பதே எமது நோக்கமாகும்.

#### 4.4 தலமை தகவல் பாதகாப்பு உத்தியோகத்தர் மற்றும் டிஜிட்டல் பாதகாப்பு உத்தியோகத்தர்.



4.4.1 சைபர் பாதகாப்பு தொடர்பான விடயங்களை கவனிப்பதற்காகவும் அதனை முகாமைத்துவம் செய்வதற்காகவும் “தலமை தகவல் பாதகாப்பு உத்தியோகத்தர்” ஒருவரை நியமிப்பதற்கு தீர்மானிக்கப்பட்டுள்ளது இந்த பதவியானது அரச நிறுவனங்களின் தகவல்களை பாதுகாக்கும் மிக உயர்ந்த பதவியாக கருதப்படுகின்றது.

4.4.2 அரச பொது நிறுவனங்களில் தகவல் தொழில்நட்பத்தை பயன்படுத்துவதற்காக நாங்கள் தலமை தகவல் உத்தியோகத்தர் என்ற பதவியை உரவாக்கி அதன் மூலமாக அரச ஊழியர்களின் தகவல் தொடர்பாடல் திறனை விருத்தி செய்வதற்கான செயற்பாடுகளை முன்வைப்போம்.

4.4.3 சைபர் (உந்தல் இலக்கம் 3) ஊடாக பாதகாப்பு மற்றும் தகவல் தொழில்நட்பம் தொடர்பாக வினைத்திறன் கட்டமைப்பு ஒன்றின் மூலமாக நாடு முழுவதிலும் இருக்கின்ற அரச உழியர்களுக்கு நாங்கள் பயிற்சியளிப்பதற்கு தீர்மானித்துள்ளோம்.

4.5 தலைமை தகவல் பாதுகாப்பு அதிகாரி மற்றும் தகவல் பாதுகாப்பு அதிகாரிகள்

4.5.1 பாதுகாப்பான வடிவமைப்பு என்பது ஒரு சிறந்த நடவடிக்கையாகும் இதன் மூலமாக அரசாங்கம் தனது நடவடிக்கைகளை முன்னெடுப்பதற்கு இலகவாக இருக்கின்றது இதன் மூலமாக அபாயகரமான வேலைகளை சமாளிப்பதற்கான செயற்திட்டங்களும் உள்ளடக்கப்பட்டிருக்கும். இதன் மூலமாக பிரச்சினைகளுக்கு தீர்வு காண்பதற்கு நாங்கள் ஊக்கமளிப்போம் டிஜிட்டல் அரசாங்க அமைப்ப மற்றும் டிஜிட்டல் கட்டமைப்பு போன்ற கோட்பாடுகளை முன்வைத்து இந்த பிரச்சினைகளுக்கு தீர்வு காணலாம்.

4.5.2 நாங்கள் அரசாங்க கொள்முதல் திணைக்களத்துடன் இணைந்து அதன் சட்டதிட்டங்களுக்கு அமைவாக பொருட்களை கொள்வனவு செய்கின்றோம்.

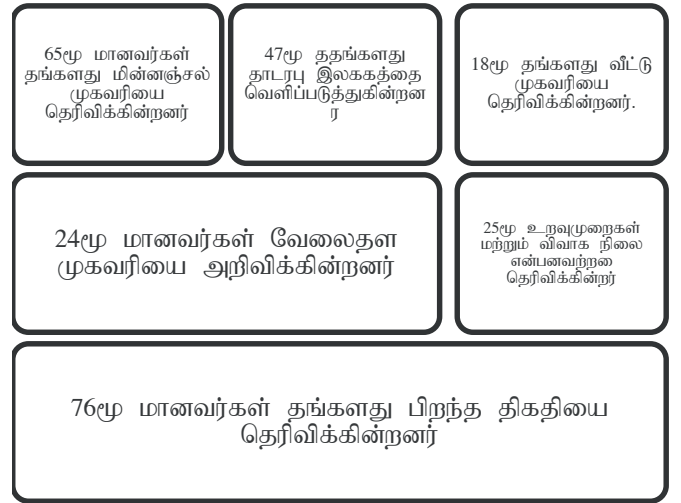
உந்தல் இலக்கம் 5: பொது மக்களக்க விழிப்பணரவூட்டதலம் வலவூட்டதலம்.

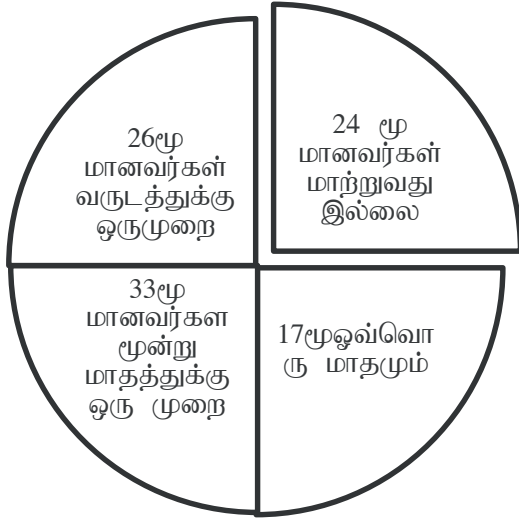
எங்களது மூலோபாயம்

இணையதளமானது நாளாந்த வாழ்க்கையில் மிகவும் முக்கியமானதாக கருதப்படுகின்றது. கல்வி, நாளாந்த வேலைகள், மற்றும் சமூக பங்களிப்பு போன்ற விடயங்களுக்கு இது முக்கியமானதாக காணப்படுகின்றது. சமூதாயத்தில் ஒரு பிரிவினர் மேலும் மேலும் இணைதளத்தினை நம்பி வாழ்கின்றனர். அதன் காரணமாக அவர்கள் சைபர் குற்றச்செயல்களுக்கு ஆளாகின்றனர். பெரும்பாலும் அவர்கள் சைபர் தாக்குதலுக்கு ஆளாவதற்கான முக்கிய காரணம் அவர்கள் அதைப்பற்றி குறைவான அறிவு உடையவர்களாக இருப்பதாகும். கடன் அட்டை இலக்கங்கள் அதிகாரம் இன்றி சமூக ஊடக வலைத்தளங்களுக்குள் பிரவேசித்தல் என்பன பொது மக்களுக்கு அது பற்றியதான போதிய அறிவினமையே காரணமாகும். சைபர் தாக்குதல்கள் மற்றும் சைபர் திருட்டு சம்பந்தமாக பொதுமக்களுக்கு தெளிவினை கொடுப்பது அவசியமாகும். சைபர் அச்சுறுத்தலில் இருந்து மக்களை பாதுகாப்பதற்கான அறிவினையும் திறனையும் கொடுப்பது முக்கியமாகும்.

சமூக ஊடகங்கள் தொடர்பாக இலங்கையிலுள்ள இளைஞர்கள் மத்தியில் காணப்படுகின்ற அடையாளங்கள் மற்றும் தனியுரிமை தொடர்பான சில குறிப்புகள்.

இளைஞர்களால் சமூக ஊடகங்களின் கடவுச் சொல்லை மாற்றுவதல்





## எங்களது தொடக்கம்

### 5.1. தேசிய தகவல் மற்றும் சைபர் பாதுகாப்பு தொடர்பான ஆயத்தநிலை மதிப்பீடு.

தேசிய புள்ளிவிபரவியல் திணைக்களத்துடன் இணைந்து இலங்கை மக்களுடைய சைபர் பாதுகாப்பு தொடர்பான விடயங்களையும் மற்றும் அது தொடர்பான பொது மக்களின் அறிவு திறன் மனப்பாங்கு தொடர்பான விடயங்களையும் பாதுகாப்பு நடவடிக்கைகள் தொடர்பாகவும் ஷெட்படை ஆய்வுகளை நடாத்துகின்றது..

### 5.2. பொதுமக்களுக்கு சமூக ஊடகங்கள் தொடர்பான சைபர் பாதுகாப்பு விழிப்புணர்வு கூட்டங்கள்.

சைபர் பாதுகாப்பு தொடர்பாக செயற்படுவதற்கு விரிவான பொருட்கள் மற்றும் செயற்பாடுகள் தொடர்பான செயற்பாட்டு தொகுதியை உருவாக்குதல். அத்துடன் அதனுடன் இணைந்த பாதிக்கப்படும் பொதுமக்கள் முறையிடுவதற்கான செயற்திட்டம் ஒன்றையும் உருவாக்குதல்.

5.2.1. விழிப்புணர்வு பிரச்சாரங்களை வழங்குவதன் மூலமாக பொது மக்கள் மத்தியில் சைபர் பாதுகாப்பு தொடர்பான விழிப்புணர்வை அதிகரிப்போம் அத்துடன் பொது மனாடுகள் மற்றும் தெருநாடகங்கள் ஊடாக பிரச்சாரங்களை முன்னெடுப்போம்.

5.2.2. இளைஞர்கள் பெண்கள் உட்பட சமுதாயத்தில் இருக்கும் வயதானவர்கள் சமுதாயத்தில் அதிகம் பாதிக்கப்படுபவர்கள் தொடர்பில் நாங்கள் அதிகம் கவணம் செலுத்துவோம்.

5.2.3. நாங்கள் அச்சு ஊடகங்கள் மற்றும் இலக்ட்ரோனிக் ஊடகங்கள் என்பனவற்றை பயன்படுத்தி மக்களை அடைவதற்கு உத்தேசித்துள்ளோம் அவை மூன்று மொழிகளையும் கொண்டிருக்கும் நாங்கள் தகவல் பாதுகாப்பை உறுதிப்படுத்துவதற்காக அதனை அதிகரிப்பதற்காகவும் சமூக ஊடகங்களை அதன் கருவியாக பயன்படுத்துவோம்.

5.2.4. நன்கு அறியப்பட்ட அரசாங்க வலைத்தளங்களின் உள்ளடக்கத்தையும் நாங்கள் மேம்படுத்துவோம் CCCC உதாரணமாக

(e.g. www.gov.lk, www.news.gov.lk, www.defence.gov.lk) தகவல் மற்றும் சைபர் பாதுகாப்பு தொடர்பான சாதனகங்களை பெற்றுக்கொள்ளல். (e.g. presentations, and webinars). அரசாங்க அழைப்பு மையம். (1919) சைபர் பாதுகாப்பு தொடர்பான அடிப்படை விடயங்களை இதன் மூலமாக தெரிந்துக்கொள்ளலாம்.

“எங்களது உபாயங்கள் நாட்டின் பிரஜைகளுக்கு சைபர் இடைவெளியினால் ஏற்படும் அச்சுறுத்தல் தொடர்பாக விழிப்புணர்வை ஏற்படுத்தல் மற்றும் அவர்களின் அடையாளத்தையும் அவர்களது தனியுரிமையையும் பொருளாதார சொத்துக்களையும் பாதுகாத்தல்”



**5.3. பாடத்திட்டங்களில் தகவல் தொழில்நுட்பம் மற்றும் சைபர் பாதுகாப்பு தொடர்பான அறிமுகம்.**

- 5.3.1. பாடசாலை பாடத்திட்டத்தில் தகவல் தொழில் நுட்ப பாடத்தில் தகவல் மற்றும் சைபர் பாதுகாப்பு தொடர்பான விடயங்களை உள்ளடக்குவதற்கு கல்வி அமைச்சு மற்றும் தேசிய கல்வி நிறுவனம் என்பனவற்றுக்கு நாங்கள் தேவையான வசதிகளை செய்து கொடுப்போம்.
- 5.3.2. பாடசாலை பிள்ளைகள் மத்தியிலும் பல்கலைக்கழக மாணவர்கள் மத்தியிலும் சைபர் பாதுகாப்பு தொடர்பான விழிப்புணர்வு விடயங்களை ஏற்படுத்துவதற்கு கல்வி அமைச்சுக்கும் நாங்கள் வசதிகள் செய்து தருவோம் அத்துடன் (சைபர் பாதுகாப்பு தொடர்பான கையேடுகள்) பாடசாலைகளுக்கு சுற்று நிருபங்களை அனுப்புதல் போன்ற விடயங்களின் மூலமாக நவீன சைபர் அச்சுறுத்தல் தொடர்பான விடயங்களை தெளிவுப்படுத்துவோம்.

**5.4. வாழ்நாள் முழுவதும் கற்கும் வாய்ப்புக்கள்**

திறந்த பல்கலைக்கழகம் மற்றும் பயிற்சி நிறுவனங்கள் பலவற்றுடன் இணைந்து நாம் பெரியவர்களுக்கான அடிப்படை தகவல் மற்றும் சைபர் பாதுகாப்பு தொடர்பான பயிற்சி நெறிகளை வடிவமைத்து திறந்த பல்கலைக்கழகம் மற்றும் தொலைக்கல்வி நிலையங்கள் என்பனவற்றின் ஊடாகவும் நெசலா நிறுவனங்கள் ஊடாகவும் நாடு முழுவதும் பரந்தளவில் பயிற்சி நெறிகளை வழங்குவதற்கு தீர்மானித்துள்ளோம்.

**5.5. உபகரணங்களின் பாதுகாப்பு தொடர்பாக பொதுமக்கள் மத்தியில் விழிப்புணர்வை ஏற்படுத்தல்.**

நாங்கள் இலங்கை தரநிர்ணய நிறுவனத்துடன் இணைந்து தகவல் தொழில் நுட்ப சாதனங்களின் பாதுகாப்பு தொடர்பாகவும் அதன் தரம் தொடர்பாகவும் உறுதி செய்வதற்கு அவர்களுக்கு ஒத்துழைப்பு வழங்குவோம். அத்துடன் தகவல் தொழில் நுட்ப சாதனங்களை உற்பத்தி செய்யும் நிறுவனங்களுடன் இணைந்து தரங்குறைந்த பொருட்களை சந்தைப்படுத்தலை தடுப்போம். அத்துடன் வினைத்திறன் மிக்க தொர்பாடலை பொது மக்கள் மத்தியில் ஏற்படுத்தி பாதுகாப்பு மட்டங்களையும் பாதுகாப்பு அம்சங்கள் பற்றியும் விளக்கமளிப்போம்.

**உந்துதல் இலக்கம் 6: பொது –தனியார் உள்ளூர் - சரவதேச அமைப்புக்களுடன் கூட்டு அபிவிருத்தி**

**எங்களது மூலோபாயங்கள்**

இலங்கை சைபர் சமுதாயமானது சர்வதேச சமூகத்தின் ஒரு அங்கமாக கருதப்படுகின்றது. அது பல்வேறு பிரச்சினைகளுக்கு முகம் கொடுக்கின்றது. சமூக தாக்கம், ட்ரோஜன் தாக்குதல், மேல்வேர் தாக்குதல், பிஸிங் தாக்குதல் உயர்தரமான தூண்டல் தாக்குதல் நிதி மோசடிகள் இத்தகைய பாதகமான விளைவுகளை இலங்கை இணையதள சமுதாயம் எதிர்கொண்டுள்ளது.

அரசாங்கம் தனியாக இந்த அச்சுறுத்தலை எதிர்த்து நிற்க முடியாது என்பதை இலங்கை அரசாங்கம் ஒப்புக்கொண்டுள்ளது. பயனாளர்களின் கூட்டு முயற்சி கல்வியலாளர்கள் மென்பொருள் வண்பொருள் விற்பனையாளர்கள், தனியார் கட்டமைப்பு உரிமையாளர்கள் போன்றோர் இந்த சைபர் தாக்குதலை தடுப்பதற்கு முக்கியமானவர்களாக கருதப்படுகின்றார்கள். சைபர் தாக்குதலை எந்தவொரு நாடும் தனித்து நின்று வெற்றிகொள்ள முடியாது பெரியளவில் அதற்கு சர்வதேச ஒத்துழைப்புகள் தேவைப்படுகின்றது. அப்போதுதான் சைபர் தாக்குதல்கள் மூலமாக வலைப்பின்னல் சேவையை சீர்குழைக்கும் செயற்பாட்டாளர்களை நாம் வெற்றிக்கொள்ளலாம்.

"

**“எங்களது மூலோபாயம் அரசு நிறுவனங்களுக்கு அப்பாற்பட்டு பொது தனியார் ஒத்துழைப்புடனும் சரவதேச – உள்ளூர் ஒத்துழைப்புடனும் ஒரு பாதுகாப்பான சைபர் சுற்று சூழலை உருவாக்க வேண்டும்”**





## எங்களது ஆரம்பம்

### 6.1 தொலை தொடர்பு நிறுவனங்களுடன் இணைந்து செயற்பட்டு இணைய பாவனையாளர்களை பாதுகாத்தல்.

6.1.1 ஐஎன்என் என்ற அமைப்பானது இலங்கையின் சைபர் பரப்பில் முக்கியமான இடத்தினை கொண்டுள்ளது. சைபர் அச்சுறுத்தலை எதிரகொள்வதற்காக டெல்கோ சேர்ட் என்ற அமைப்பை ஏற்படுத்தி சைபர் தாக்குதலை கையாளும் வகையில் இணைய சேவையை தடுத்தல் அதன் மீது தாக்குதல் நடத்தல் மற்றும் தொலை தொடர்பு துறை ஸ்தம்பிதம் அடைய செய்யும் விடயங்களை தடுப்பதற்கான நடவடிக்கைகளை மேற்கொண்டுள்ளோம்.

6.1.2 சைபர் பாதுகாப்பு தொடர்பாக வாடிக்கையாளர்களுக்கு விழிப்புணர்வுகூட்டுதல் மற்றும் சைபர் பாதுகாப்பு தொடர்பான விடயங்களை செயற்படுத்துவது தொடர்பான விடயங்களில் நாங்கள் கவணம் செலுத்துகின்றோம்.

## 6.2 புகழ்மிக்க சேவை

நாங்கள் தொலை தொடர்பு ஒழுங்குப்படுத்தும் அதிகார சபையுடன் இணைந்து ISPS என்ற அமைப்பின் மூலமாக இணைய புரொட்கோள் சேவையை செயற்படுத்துவதற்கான சாதகமான சூழ்நிலையை உருவாக்க எதிர்பார்த்துள்ளோம். இதன் மூலமாக ஒன்லைன் சேவையாளர்கள் லி முகவரியை பெற்றுக்கொள்வார்கள். இந்த சேவை மூலமாக தீமையான விடயங்கள் பரவுகின்றதை ஒரளவுக்கு குறைக்கலாம்.

### 6.3 முக்கிய தகவல் தொடர்பு உட்கட்டமைப்பு நிறுவனங்களுக்கு பங்கு தாரர் துணைக் குழுவை உருவாக்குதல்

எங்கள் அமைப்பு சிறப்பான உட்கட்டமைப்பை கொண்டுள்ளது அவை அரசு சாராத அமைப்பாக செயற்படுகின்றது. பல தனியார் நிறுவனங்கள் இது தொடர்பாக சிறந்த முக்கியமான சேவையை வழங்குகின்றது. நிதி, அதிகாரம், வலு, போக்குவரத்து, விமான போக்குவரத்து, சுகாதாரம் போன்ற இன்னும் பல விடயங்கள் உள்ளடங்கும்.. தனியாருக்கு சொந்தமான இந்த நிறுவனங்களிடம் இருந்து அரசாங்கம் எந்த சேவையையும் பெற்றுக்கொள்ளாது. இந்த தனியார் நிறுவனங்களுக்கு உதவுவது மிகவும் முக்கியமானதாகும் அவர்களின் தகவல் கட்டமைப்பை பாதுகாப்பது மிகவும் முக்கியமாகும். அவர்களின் தகவல் கட்டமைப்பு தடைபடுகின்றபோது மக்களின் நாளாந்த வாழ்கையும் ஊஜஊ சுற்றாடலின் மூலமாக இத்தகைய தகவல் தொழில்நுட்ப தனியார் அமைப்புக்களுடன் இணைந்து சேவையாற்றுகின்றோம். அத்துடன் அவர்களின் சேவையையும் விரிவுபடுத்த உதவுகின்றோம். இதன் மூலமாக தேவையற்ற தொழில்நுட்ப கோளாறுகளையும் தவிர்த்துக்கொள்ளலாம்.

### 6.4 துறை சார்ந்த அமைச்சுக்களை வலுவூட்டுதலும் அதனூடாக டிஜிட்டல் அரசாங்க முறையை ஏற்படுத்தலும்.

ஒவ்வொரு அமைச்சும் அதன் துறைசார்ந்த விடயத்தில் டிஜிட்டல் அரசாங்க முறையை பாதுகாப்பது மிகவும் முக்கியமானதாகும். அத்துடன் தனது அமைச்சுக்களின் விடயங்களை சைபர் தாக்குதலில் இருந்து பாதுகாப்பதும் மிகவும் முக்கியமானதாகும். ஒவ்வொரு துறைசார்ந்த அமைச்சுக்களும் அபாயகரமான கட்டமைப்புக்களை அடையாளம் காண்பது மிகவும் அவசியமாகும். அதற்கு போதுமான பாதுகாப்பை வழங்குதல் மற்றும் அதனை செயற்படுத்தல் அதற்கு அமைவாக தீர்மானம் எடுத்தலும் முக்கியமாகும்.

## 6.5 ஒரு கூட்டு இராணுவ பாதுகாப்பு மையம் ஒன்றை உருவாக்கள் மற்றும் கூட்டு இராணுவ பாதுகாப்பு செயற்பாடுகளை முன்னெடுத்தல்.

தீங்கிழைக்கும் சைபர் செயற்பாட்டாளர்களை எதிர்கொள்ளும் வகையில் பொலிஸ் மற்றும் உளவுதறை ஆகியவை தனித்தனியாக செயற்படுகின்றன. எனினும் இந்த நிறுவனங்களிடையே ஒருங்கிணைப்பு இல்லாததால் சைபர் அச்சுறுத்தல் தொடர்பான தகவல்களை பகிர்ந்து கொள் முடியாது இருக்கின்றது. இத்தகைய சூழலில் சமபந்தப்பட்ட அதிகாரிகளின் ஈடுபாட்டுடன் எங்களை இணைய பாதுகாப்புக்களை வலுப்படுத்தி எங்களின் துணையுடன் பாதுகாப்பு படைகள் சிறப்பாக செயற்பட முடியும் என்பதை உறுதிப்படுத்தும் வகையில் ஒரு கூட்டு இணையதள பாதுகாப்பு மையம், பாதுகாப்பு சான்றிதழ் என்பனவற்றை உருவாக்குவோம். இதன் மூலம் தனியான இராணுவ பாதுகாப்பு மையம் ஒன்று உருவாக்கப்படுகின்றது. இதன் மூலமாக சைபர் அச்சுறுத்தல்களை இலகுவாக சமாளிக்கலாம்.

## 6.6 தொழில் துறையுடன் ஒத்துழைப்பை மேம்படுத்தல்.

6.6.1 தொழில் துறையினர் கூட்டாக தடுத்தல், முன்னெச்சரிக்கையாக நடத்தல் மற்றும் மீட்பு திறன்களை அதிகரித்தல் போன்ற விடயங்களில் நாங்கள் தொழில் துறையினரை ஊக்குவிப்போம். தொழில் துறையினருக்கு சைபர் அச்சுறுத்தல் தொடர்பான தகவல்களை வழங்குவதற்கு நாங்கள் தனியான செனல் ஒன்றை உருவாக்குவோம். நடுத்தர தொழில் வழங்குவோர் மற்றும் வியாரிகளுக்கு தனியான பொறிமுறையொன்றை உருவாக்குவோம். அவர்கள் தற்போது மெலிசியஸ் சைபர் தாக்குதலினால் பாதிக்கப்பட்டுள்ளார்கள். அவர்களுக்கு முன்னெச்சரிக்கை செயற்பாடுகளை கொடுத்து அவர்களுக்கு அறிவுரை வழங்கப்படும்.

## 6.7 சர்வதேச பங்களிப்பையும் ஒத்துழைப்பையும் வலுப்படுத்தல்

சைபர் ஸ்பேஸ் நிலைத்தன்மையை பேணுவதற்கு பிராந்தியங்களுக்கிடையிலும் நாடுகளுக்கிடையேயும் செயற்பாடுகளை முன்னெடுத்து அதனை வலுப்படுத்துவதற்கு உதவுவோம். சர்வதேச தொலை தொடர்பு சங்கம் (ஐவுரு) நெட்வோக் மற்றும் தகவல் (ISOC)இ (NCCIC) சம்பவம் பதில் பாதுகாக்கும் மன்றம் (FIRST)இ ஐக்கிய நாடுகள் இணைய ஆளுகை மன்றம். (UNIGF) இணைய சமூகம் (ஐஎம்முஊ)இ சர்வதேச இணைய அவதானிப்பு மையம். (ஐஹுடு)இ சர்வதேச பொலிஸார் பாதிக்கப்படுகின்ற தொழில் நுட்ப தகவல்கள் தொடர்பான அச்சுறுத்தல்கள். நவீன வனபொருள் மற்றும் மென்பொருட்களை பெற்றுக்கொள்ளல்.

சைபர் அச்சுறுத்தல் தொடர்பான ஆற்றல்களை அபிவிருத்தி செய்வதற்கு உதவுதல்.

## 6.8 பட்டெபெஸ்ட் (Budapest) உடன்படிக்கை

01 செப்டம்பர் 2015 ம் ஆண்டு இலங்கை சைபர் குற்றங்கள் தொடர்பான ஐரோப்பிய பட்டெபெஸ்ட் உடன்படிக்கையில் கைசாத்திட்டது இந்த உடன்படிக்கையில் கைசாத்திட்ட முதலாவது தெற்காசிய நாடு இலங்கையாகும். சைபர் குற்றங்கள் தொடர்பாக சர்வதேச சட்டங்களுக்கு அமைவாக ஏற்படுத்தப்பட்ட ஒரே அமைப்பு இதுவாகும். சர்வதேச விதி முறைகளை அடிப்படையாக கொண்டு மேம்பட்ட புலனாய்வு விடயங்களை பெறவும். ஐசபர் குற்றங்களை திறம்பட எதிர்க்கும் வகையில் நாடுகளுக்கிடையில் குற்றவியல் மற்றும் நீதி விடயங்களில் ஒத்துழைப்பு தருகின்றது. நாம் பாதுகாப்பான இணையதளம் ஒன்றை உருவாக்குவதற்கு உறுப்பு நாடுகளுடன் இணைந்து செயற்படுகின்றோம்.

## 6.9 சர்வதேச அளவில் எமது செயற்பாட்டை அதிகரித்தல்.

சைபர் பாதுகாப்பு பற்றிய சர்வதேச மாநாடுகளில் கலந்துக்கொள்வதனால் நாம் சர்வதேச அளவில் நமது பயகளிப்பை அதிகரிக்க செய்வதுடன். சர்வதேச நாடுகளுடன் பயிற்சி மற்றும் அனுபவங்களை பகிர்ந்து கொள்வதில் முக்கிய பங்கு வகிக்கின்றோம்.

**6.9 தயாரிப்புக்கள் மற்றும் சேவைகள் பாதுகாப்புக்களை மேம்படுத்துவதற்காக வியாபார பங்களியாக செயற்படுதல்.**

வாடிக்கையாளரின் தனியுரிமையை பாதுகாப்பதற்கும் மற்றும் பாதுகாப்பை உறுதிப்படுத்துவதற்கும் உயர்ந்த பாதுகாப்புடன் சந்தை தயாரிப்புக்களையும் சேவைகளையும் வழங்குமாறு வினயோகஸ்தர்களுக்கு நாங்கள் அறிவுறுத்தல் வழங்குவோம்.

**6.10 ஒரு இணைய பாதுகாப்பு ஆராய்ச்சி கலாசாரத்தை உருவாக்க பல்கலைக்கழகங்களுடன் இணைந்து ஒரு ஒரு பங்குதாரராக செயற்படுதல்**

6.10.1 இலங்கையில் சைபர் ஆராய்சி பண்பாட்டை உருவாக்குவதற்காகவும் அதனை மேம்படுத்துவதற்காகவும் இலங்கை பல்கலைக்கழகங்களுடன் இணைந்து நாங்கள் செயற்படவுள்ளோம்.

6.10.2 நன்கொடையாளர்கள் மற்றும் மற்றும் பல்கலைக்கழகங்களுடன் இணைந்து இணைய பாதுகாப்பு குறித்த ஆராய்சியை மேற்கொள்வதற்கு மாணவர்களுக்கு ஆராய்சி மானிய திட்டங்களை அறிமுகப்படுத்துவோம்.

6.10.3 இந்த களப்பணியல் அனைத்து பங்குதாரர்களுடனும் இணைந்து தொடர்ந்து சைபர் பாதுகாப்பு வாரத்தை அனுஸ்டிப்போம் அத்துடன் அதனை தொடர்ந்து சைபர் பாதுகாப்பு தொடர்பான தேசிய மாநாட்டிற்கு தயாராவோம்.

**6.11 அரச நிறுவனங்கள் மற்றும் சமூக குழுக்கள் மற்றும் அரசசார்பற்ற நிறுவனங்களின் பங்களிப்புக்கள்.**

6.11.1 சமூக மேம்பாடு மற்றும் நலன்புரி அமைச்சு, பெண்கள் மற்றும் குழந்தைகள் விவகார அமைச்சு. சிறுவர் பாதுகாப்பு அதிகார சபை சட்டமற்றும் ஒழுங்கு அமைச்சு ஆகியவை உள்ளடங்கிய அரசாங்க நிறுவனங்களுடன் இணைந்து இது தொடர்பாக கிராம சமுதாயத்தில் விழிப்புணர்வு செயற்திட்டம் ஒன்றை நடாத்துதல். சமூகத்தில் அதிகம் பாதிப்படையும் மக்களுக்கு இணைய பாதுகாப்பு தொடர்பான அறிவுரைகளை வழங்குதல்.

6.11.2 சிவில் சமுதாயத்தின் ஈடுபாட்டுடன் (ஸ்மார்ட் சமூக வட்டங்கள், நெனசெல நிலையங்கள், சமூக நிலையங்கள்) அரசசார்பற்ற நிறுவனங்கள் என்பனவற்றுடன் இணைந்து நாங்கள் கிராமத்தையும் நகரத்தையும் இணைந்த பிரஜைகளை உருவாக்குவதற்கு தீர்மானித்துள்ளோம். அவர்களுக்கு சைபர் அச்சுறுத்தல் தொடர்பான விடயங்களில்

விளக்கமளிப்பதுடன் தரமான ஒன்லைன் சேவைகளை அவர்களுக்கு வழங்குவதற்கு நடவடிக்கைகளை எடுத்துள்ளோம்.

**6.12 வளர்ச்சிக்கான தொடக்கம்.**

நாங்கள் இளம் தொழில் முயற்சியாளர்களுக்கு சைபர் பாதுகாப்பு தொடர்பான விடயங்களை செயற்படுத்துவதற்கு தேவையான ஆலோசனைகளை வழங்குகின்றோம். இலங்கையில் மென்பொருள் உற்பத்திகளிலும் வனபொருள் உற்பத்திகளிலும் ஆர்வமாக இருக்கின்ற நிறுவனங்களுக்கு தீர்வுகளை பெற்றுக்கொடுத்து அவர்களை சிறந்த செயற்பாட்டாளர்களாக மாற்றுவதற்கு நாங்கள் முயற்சி செய்வதுடன் அவர்களுக்கு சரவதேச ரீதியிலும் உள்நாட்டிலும் சந்தை வாய்ப்புக்களை பெற்றுக்கொடுப்பதற்கு நடவடிக்கைகள் எடுப்போம்

**இறுதி குறிப்புகள்**

1. <https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/>
2. [2. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion](https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion)
3. [3. http://www.statistics.gov.lk/education/ComputerLiteracy/ComputerLiteracy-2017Q1-Q2-final.pdf](http://www.statistics.gov.lk/education/ComputerLiteracy/ComputerLiteracy-2017Q1-Q2-final.pdf)
4. [4. http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf](http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf)
5. [5. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2010](https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2010)
6. [6. https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf)
7. [7. http://www.internetworldstats.com/stats3.htm](http://www.internetworldstats.com/stats3.htm)
8. [8. https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg](https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg)
9. [9. http://www.apbsrilanka.org/articales/28\\_ann\\_2016/7\\_28th\\_conv\\_a\\_Jayantha\\_Fernando.pdf](http://www.apbsrilanka.org/articales/28_ann_2016/7_28th_conv_a_Jayantha_Fernando.pdf)
10. [10. https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf](https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf)