AAT SRILANKA EXAMINATION

L E V E L - II

C U R R I C U L U M 2 0 2 0

202 – INFORMATION SYSTEMS IN DIGITAL ENVIORNMENT

(SINHALA MEDIUM CLASS)

BY;

BHAGYA FERNANDO

B.Sc. Business Adminstration (SP) USJP, CA Finalist,
AAT Passed Finalist,
REGISTERED LECTURER OF AAT SRI LANKA

CHAPTER 04
Ethical, Social and Legal Environment for Information Systems
(තොරතුරු පද්ධති සඳහා ආචාරධර්ම, සමාජීය හා නෛතික පරිසරය)

සමාජ ජාල සහ සමාජ මාධ්‍ය (Social Networks and Social Media)

සමාජ ජාල හා සමාජ මාධ්‍ය යනු එක් සංකල්පයක් නොවේ.

සමාජ මාධ්‍ය යනු මිනිසුන් විසින් උඩුගත කරනු ලබන බ්ලොග් අඩවියක්, වීඩියෝවක්, ඉදිරිපත් කිරීමක්, සංගීත බෙදාහැරීමක්, ප්‍රවෘත්ති පත්‍රයක් හෝ විද්‍යුත් ග්‍රන්ථයක් යනාදියයි. එබැවින් සමාජ මාධ්‍ය යනු එක් පාර්ශවයක සිට බොහෝ පාර්ශවයන්ට සන්නිවේදනය කරන ක්‍රමයක් ලෙස සැලකිය හැක. පුද්ගලයින් විසින් මෙසේ උඩුගත කරනු ලබන දෑ, අන්තර්ගතයන් (Content) ලෙස හැඳින්වේ. අනෙකුත් පුද්ගලයන්ට අන්තර්ගතයන් සඳහා අදහස් දැක්වීමට සහ ප්‍රතිචාර දැක්වීමට හැකි වූවත්, අන්තර්ගතයේ හිමිකාරීත්වය එහි මුල් ප්‍රකාශකයා සතුව පවතී.

සමාජ ජාල යනු සබඳතා නිර්මාණය කිරීම, අන් අය සමඟ සමඟ සන්නිවේදනය කිරීම, අනුගාමිකයන් සමඟ සබඳතා ගොඩනැගීම සහ මාර්ගගත ප්‍රේක්ෂකයන් සමඟ සම්බන්ධ වීම යනාදිය සඳහා කිසියම් මාධ්‍යයක නියැලීමයි. Facebook, Twitter, LinkedIn, Youtube, Instagram හා Pinterest යන ආදිය සමාජ ජාල වශයෙන් හඳුනාගත හැක.

සමාජ ජාලකරණයේ ඉලක්කය වන්නේ අන්තර් ක්‍රියා කිරීම, සංවාද කිරීම සහ සංවාද නිර්මාණය කිරීමයි. එකිනෙකා සමඟ සම්බන්ධ වීමට නව ක්‍රම සොයා ගැනීම සඳහා සමාජ ජාලකරණය පහසුකම් සපයයි. ඉහත එකෙක් එක් එක් සමාජ ජාල වල ක්‍රියාකාරීත්වය එකිනෙකට වෙනස් වන අතර උදාහරණයක් වශයෙන් Youtube යනු වීඩියෝ සඳහා වන මෙවලමක් වන අතර එය සමාජ මාධ්‍යයක් ද වේ. LinkedIn යනු වෘත්තීය ප්‍රගමනය සඳහා උපකාර කරනු ලබන අධිකාරීන් සමඟ ගනුදෙනු කිරීමේ හැකියාව සහ පහසුකම සහිත සමාජ ජාලයකි.

මෙකී සමාජ මාධ්‍ය වල පළමුවෙන්ම ඔබ සඳහා පැතිකඩක් (Profile) නිර්මාණය කරගත යුතු අතර ඉන් අනතුරුව මිතුරන් හා අනෙකුත් වෘත්තිමය පාර්ශවයන් සමඟ තම අදහස් හා තොරතුරු බෙදා ගැනීමේ හැකියාව ඇත.

පුද්ගලයින්, සමාජය සහ ව්‍යාපාර කෙරෙහි සමාජ මාධ්‍යයන්හි යහපත් බලපෑම

වර්තමානයේ දී ලෝකයේ සමස්ත ජනගහනයෙන් බිලියන 3ක පමණ ජනගහනයක් සමාජ මාධ්‍ය භාවිතා කරයි. සමාජ මාධ්‍ය මඟින් පවුලේ අය, හිත මිතුරන් සහ ව්‍යාපාරික පුද්ගලයන් සමඟ සම්බන්ධතාවයන් වඩාත් පහසු කර ඇත. එමෙන්ම බොහෝ ඉහළ ඉහල පෙලේ සමාගම් සිය ප්‍රේක්ෂකයන් වෙත සෘජුවම ප්‍රවේශ වීම සඳහා සමාජ මාධ්‍ය වල පහසුකම් භාවිතා කරයි.

ව්‍යාපාර සඳහා සමාජ මාධ්‍යයන්හි යහපත් බලපෑම්

1. තත්කාලීනව කර්මාන්ත ප්‍රවණතාවයන් අනාවරණය කර ගැනීමේ හැකියාව
2. වඩාත් පුළුල් තරඟකාරී විශ්ලේෂනය
3. වඩා හොඳ පාරිභෝගික සේවාව සහ පාරිභෝගික තෘප්තියක් ලබා දීම
4. ගණුදෙනුකරුවන්ගේ අන්තර්ගත සහ කතා (Comments) වලට එකවරම විසඳුම් ලබාදීම
5. බඳවා ගැනීම සඳහා සහාය වීම

පුද්ගලයින් සහ සමාජය කෙරෙහි සමාජ මාධ්‍ය සහ සමාජ ජාලාවල සෘණාත්මක බලපෑම්

1. සයිබර් හිරිහැර කිරීම (Cyber Bullying)

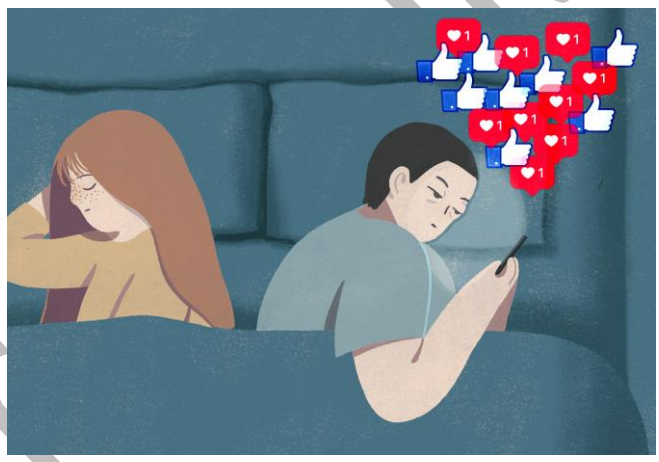
මෙය මාර්ගගත සමාජ කෲරත්වය හෝ ඉලෙක්ට්‍රොනික හිරිහැර කිරීම ලෙස හඳුන්වනු ලැබේ. විශේෂයෙන් පරිශීලකයන් විසින් ව්‍යාජ ගිණුම් සකස් කර ගැනීමෙන් අනතුරුව අනෙක් පුද්ගලයන් හෝ කණ්ඩායම් සඳහා තර්ජනය කිරීම්, බිය ගැන්වීම් හා කටකතා පැතිරවීම යනාදිය හරහා බාධා පැමිණවීම සිදු කෙරේ.

2. සැසීම (Hacking)

පරිගණකයක හෝ තොරතුරු පද්ධතියක ඇති දුර්වලතා හෝ අඩුපාඩුකම් හඳුනාගනිමින් පුද්ගලික තොරතුරු වලට අනවසරයෙන් ප්‍රවේශ ප්‍රවේශ වීම මෙලෙස හැඳින්වේ. මෙම ක්‍රියාදාමය මගින් පොදුවේ පුද්ගලයෙකුගේ පෞද්ගලිකත්වය සහ රහස තොරතුරු උල්ලංඝනය කරනු ලබයි. මෙය අනවසර ප්‍රවේශය ලෙස ද හඳුනා ගත හැක. මෙලෙස ලබාගන්නා තොරතුරු භාවිතයෙන් මූල්‍යමය අලාභ මෙන්ම පෞද්ගලික ජීවිතයටද හානි සිදුකර වීමේ හැකියාවක් පවතී.

3. ඇබ්බැහි වීම (Addiction)

සමාජ මාධ්‍ය කෙරෙහි ඇබ්බැහි වීම ඉතාමත්ම නරක ප්‍රවණතාවයක් වන අතර එය පුද්ගලයින්ගේ පෞද්ගලික ජීවිතය සඳහා ද බාධාවකි. පුද්ගලයින් සෙසු සමාජයෙන් ඈත් වීම මෙහිදී සිදුවේ.



4. කීර්තිය නැතිවීම (Loss of Reputation)

අසත්‍ය තොරතුරු නිර්මාණය කිරීමෙන් සහ සමාජ මාධ්‍ය පුරා පැතිරි වීමෙන් යමෙකුගේ කීර්තිය පහසුවෙන් හානි කළ හැකිය.

හරිත පරිගණකකරණය (Green Computing)

හරිත පරිගණකකරණය නැතහොත් හරිත පරිගණනය යනු පරිගණක සහ ඒවායේ සම්පත් පාරිසරික වශයෙන් වගකීම් සහිතව පරිසර හිතකාමී ලෙස භාවිතා කිරීමයි. ඒ තුළින් පාරිසරික බලපෑම අවම කරන අයුරින් පරිගණක උපාංග සැලසුම් කිරීම, නිෂ්පාදනය කිරීම, ඉංජිනේරුකරණය කිරීම, භාවිතා කිරීම සහ බැහැර කිරීම යන ක්‍රියාවලින් හඳුනාගනී. මෙහිදී බලශක්තිය කාර්යක්ෂම අයුරින් උපයෝජනය කෙරෙන පරිගණක නිපදවීම සහ සම්පත් පරිභෝජනය අවම කිරීම තුලින් විද්‍යුත් අපද්‍රව්‍ය නිසි ලෙස බැහැර කිරීම කෙරෙහි අවධානය යොමු කරනු ලබයි.

ඇමරිකා එක්සත් ජනපදයේ හරිත පරිගණනය සඳහා මුල්ම පියවර වූයේ **energy star** නමින් හැඳින්වෙන ස්වෙච්ඡා ලේබල කිරීමේ වැඩසටහනයි. සියලුම වර්ගයේ දෘඩාංග වල බලශක්ති කාර්යක්ෂමතාව ප්‍රවර්ධනය කිරීම සඳහා 1992 වර්ෂයේදී පරිසර ආරක්ෂණ ඒජන්සිය මගින එය සංකල්පයක් බවට පත් කරන ලදී.

හරිත භාවිතය - පරිගණක සහ වෙනත් තොරතුරු පද්ධති වල බලශක්ති පරිභෝජනය අවම කිරීම මෙන්ම පරිසර හිතකාමී ලෙස භාවිතා කිරීම

හරිත බැහැර කිරීම - පැරණි පරිගණක අලුත්වැඩියා කිරීම සහ නැවත භාවිතා කිරීම, ප්‍රතිචක්‍රීකරණය කිරීම

හරිත සැලසුම් කිරීම - බලශක්ති කාර්යක්ෂම හා පරිසර හිතකාමී, පරිගණක හා ඒවායේ සංරචක සැලසුම් කිරීම

හරිත නිෂ්පාදන - පරිසරයට කිසිදු බලපෑමක් නොමැති හෝ අවම බලපෑමක් ඇති ඉලෙක්ට්‍රොනික උපාංග නිෂ්පාදනය

ගෝලීය පරිසරයට සිදුවන අහිතකර බලපෑම් අවම කිරීම සඳහා පරිගණක පරිශීලකයන් සහ ව්‍යාපාර වලට ගත හැකි පියවර

- දීර්ඝ කාලයක් අකර්මණ්‍යව පවතින සියලුම පරිගණක යන්ත්‍ර සහ පර්යන්ත ක්‍රියා විරහිත කිරීම
- අවශ්‍ය නොවන අවස්ථාවන්හිදී දෘඩාංග ක්‍රියා විරහිත කොට තැබීම
- අවශ්‍යතාවය අනුව භාවිතා කරන බලශක්තිය වෙනස් කරනු ලබන දෘඩාංග භාවිතා කිරීම
- දර්ශන තිර ක්‍රියා විරහිත කිරීම සඳහා බල කළමණාකරන විශේෂාංග (Power Management) භාවිතා කිරීම
- කඩදාසි භාවිතය අඩුකිරීම සහ අඩු කිරීම සහ අපද්‍රව්‍ය කඩදාසි නිසි ලෙස බැහැර කිරීම
- පවත්නා රෙගුලාසිවලට අනුකූලව විද්‍යුත් අපද්‍රව්‍ය බැහැර කිරීම

<u>හරිත පරිගණනය සඳහා අනුගත වීම / පවත්නා බාධක</u>

මෙහිදී පහත සාධක කෙරෙහි අවධානය යොමු කළ යුතුය.

<u>1. අන්තර්ජාලයේ ශීඝ්‍ර වර්ධනය</u>
වර්තමානය වන විට අන්තර්ජාලය පදනම් කරගනිමින් සන්නිවේදන හා අනෙකුත් කාර්යයන් සිදුකර ගන්නා මිනිසුන් ප්‍රමාණය ශීඝ්‍ර ලෙස වර්ධනය වන බැවින් ඔවුන් තැන්පත් කරන හා භාවිතා කරන දත්ත ප්‍රමාණය ඉහළ යෑමක් සිදුවී ඇත. එබැවින් වැඩි වශයෙන් දත්ත මධ්‍යස්ථාන භාවිතා කිරීමට සිදු වී ඇත.

<u>2. උපකරණ බල ඝනත්වය වැඩි කිරීම</u>
විශේෂයෙන්ම සේවා සැපයුම් පරිගණක වල ක්ෂුද්‍ර සකසන මගින් අඩු බලශක්තිය පරිභෝජනයක් සහිතව ඉහළ කාර්ය සාධනයක් ලබාදී ඇතත්, වර්තමානයේ භාවිතා වන මතක ධාරිතාවන් සහ වැඩි බල ශක්තියක් අවශ්‍ය කරන අනෙකුත් උපාංග වැඩි ප්‍රමාණයක් ඒවායේ ස්ථාපිත කර ඇති බැවින්, සමස්ථ බලශක්ති පරිභෝජනය ඉහළ ගොස් ඇත.

<u>3. සිසිලන අවශ්‍යතාවයන්ගේ වැඩිවීම</u>
දත්ත මධ්‍යස්ථාන වල පමණක් නොව වර්තමානය පෞද්ගලිකව භාවිතා කරන පරිගණක වල පවා ඇතිවන තාපයට ඔරොත්තු දීම සඳහා වැඩි වශයෙන් සිසිල් කිරීමේ අවශ්‍යතාවක් පැන නැඟී ඇත.

4. බලශක්ති පිරිවැය ඉහළ යාම

5. බලශක්ති සැපයුම සහ ප්‍රවේශ සීමා කිරීම

<u>6. අඩු සේවාදායක උපයෝගිතා අනුපාත</u>
ඇතැම් අවස්ථාවල සේවාදායක පරිගණක වල ධාරිතාවෙන් සුළු ප්‍රතිශතයක් පමණක් භාවිතා වුවත්, ඒ සඳහා වන පිරිවැයේ අවම වීමක් නොමැත.

<u>විද්‍යුත් අපද්‍රව්‍ය සහ එහි පාරිසරික බලපෑම (E-Waste and It's Impact on the Environment)</u>

සෑම වසරකම ටොන් ගණනින් විද්‍යුත් අපද්‍රව්‍ය නිපදවන අතර ඒවා බැහැර කිරීම විශාල ගැටලුවක් වී ඇත. ඊයම් සහ රසදිය වැනි ලොව දිරාපත් වීමට බොහෝ කාලයක් ගත වන අතර එයට නිරාවරණය වන පුද්ගලයන්ට දිගුකාලීනව ආපසු හැරවිය නොහැකි සෞඛ්‍යමය බලපෑම ඇති වෙයි. තවද මෙම ඊයම් වැනි ලෝහ පසෙහි වාසය ස්වභාවයට හානි කෙරේ. නිපදවන රසායනික ද්‍රව්‍ය ජෛව අවක්‍රමණයට ලක් නොවන අතර ඒවා දීර්ඝ කාලයක් තිස්සේ පරිසරය පවතින අතර එමගින් නිරාවරණ අවදානම් වැඩි වේ. පරිගනක මව් පුවරු වල අසාමාන්‍ය ලෙස රසදිය ඇති අතර නුසුදුසු ලෙස බැහැර කිරීම චර්ම හා ශ්වසන රෝග ඇති කරයි. තවද ඊයම් තුළින් අපවිත්‍ර වූ පානීය ජලය ස්නායු පද්ධතියට බලපාන අතර මොලේ වර්ධනය දුර්වල වීම, චර්ම රෝග, ශ්‍රවණාබාධිත භාවයට සහ රුධිර සෛලවල ක්‍රියාකාරිත්වය අඩපන වීමට හේතු වේ.

ශ්‍රී ලංකාවේ විද්‍යුත් අපද්‍රව්‍ය කළමනාකරණය පිළිබඳ ජාතික නීති, රෙගුලාසි සහ ප්‍රමිතීන්

ශ්‍රී ලංකාවේ ද ඉලෙක්ට්‍රොනික හා උපකරණ ආනයනය ක්‍රමයෙන් ඉහළ යන අතර එහි ප්‍රතිඵලයක් ලෙස අපද්‍රව්‍ය විදුලි හා ඉලෙක්ට්‍රොනික් උපකරණ (**WEEE - Waste Electrical and Electronic Equipment**) විශාල ප්‍රමාණයක් ජනනය වේ. කෙසේවෙතත් මෙම WEEE ප්‍රතිපත්තියක් වශයෙන් තවමත් හඳුනාගෙන නොමැත.

පරිසර හා පුනර්ජනනීය බලශක්ති අමාත්‍යාංශය
මෙය දිවයිනේ පරිසරය හා ස්වභාවික සම්පත් කළමනාකරණය පිළිබඳ ප්‍රතිපත්ති සම්පාදනය සඳහා නම් කරන ලද රේඛීය අමාත්‍යාංශයයි. මෙම අමාත්‍යාංශය යටතේ ප්‍රතිපත්ති ක්‍රියාත්මක කිරීම සඳහා මධ්‍යම පරිසර අධිකාරිය ඇතුළු ආයතන කිහිපයක් ගොඩනගා ඇත.

මධ්‍යම පරිසර අධිකාරිය
සංවර්ධන ක්‍රියාදාමයේ දී පාරිසරික සලකා බැලීම් ඒකාබද්ධ කිරීම මධ්‍යම පරිසර අධිකාරිය පිහිටුවීමේ මූලික පරමාර්ථය විය. 1980 අංක 47 දරණ ජාතික පාරිසරික පනතේ විධිවිධාන ප්‍රකාරව 1981 දී මධ්‍යම පරිසර අධිකාරිය පිහිටුවන ලදී. අන්තරායකර ස්වභාවය සැලකිල්ලට ගනිමින් 2008 පෙබරවාරි 1 වන දින සිට අංක 1534/18 දරණ ගැසට් නිවේදනය මගින් සමහර විද්‍යුත් අපද්‍රව්‍ය අන්තරායකර ගණයට ඇතුළත් කර ඇත.


මධ්‍යම පරිසර අධිකාරිය
மத்திய சுற்றாடல் அதிகாரசபை
Central Environmental Authority

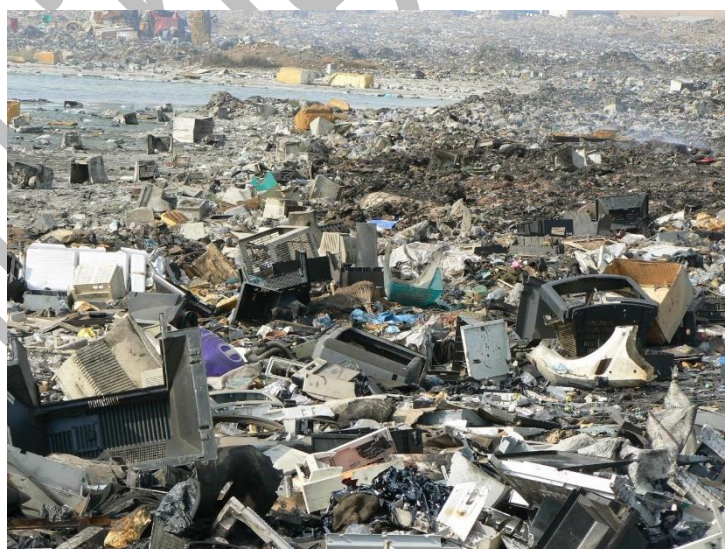
E-waste to be collected through Postal offices: CEA

Written by Pavani Hapuarachchi
09 Sep, 2020 | 10:52 AM

Share:

COLOMBO (News 1st): A decision has been reached to collect all Electronic waste (E-waste) in the country through postal offices, the Central Environmental Authority said.

"The collection of e-waste will be carried out by postmen," S. Samarasinghe, the Chairman at the Central Environmental Authority said on Wednesday (Sep 09).



පරිසරයට වන බලපෑම අවම කිරීම සඳහා හොඳම භාවිතයන් (Best Practices)

1. අවසාන පරිශීලකයා (End User)

බොහෝ පුද්ගලික ඩෙස්ක්ටොප් පරිගණක භාවිතා නොකරන විට පවා ධාවනය වන අතර අති විශාල විදුලියක් නාස්ති වේ. පරිශීලකයින් ඒවා අනවශ්‍ය ලෙස අත් නොහැරිය යුතු ය. මේ සඳහා පහත පියවර අනුගමනය කළ හැක.

- බල කළමණාකරන අංග සක්‍රීය කිරීම (Power Management)
- භාවිතා නොකරන අවස්ථාවලදී පරිගණක උදාසීන තත්ත්වයට පත් කිරීම (Hibernation / Sleep)
- ඩෙස්ක්ටොප් පරිගණක වලට වඩා අඩු බලශක්තියක් වැයවන පරිගණක භාවිතා කිරීම
- අනවශ්‍ය අවස්ථාවලදී පරිගණක තිර ක්‍රියාවිරහිත කිරීමයි
- අනවශ්‍ය ලෙස කඩදාසි මුද්‍රණය කිරීමෙන් වැළකී සිටීම
- මුද්‍රණ කටයුතු සඳහා භාවිතා කරන cardrige සහ laser toner නැවත පිරවීම. ඒ තුළින් ඒවා පරිසරයට එකතු වීම සිදු නොවේ

2. නැවත භාවිතය

මෙහිදී **3R** සංකල්පය භාවිතා කළ හැක

Reuse (නැවත භාවිතය)
පරිශීලක අවශ්‍යතා සපුරන්නේ නම් පැරණි පරිගණකයක් දිගටම භාවිතා කළ යුතුය. එසේ නැතහොත් ඉවතලන නිෂ්පාදනයකින් ක්‍රියාකාරී සංරචක භාවිතා කළ හැකිය.

Refurbish (අලුත්වැඩියා කිරීම)
ඇතැම් විට පවත්නා පරිගණක අලුත්වැඩියා කිරීමෙන්, ඒවා ඉවත් කිරීමකින් තොරව දිගු කලක් භාවිතා කළ හැක. නව පරිගණකයක් මිලට ගැනීම වෙනුවට නවීකරණය කරන ලද දෘඩාංග වෙළඳපොළෙන් මිලදී ගත හැක.

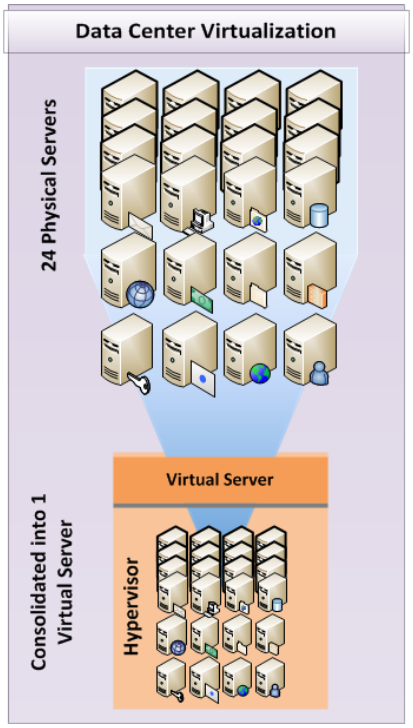
Recycle (ප්‍රතිචක්‍රීකරණය)
පරිගණක භාවිතා කළ නොහැකි තත්ත්වයට පත්වූ විට ඒවා පරිසර හිතකාමී ආකාරයෙන් නිසි ලෙස බැහැර කළ යුතුය.

3. දත්ත මධ්‍යස්ථාන **(Data Centers)**

අන්තර්ජාල හා වෙබ් යෙදුම්වල අඛණ්ඩ ජනප්‍රියතාවය දත්ත මධ්‍යස්ථාන වල වේගවත් වර්ධනයට හේතු වන අතර දිනෙන් දින ඉහළ යන ඉල්ලුමට සරිලන පරිදි ධාරිතාව පුළුල් කරන බව ඔබ මේ වන විට දනී. පසුගිය දශකය තුල විදුලි භාවිතය දෙගුණයක් වූ අතර ඉන් වැඩි ප්‍රමාණයක් පැමිණියේ නව සේවා සැපයුම් විශාල සංඛ්‍යාවක් ස්ථාපනය කරන ව්‍යාපාරවලිනි.

- නව බලශක්ති කාර්යක්ෂම උපකරණ භාවිතා කිරීම
- සිසිලන අවශ්‍යතා අවම කිරීම සඳහා වායු ගලන කළමණාකරනය වැඩි දියුණු කිරීම
- බලශක්ති කළමනාකරණ මෘදුකාංග සඳහා ආයෝජනය කිරීම
- දත්ත මධ්‍යස්ථාන සඳහා පරිසර හිතකාමී සැලසුම් අනුගමනය කිරීම
- දත්ත මධ්‍යස්ථානවල බලශක්ති පරිභෝජනය පාලනය කිරීම සඳහා නව පියවර ගැනීම
- තුලින් දත්ත මධ්‍යස්ථානවල කාර්යක්ෂමතාව වැඩි දියුණු කළ හැක.

අථත්‍යකරණය (Virtualization)
අථත්‍යකරණය යනු දත්ත මධ්‍යස්ථාන බලශක්ති පරිභෝජනය අඩු කිරීමේ ප්‍රධාන උපාය මාර්ගයකි. මෙහිදී එක් භෞතික සේවාසැපයුම් පරිගණකයක්, බහු අථත්‍ය සේවා සැපයුම් පරිගණක සඳහා සත්කාරක සේවාව සපයයි. මේ තුලින් දත්ත මධ්‍යස්ථානයකට අවශ්‍ය බිම් අවකාශය අඩු කරයි. පරිගණක බලය වඩා හොඳින් භාවිතා කරන අතර දත්ත මධ්‍යස්ථානයේ බලශක්ති ඉල්ලුම බෙහෙවින් අඩු කරයි.



තොරතුරු ආරක්ෂාව සහ පෞද්ගලිකත්වය (Information Security and Privacy)

තොරතුරු ආරක්ෂාව යනු දත්ත ආරක්ෂා කරනු ලබන යාන්ත්‍රණයන් ය. මේවා තොරතුරු තාක්ෂණ පද්ධති තුළ ක්‍රියාත්මක කරනු ලබන තාක්ෂණික පාලනයක් ලෙස සැලකුවත්, මෙමගින් තාක්ෂණික පාලනයකට එහා ගොස් සියලු ආකාර වලින් සිදුවන හානි වලින් ආරක්ෂා කිරීම අදහස් කෙරේ. තොරතුරු ආරක්ෂණයට අදාළ ප්‍රධාන සංකල්ප තුනක් හඳුනා ගත හැක.

1. රහස්‍යභාවය

එනම් අනවසර ප්‍රවේශයන් (Unauthorized Access) ඇතුළු සියලු ආකාර වලින් දත්ත ආරක්ෂා කිරීමයි. අනවසර ප්‍රවේශය යනු පද්ධතියට අනුබද්ධ නොවන පාර්ශව විසින් පද්ධතිය වෙත ප්‍රවේශ වීමයි. මෙය කිසියම් අපරාධමය ක්‍රියාවක් සිදු කිරීම හෝ දත්ත සොරකම් කිරීම හෝ පිටපත් කිරීම යනාදී සඳහා සිදුවිය හැක.

2. අඛණ්ඩතාව

එනම් තොරතුරු තාක්ෂණ පද්ධති තුළ නිවැරදි බව සහතික කිරීමයි. එනම් පද්ධති නිර්මාපකයන් සහ කළමනාකරුවන් විසින් පද්ධතිය තුළ පාලනයන් ක්‍රියාවට නංවන අතර, පරිශීලකයන් දත්ත නිවැරදිව ඇතුලත් කර සැකසීම සහ ගැටුම්කාරී දත්ත කොටස් හඳුනාගෙන විසඳා ඇති බවයි. අවසර ලත් පරිශීලකයන්ට පමණක් දත්ත ගොනු වෙනස් කිරීමට ගෙන යාමට හෝ මකා දැමීමට අවසර දීමෙන් අඛණ්ඩතාව ආරක්ෂා කර ගත හැක. එමෙන්ම අඛණ්ඩත්වයෙන් යුතු දත්ත මත විශ්වාසය තබා තීරණ ගැනීම සිදු කළ හැක.

3. උපයෝජ්‍යතාව

එනම් අවශ්‍ය විටෙක දත්ත ලබා ගත හැකි බවත් තොරතුරු තාක්ෂණ පද්ධති විශ්වසනීයව ක්‍රියාත්මක වන බවත් සහතික කිරීමයි. මේ සඳහා පරීක්ෂණ ගෙන් විසින් නිතිපතා දත්ත උපස්ථ කිරීම (Backup) සිදුකළ යුතු අතර එය සහතික කිරීම ද සිදුවිය යුතුය.

තොරතුරු තාක්ෂණ පද්ධති වලට එල්ල විය හැකි තර්ජන

- අනිෂ්ට මෘදුකාංග (Malware)
- ඔත්තු මෘදුකාංග (Spyware)
- යතුරු ලොගර්ස් (Key Loggers)
- පරිශීලක දත්ත සොරකම් කිරීම සඳහන් නිර්මාණය කර ඇති තතුබෑම් (Phishing) සහ ඉලක්ක ගත වංචා (Targeted Scams)
- නීත්‍යානුකූල ප්‍රවේශයක් ඇති අයෙකු හිතාමතාම අනිසි ලෙස භාවිතා කිරීම

තවද මීට අමතරව ස්වභාවික විපත්, විදුලිය බිඳවැටීම හෝ අස්ථානගත වූ තොරතුරු තාක්ෂණික සම්පත් වැනි අනපේක්ෂිත හෝ අහඹු සිදුවීම් වලින් තොරතුරු පද්ධති ආරක්ෂා කළ යුතුය.

පුද්ගලිකත්වය (Privacy)

පුද්ගලිකත්වය යනු පුද්ගලයෙකුට ඔහුගේ හෝ ඇයගේ දත්ත පාලනය කිරීමට ඇති අයිතිය සහ එම දත්ත එක්රැස් කරන, භාවිතා කරන හා බෙදා ගන්නා ආකාරයෙන් නියම කිරීමට ඇති අයිතියයි.

තොරතුරු තාක්ෂණ හා තොරතුරු පද්ධති සම්බන්ධ ශ්‍රී ලංකාවේ නීති හා රෙගුලාසි

2003 අංක 36 දරණ බුද්ධිමය දේපල පනත

ප්‍රධාන පරමාර්ථය වන්නේ පේටන් බලපත්‍ර, වෙළඳ ලකුණු, වෙළඳනාම වැනි බුද්ධිමය දේපළ ආරක්ෂා කිරීමයි. මෙම නීතිය යටතේ ජාතික බුද්ධිමය දේපල කාර්යාංශය (NIPO - National Intellectual Property Office) පිහිටුවන ලදී.

2003 අංක 27 දරන තොරතුරු හා සන්නිවේදන තාක්ෂණ පනත

මෙම පනත යටතේ ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ ඒජන්සිය (ICTA - Information and Communication Technology Agency) පිහිටුවනු ලැබීය. මෙම පනත යටතේ රජයේ සහ පෞද්ගලික අංශයේ උපායමාර්ග හා වැඩසටහන් සම්පාදනය කිරීමට හා ක්‍රියාත්මක කිරීමට තොරතුරු හා සන්නිවේදන තාක්ෂණ අධිකාරියට බලය ලබාදී ඇත. තවද මේ යටතේ යටිතල පහසුකම් නිර්මාණය කිරීමට සහ විද්‍යුත් රාජ්‍ය සේවා ස්ථාපිත කිරීමට කටයුතු සම්පාදනය කරමින් පවතී.

2005 අංක 28 දරණ ගෙවීම් නිෂ්කාශන හා නිරවුල්කරණ පද්ධති පනත

- ගෙවීම් නිෂ්කාශන සහ නිරවුල්කරණ පද්ධති නියාමනය හා අධීක්ෂණය
- මහ බැංකුවේ පවත්වාගෙන යනු ලබන සුරකුම්පත් ගිණුම් වල සුරකුම්පත් තැන්පත් කිරීම සඳහා ආරක්ෂාව සැපයීම
- මුදල් සේවා සපයන්නන් නියාමනය සහ අධීක්ෂණය
- විද්‍යුත් චෙක් පත් ඉදිරිපත් කිරීම සඳහා පහසුකම් සැපයීම

2006 අංක 19 දරන විද්‍යුත් ගනුදෙනු පනත

මෙම පනත පදනම් වී ඇත්තේ එක්සත් ජාතීන්ගේ ජාත්‍යන්තර වෙළඳ නීතිය පිළිබඳ කොමිසම (UNCITRAL) මගින් ඉලෙක්ට්‍රොනික වාණිජ පිළිබඳ ආදර්ශ නීතිය සහ ඉලෙක්ට්‍රොනික අත්සන් පිළිබඳ ආදර්ශ නීතිය විසින් පිහිටුවන ලද ප්‍රමිතීන් මතය. මෙහි අරමුණු පහත පරිදි වේ.

- දෛනික බාධක ඉවත්කර නයි ටික නිශ්චිත භාවයක් ඇති කර ගනිමින් දේශීය හා ජාත්‍යන්තර විද්‍යුත් වාණිජය පහසුකම් සැලසීම
- විශ්වසනීය ඉලෙක්ට්‍රොනික වාණිජ්‍ය භාවිතා කිරීම දිරිමත් කිරීම
- ලිපි ලේඛන හා ගිවිසුම්, විද්‍යුත් ක්‍රමයට පවත්වාගෙන යාම සඳහා පහසුකම් සැලසීම

2006 අංක 30 දරණ ගෙවීම් උපකරණ වංචා පනත

මෙමගින් අනවසර හෝ ව්‍යාජ ගෙවීම් උපකරණ සන්තකයේ තබා ගැනීම සහ භාවිතා කිරීම වැලැක්වීමට, ඒ හා සම්බන්ධව වැරදි වැලැක්වීමටත්, නීත්‍යානුකූලව නිකුත් කරන එවැනි ගෙවීම් උපකරණ භාවිතා කරන පුද්ගලයින් ආරක්ෂා කිරීමටත් උපකාරී වේ.

2007 අංක 24 දරන පරිගණක අපරාධ පනත

මෙම පනතේ පදනම වනුයේ පරිගණකයක්, පරිගණක වැඩසටහනක්, දත්ත හෝ තොරතුරු වෙත නීත්‍යානුකූල නීත්‍යානුකූල නොවන අන්දමින් ප්‍රවේශවීම අපරාධයක් ලෙස හඳුනා ගැනීමයි. අධිකාරී බලයක් නොමැතිව අනවසරයෙන් දත්ත වෙනස් කිරීම හෝ මකා දැමීම මෙම පනත අනුව වරදක් වන අතර අධිකාරී බලය සහිත පුද්ගලයකුට ප්‍රවේශය අත්කර ගැනීම වැළැක්වීම පිණිස පරිගණකය වැඩසටහන් සකස් කිරීමද වරදකි.

2016 අංක 12 දරණ තොරතුරු දැනගැනීමේ අයිතිය පිළිබඳ පනත
මෙමගින් තොරතුරු ලබා ලබාගැනීමේ අයිතිය සහතික කරන අතර තොරතුරු ලබා ලබා ගැනීමේ අයිතියට බලපෑමක් ඇති කරමින් රාජ්‍ය බලධාරීන් තුල විනිවිදභාවය සහ වගවීම පිළිබඳ සංස්කෘතියක් පෝෂණය කිරීමේ අවශ්‍යතාවයක් පවතින අතර එමගින් සමාජය ප්‍රවර්ධනය කරනු ලැබේ.

2017 අංක 25 දරණ විද්‍යුත් ගනුදෙනු (සංශෝධන) පනත
මෙමඟින් ශ්‍රී ලංකාවේ දත්ත පණිවිඩ, විද්‍යුත් ලේඛන, විද්‍යුත් වාර්තා සහ වෙනත් සන්නිවේදනයන් විවිධ ස්වරූපයෙන් හඳුනාගැනීම, සහතික කිරීමේ අධිකාරයක් පත් කිරීම සහ සහතික කිරීමේ සේවා සපයන්නන් සඳහා බලපත්‍ර ලබා දීම සහ බලය පැවරීම සඳහා පහසුකම් සහ විධිවිධාන සලසයි. එනම් මෙම පනත මඟින් අපරාධ වල දී සාක්ෂි ලෙස විද්‍යුත් ක්‍රමයට පවතින ඕනෑම දෙයක් හඳුනාගැනීම ආරම්භ විය.

සයිබර් ආරක්ෂාව (Cyber Security)

සයිබර් ආරක්ෂාව යනුවෙන් හඳුන්වන්නේ දත්ත, පරිගණක හෝ ජංගම උපාංග වලට එල්ල වන ප්‍රහාරයකින් ඇතිවන බාධාවන් වළක්වා ගැනීමට හෝ අවම කිරීමට ගන්නා ආරක්ෂාවන් සඳහා වන නාමයයි. එබැවින් මෙවැනි ආරක්ෂණ ක්‍රමවේද හරහා රහස්‍යභාවය හා පෞද්ගලිකත්වය ආරක්ෂා කිරීම පමණක් නොව දත්ත ලබාගැනීමේ හැකියාව සහ අඛණ්ඩතාව ද ආවරණය කරයි. විශේෂයෙන් ආයතන වල ආරක්ෂක පියවර ක්‍රියාත්මක කරන්නේ කෙසේද යන්න පිළිබඳව එහි සියලු කාර්ය මණ්ඩලය දැනුවත් කළ යුතුය.

මාර්ගගත ආරක්ෂාව වැඩි දියුණු කිරීම සඳහා ගතහැකි පියවර කීපයකි.

1. සහාය නොදක්වන මෘදුකාංග භාවිතා කිරීමෙන් ඉවත් වීම.
මෙහෙයුම් පද්ධති ඇතුළු බොහොමයක් මෘදුකාංග සඳහා කිසියම් කාලයකට පසුව මෘදුකාංග නිර්මාණකරුවන් විසින් සහය දැක්වීම නවතා දමනු ලබයි. (උදාහරණ වශයෙන් මේ වන විට Microsoft ආයතනය Windows 7 හා ඊට පෙර පැමිණි මෙහෙයුම් පද්ධති සඳහා සහාය දැක්වීම නවතා ඇත) මෙලෙස සහාය දැක්වීම අවසන් වූවත් එකී මෘදුකාංග දිගටම භාවිතා කළ හැකි නමුත් යාවත්කාලීන වීමක් සිදු නොවන නිසා ආරක්ෂාව සම්බන්ධයෙන් ගැටලු පවතී. එවැනි මෘදුකාංග ඔස්සේ සයිබර් ප්‍රහාර වලට ගොදුරු වීමේ වැඩි හැකියාවක් පවතී.

2. සෑමවිටම මෘදුකාංග සහ යෙදුම් යාවත්කාලීන කිරීම

3. ප්‍රති-වයිරස මෘදුකාංග (Antivirus Software) ස්ථාපනය කිරීම සහ යාවත්කාලීන කිරීම.
පරිගණක, ටැබ්ලට් සහ ජංගම දුරකථන වල ප්‍රති වයිරස මෘදුකාංග ස්ථාපනය කිරීමෙන් ඉහත සඳහන් කරලා ද අනිෂ්ට මෘදුකාංග වලින් ආරක්ෂාව ලබා ගත හැක. මේවා නිරන්තරයෙන් යාවත්කාලීන කිරීම ඉතා වැදගත් වේ.

4. ශක්තිමත් මුරපද භාවිතා කිරීම
එනම් මුරපද මතක තබා ගැනීම පහසු විය යුතු අතර අනුමාන කිරීමට අපහසු විය යුතුය. එමෙන්ම බැංකු ගිණුම් යනාදිය සඳහා ද්වී සාධක සත්‍යාපනය (Two-Factor Authentication) භාවිතා කළ හැක. ඉන් අදහස් කරනු ලබන්නේ මුරපදය පමණක් ඇතුළත් කිරීමෙන් ගිණුමට ප්‍රවේශ විය නොහැකි අතර, ඇඟිලි සලකුණක්, ප්‍රශ්නයකට පිළිතුරු සැපයීමක් හෝ පරිශීලකයාගේ ජංගම උපාංගය ට යවන ලද කේතයක් ඇතුලත් කිරීම හරහා ප්‍රවේශය සකසා දීමයි.

5. සැක සහිත ඊමේල් මැකීම සහ නොදන්නා ඇමුණුම් (Attachments) හෝ සබැඳි (Links) වලට ප්‍රවේශ වීමෙන් වැළකීම.

6. දත්ත නිරන්තරයෙන් උපස්ථ කිරීම
එවිට පරිගණකයට හෝ පරිගණක පද්ධතියට කිසියම් හානියක් සිදු වුවහොත් දත්ත වෙනත් ස්ථානයක පවතින බැවින් ආරක්ෂාව සැපයේ.

7. සයිබර් දැනුවත් වීමට කාර්ය මණ්ඩලය පුහුණු කිරීම
එනම් ඉහත ක්‍රියාමාර්ග පිළිබඳව ආයතනයක සේවකයන් දැනුවත් කිරීම හා පුහුණු කිරීම සිදු කළ යුතුය.

---------- END ----------