

15 -ാം കേരള നിയമസഭ

9 -ാം സമ്മേളനം

നക്ഷത്ര ചിഹ്നം ഇല്ലാത്ത ചോദ്യം നം. 679

09-08-2023 - ൽ മറുപടിയ്ക്ക്

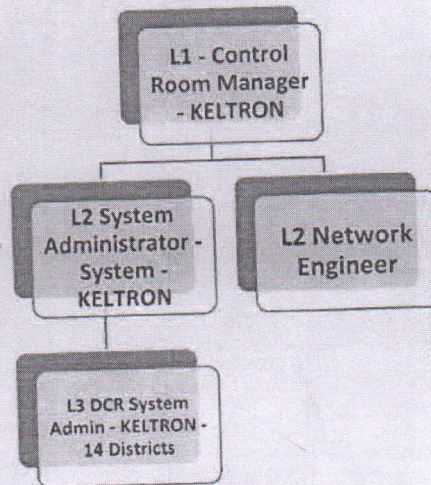
എ.ഐ. ക്യാമറകളുടെ ഡാറ്റ സുരക്ഷ

ചോദ്യം		ഉത്തരം	
ശ്രീ. ടി. സിദ്ദിഖ്		ശ്രീ. പി. രാജീവ് (നിയമം, വ്യവസായം, കയർ വകുപ്പ് മന്ത്രി)	
(എ)	സേഫ് കേരള പദ്ധതിയുടെ ഭാഗമായി എ.ഐ. ക്യാമറകൾ കണ്ടെത്തുന്ന നിയമലംഘനങ്ങളുമായി ബന്ധപ്പെട്ട രേഖകൾ, ചിത്രങ്ങൾ, വിഡിയോകൾ എന്നിവ സൂക്ഷിക്കുന്ന സെർവറുകൾ ഏതാണ് എന്ന് വ്യക്തമാക്കാമോ;	(എ)	മോട്ടോർ വെഹിക്കിൾ ഡിപ്പാർട്ട്മെന്റിന്റെ അധീനതയിൽ ഉള്ള തിരുവനന്തപുരത്തെ സെൻട്രൽ കൺട്രോൾ റൂമിലെ സെർവറുകളിലും ഇതു കൂടാതെ കേന്ദ്ര സർക്കാരിന്റെ MORTH-ന്റെ അധീനതയിലുള്ള വാഹന്റെ ഡൽഹിയിലുള്ള സെർവറുകളിലും ആണ് സൂക്ഷിക്കുന്നത്.
(ബി)	പ്രസ്തുത പദ്ധതിയുടെ ഭാഗമായുള്ള സെർവറുകൾ കൈകാര്യം ചെയ്യുന്നത് ഏതു സ്ഥാപനമാണ് എന്ന് വിശദമാക്കാമോ;	(ബി)	സേഫ് കേരളയുമായി ബന്ധപ്പെട്ട സെൻട്രൽ കൺട്രോൾ റൂമിലെ സെർവറുകൾ കൈകാര്യം ചെയ്യുന്നത് എം. വി. ഡി. യും കെൽടോൺ ആണ്
(സി)	പ്രസ്തുത വിവരങ്ങളുടെ സുരക്ഷ ഉറപ്പാക്കുന്നതിന് എന്തൊക്കെ സംവിധാനങ്ങളാണ് ഉറപ്പു വരുത്തിയിരുന്നത്; ഡാറ്റ സുരക്ഷ ഉറപ്പാക്കുന്നതുമായി ബന്ധപ്പെട്ട രേഖകളുടെയും ഉടമ്പടികളുടെയും പകർപ്പ് ലഭ്യമാക്കാമോ?	(സി)	വിവരങ്ങളുടെ സുരക്ഷ ഉറപ്പാക്കുന്നതിന് കെൽടോൺ സ്വീകരിച്ചിരിക്കുന്ന സംവിധാനങ്ങളുടെ വിശദവിവരം അനുബന്ധം 1 ആയി ചേർത്തിരിക്കുന്നു. സേഫ് കേരള പദ്ധതിയുടെ ഭാഗമായി എ.ഐ. ക്യാമറകൾ കണ്ടെത്തുന്ന നിയമലംഘന-ങ്ങളുമായി ബന്ധപ്പെട്ട വിവരങ്ങൾ മോട്ടോർ വെഹിക്കിൾ ഡിപ്പാർട്ട്മെന്റിന്റെ അധീന-തയിൽ ഉള്ള സെൻട്രൽ കൺട്രോൾ റൂമിലെ സെർവറുകളിലും ഇതു കൂടാതെ കേന്ദ്ര സർക്കാരിന്റെ MORTH-ന്റെ അധീനതയിലുള്ള വാഹന്റെ ഡൽഹിയിലുള്ള സെർവറുകളിലും ആണ് സൂക്ഷിക്കുന്നത്.

സെക്ഷൻ ഓഫീസർ

CRITICAL DATA SECURITY MEASURES ADOPTED IN SAFE KERALA PROJECT

- All the enforcement systems are securely connected using 128 bit encryption, to a State Central Control Room with a Datacenter installed at the Office of the RTO(Enforcement) Trivandrum.
- The connectivity between Enforcement systems and Control room is done using IOT sim cards which are programmed to communicate only with the Static IPs of the Datacenter.
- Access to devices at sites can only be done by personnel having valid software certificate authorized by keltron. Only pre-authorized Laptop with known credentials can log into the system for maintenance purposes. This software certificate will not work in another laptop.
- Access to the Field device is limited to maintenance purpose only. Access to data is not possible for the field maintenance staff.
- Physical entry to the data centre is restricted using a secure access control device with only fingerprint or facial recognition authorization.
- The security of the Datacenter is managed using high-end Firewall devices from Checkpoint by a team of System Administrators and Managers from Keltron.
- The connectivity to the Central Control Room is restricted to 14 district control rooms using secure VPNs created using firewall devices and Static IP's.
- The applications used for verification of violations can be accessed only through a specific set of IPs provided in the VPN. Internet will not be accessible on these IPs.
- All data download, server management, Data backup is done by the Keltron System Administrator. This data is managed by a 3-level team employed by Keltron as follows



- Data collection is required for improving AI models and debugging processes due to ever-evolving technology. For the project to run successfully, this procedure cannot be avoided. Policies for data collection should have prior intimation and approval from KELTRON. Data will be provided by keltron only with prior permission from MVD. Such data collected should be used for training and debugging purposes only. Data should not be sent to any other 3rd party.

Duyal
ഒമ്പലം അറിവ്