sflc.in

മാർഗ്ഗനിർദ്ദേശം

ഇലക്ട്രോണിക് ഉപകരണങ്ങളുടെ പരിശോധനയും കണ്ടുകെട്ടലും സംബന്ധിച്ച

Guide on Search and Seizure of Electronic Devices, 2025
By SFLC.in in partnership with UNESCO

© Copyright 2024 SFLC.in Licensed under Creative Commons BY SA NC 4.0

Published by: SFLC.in
K9, 2nd Floor, Birbal Road, Jangpura Extension, New Delhi – 14, India.

Email: mail@sflc.in

Website: https://www.sflc.in

ഉള്ളടക്ക പട്ടി

01\. വിഭാഗം 1
അടിസ്ഥാന കാര്യങ്ങൾ 4

02\. വിഭാഗം 2
പരിശോധനാ സമയത്ത് എന്ത് ചെയ്യണം? 10

03\. വിഭാഗം 3
ഇലക്ട്രോണിക് ഉപകരണങ്ങളും നിയമവും 14

04\. വിഭാഗം 4
കണ്ടുകെട്ടിയതിന് ശേഷമുള്ള നടപടിക്രമം 16

05\. വിഭാഗം 5
തയ്യാറെടുപ്പ് 25

- ഗ്ലോസറി 33
- അനുബന്ധം 36
- റഫറൻസുകൾ 45

വിഭാഗം 1

അടിസ്ഥാന കാര്യങ്ങൾ

നിങ്ങളെ ആരെങ്കിലും പരിശോധിച്ചിട്ടുണ്ടോ?
അവർ നിങ്ങളുടെ ശരീരമോ, വാഹനമോ, വീടോ എന്നിവ പരിശോധിച്ചിട്ടുണ്ടോ?
അവർ നിങ്ങളുടെ ഉപകരണങ്ങൾ കണ്ടുകെട്ടിയിട്ടുണ്ടോ?
ഇവയിൽ ഏതെങ്കിലും ഒന്നിന് ഉത്തരം 'ഉണ്ട്' എന്നാണെങ്കിൽ...

തിരച്ചിലും പിടിച്ചെടുക്കലും: ഒരു വിശകലനം

പരിശോധനയും കണ്ടുകെട്ടലും: എന്തുകൊണ്ട്, എന്തിന്, എവിടെ

'പരിശോധന' എന്നാൽ നടന്നുകൊണ്ടിരിക്കുന്ന അന്വേഷണത്തിനോ നീതിന്യായ നടപടിക്രമത്തിനോ വേണ്ടി തെളിവുകൾ കണ്ടെത്തുന്നതിനായി ഒരു വ്യക്തിയെയോ അവരുടെ സ്വത്തിനെയോ പരിശോധിക്കുക എന്നാണ്. [1][2]ഇതു വാറന്റിനോടുകൂടിയോ അല്ലാതെയോ ചെയ്യാം.[3][4]

കണ്ടുകെട്ടൽ' എന്നാൽ പരിശോധന പൂർത്തിയായ ശേഷം ആ സ്വത്ത് തെളിവായി അല്ലെങ്കിൽ അന്വേഷണവുമായി ബന്ധപ്പെട്ട സ്വത്തായി കൈവശപ്പെടുത്തുക എന്നാണ്.[5]

എന്തുകൊണ്ട്: ഇത് നിയമ നിർവഹണ ഏജൻസികൾ ഒരു കേസ് അന്വേഷിക്കുന്നതിനുള്ള പ്രക്രിയയാണ്.

കാരണം: തെളിവുകൾശേഖരിക്കുന്നതിനും, കുറ്റം തടയുന്നതിനും, നീതിന്യായത്തിലെ അന്യായം തടയുന്നതിനുമാണ് ഇത് ചെയ്യുന്നത്.

സ്ഥലം: കുറ്റം നടന്ന സ്ഥലങ്ങൾ, കുറ്റവുമായി ബന്ധപ്പെട്ട വ്യക്തികൾ ഒളിവിൽ കഴിയുന്ന സ്ഥലങ്ങൾ, കുറ്റവുമായി ബന്ധപ്പെട്ട വസ്തുക്കൾ സൂക്ഷിക്കുന്ന സ്ഥലങ്ങൾ.

പരിശോധനയ്ക്കും കണ്ടുകെട്ടലിനുമുള്ള കാരണങ്ങൾ

- നിർണായകമായ വസ്തുക്കളും രേഖകളും, ഇലക്ട്രോണിക്, ഡിജിറ്റൽ റെക്കോർഡുകൾ ഉൾപ്പെടെ ഒരു വ്യക്തിക്കെതിരായ അന്വേഷണം, പരിശോധന അല്ലെങ്കിൽ വിചാരണയ്ക്കായി ഏതെങ്കിലും ഏജൻസിക്ക് ലഭ്യമാക്കുന്നതിനാണ് ഇത് ചെയ്യുന്നത്.
- അന്വേഷണ ഏജൻസികൾ/പോലീസ് പരിശോധനയിലും കണ്ടുകെട്ടലിലും ലഭിച്ച രേഖകളുടെ ഉള്ളടക്കം കോടതിയിൽ ഒന്നാം അല്ലെങ്കിൽ രണ്ടാം തരം തെളിവുകളിലൂടെ സ്ഥിരീകരിക്കാൻ കഴിയും.

ഈ പ്രവൃത്തികൾക്ക് നിയമപരമായ അടിസ്ഥാനം

പരിശോധനയിലും കണ്ടുകെട്ടലിനുള്ള അധികാരം വിവിധ നിയമങ്ങളിൽ നിന്ന് ലഭിക്കുന്നു:[6]:

+ ഭാരതീയ നാഗരിക് സുരക്ഷാ സംഹിത, 2023 (BNSS) [7]
+ ഭാരതീയ സാക്ഷ്യ അധിനിയം, 2023 (BSA) [8]
+ ഭാരതീയ ന്യായ സംഹിത, 2023 (BNS) [9]
+ 1961 വരുമാന നികുതി നിയമം (ITA)
+ 1967 ലെ അനധികൃത പ്രവർത്തനങ്ങൾ (തടയൽ) നിയമം, (UAPA)
+ 2002 ലെ മണി ലോണ്ടറിംഗ് തടയൽ നിയമം (PMLA)
+ 2020 ലെ CBI മാനുവൽ
+ 2000 ലെ വിവരസാങ്കേതികവിദ്യാ നിയമം (IT Act)
+ 2023 ലെ ടെലികമ്മ്യൂണിക്കേഷൻസ് നിയമം
+ 1985 ലെ മയക്കുമരുന്ന് സൈക്കോട്രോപിക് പദാർത്ഥങ്ങളും നിയമം

പിന്നണിയിൽ (BTS): പരിശോധനയ്ക്കും കണ്ടുകെട്ടലിനും അധികാരപ്പെട്ടവർ.

പരിശോധനയും കണ്ടുകെട്ടലും നടത്താൻ അധികാരമുള്ളവർ നിയമങ്ങളനുസരിച്ച് വ്യത്യാസപ്പെടുന്നു. പരിശോധനയ്ക്കുള്ള ഉത്തരവിടാനുള്ള അധികാരം ആർക്കാണ് എന്നതിനെക്കുറിച്ച് പൊതു വിവരം നൽകുക എന്നതാണ് ഈ വിഭാഗത്തിന്റെ ഉദ്ദേശ്യം. ഇത് പരിശോധിക്കുന്നതിലൂടെ, അന്വേഷണ അധികൃതരോട് ഉചിതമായ ചോദ്യങ്ങൾ ചോദിക്കാൻ നിങ്ങളെ സഹായിക്കും.

നിയമങ്ങളും സാഹചര്യങ്ങളും അനുസരിച്ച് പരിശോധനയും കണ്ടുകെട്ടലും നടത്തുന്ന രീതി മാറാം.

I. WHO HAS THE AUTHORITY TO ISSUE THE ORDER FOR THE SEARCH?

BNSS	ഒരു ജഡ്ജി (ജില്ലാ മജിസ്ട്രേറ്റ്, സബ്-ഡിവിഷണൽ മജിസ്ട്രേറ്റ് അല്ലെങ്കിൽ ഫസ്റ്റ് ക്ലാസ് മജിസ്ട്രേറ്റ്) കോൺസ്റ്റബിൾ റാങ്കിന് മുകളിലുള്ള ഒരു പോലീസ് ഉദ്യോഗസ്ഥന് മോഷണവസ്തുക്കളോ അപകടസാധ്യതയുള്ള വസ്തുക്കളോ ഒളിച്ചിരിക്കുന്ന സ്ഥലം പരിശോധിക്കാനുള്ള പ്രത്യേക അനുമതി നൽകാൻ കഴിയും. ആവശ്യമെങ്കിൽ ഈ ഉദ്യോഗസ്ഥന് മറ്റുള്ളവരിൽ നിന്ന് സഹായം തേടാനും കഴിയും.
Income Tax Act	ഡയറക്ടർ/ജനറൽ/ചീഫ് കമ്മീഷണർ അല്ലെങ്കിൽ കമ്മീഷണർ എന്നിവർക്ക് പരിശോധനയ്ക്ക് ഉത്തരവിടാൻ അധികാരമുണ്ട്.
UAPA	കേന്ദ്ര/സംസ്ഥാന സർക്കാരിന് പരിശോധനയ്ക്ക് ഉത്തരവിടാൻ അധികാരമുണ്ട്. എന്നിരുന്നാലും ഏത് മന്ത്രാലയം/വിഭാഗത്തിനാണ് ഈ ഉത്തരവിടാനുള്ള അധികാരമെന്ന് നിയമത്തിൽ പറയുന്നില്ല.
PMLA	**സർവ്വേയ്ക്ക് ഉത്തരവിടാൻ:** അഡ്ജഡിക്കേറ്റിങ് അതോറിറ്റിക്കാണ് അധികാരമുള്ളത്. **കണ്ടുകെട്ടലുകൾക്ക്:** ഡയറക്ടർ അല്ലെങ്കിൽ ഡെപ്യൂട്ടി ഡയറക്ടർ റാങ്കിന് താഴെയല്ലാത്ത ഏതെങ്കിലും ഉദ്യോഗസ്ഥന് ഉത്തരവിടാനാകും.
IT Act	കേന്ദ്ര സർക്കാരിന് പരിശോധന നടത്താൻ കേന്ദ്ര/സംസ്ഥാന സർക്കാർ ഉദ്യോഗസ്ഥനോട് ഉത്തരവിടാനുള്ള അധികാരമുണ്ട്. കമ്പ്യൂട്ടറുകളിലെ ഡേറ്റ ആക്സസ് ചെയ്യാൻ കൺട്രോളർക്കും പരിശോധനയ്ക്ക് ഉത്തരവിടാനാകും.

പിന്നണിയിൽ (BTS): പരിശോധനയ്ക്കും കണ്ടുകെട്ടലിനും അധികാരപ്പെട്ടവർ.

പരിശോധനയും കണ്ടുകെട്ടലും നടത്താൻ അധികാരമുള്ളവർ നിയമങ്ങളനുസരിച്ച് വ്യത്യാസപ്പെടുന്നു. പരിശോധനയ്ക്കുള്ള ഉത്തരവിടാനുള്ള അധികാരം ആർക്കാണ് എന്നതിനെക്കുറിച്ച് പൊതു വിവരം നൽകുക എന്നതാണ് ഈ വിഭാഗത്തിന്റെ ഉദ്ദേശ്യം. ഇത് പരിശോധിക്കുന്നതിലൂടെ, അന്വേഷണ അധികൃതരോട് ഉചിതമായ ചോദ്യങ്ങൾ ചോദിക്കാൻ നിങ്ങളെ സഹായിക്കും.

നിയമങ്ങളും സാഹചര്യങ്ങളും അനുസരിച്ച് പരിശോധനയും കണ്ടുകെട്ടലും നടത്തുന്ന രീതി മാറാം.

II. പരിശോധന നടത്താനുള്ള അധികാരം ആർക്കാണ്?

BNSS	പരിശോധനയുടെയും കണ്ടുകെട്ടലിന്റെയും നിയമം എങ്ങനെ പ്രവർത്തിക്കുന്നു എന്നതിന്റെ അടിസ്ഥാന ധാരണ ഇതാണ്: സ്റ്റേഷൻ ഹൗസ് ഓഫീസർക്കോ (SHO) അല്ലെങ്കിൽ അന്വേഷണ ഉദ്യോഗസ്ഥനോ (IO) പരിശോധനയോ കണ്ടുകെട്ടലോ നടത്തിയേക്കും, ഇവരുടെ അഭാവത്തിൽ, രേഖാമൂലം അധികാരം നൽകിയിട്ടുള്ള ഏതൊരു ഉദ്യോഗസ്ഥനും ഇത് ചെയ്യാവുന്നതാണ്. **ഒരാളെ അറസ്റ്റ് ചെയ്താൽ:** പോലീസ് അവരെ പിടികൂടിയ സ്ഥലം പരിശോധിക്കാം കൂടാതെ കുറ്റകൃത്യവുമായി ബന്ധപ്പെട്ട എന്തും എടുക്കാം. ഇത് പോലീസിന് മാത്രമേ ചെയ്യാൻ കഴിയൂ, ആവശ്യമെങ്കിൽ വാതിലുകളോ ജനലുകളോ തകർക്കാനും കഴിയും. **എന്തെങ്കിലും സംശയാസ്പദമായ വസ്തുക്കൾ ഒളിപ്പിച്ചിട്ടുണ്ടെങ്കിൽ:** ഒരു ജഡ്ജിക്ക് (ജില്ലാ മജിസ്ട്രേറ്റ്, സബ്-ഡിവിഷണൽ മജിസ്ട്രേറ്റ് അല്ലെങ്കിൽ ഫസ്റ്റ് ക്ലാസ് മജിസ്ട്രേറ്റ്) ഒകോൺസ്റ്റബിൾ റാങ്കിന് മുകളിലുള്ള ഒരു പോലീസ് ഉദ്യോഗസ്ഥന് (ഏത് ഉദ്യോഗസ്ഥനും അല്ല!) മോഷണവസ്തുക്കളോ അപകടസാധ്യതയുള്ള വസ്തുക്കളോ ഒളിച്ചിരിക്കുന്ന സ്ഥലം പരിശോധിക്കാനുള്ള പ്രത്യേക അനുമതി നൽകാൻ കഴിയും, ആവശ്യമെങ്കിൽ ഈ ഉദ്യോഗസ്ഥന് മറ്റുള്ളവരിൽ നിന്ന് സഹായം തേടാനും കഴിയും. **വകുപ്പുകൾ: 44 & 97**
UAPA	UAPA അന്വേഷിക്കാനുള്ള അധികാരം വിവിധ നഗരങ്ങളിൽ വ്യത്യസ്തമാണ്: **ഡൽഹി സ്പെഷ്യൽ പോലീസ് എസ്റ്റാബ്ലിഷ്മെന്റ്:** ഡെപ്യൂട്ടി സൂപ്രണ്ട് ഓഫ് പോലീസ് അല്ലെങ്കിൽ തത്തുല്യമായ റാങ്കിലുള്ള ഉദ്യോഗസ്ഥൻ. **മുംബൈ, കൊൽക്കത്ത, ചെന്നൈ, അഹമ്മദാബാദ് തുടങ്ങിയ മെട്രോപൊളിറ്റൻ പ്രദേശങ്ങളിലും അറിയിപ്പ് നൽകിയിട്ടുള്ള പ്രദേശങ്ങളിലും:** അസിസ്റ്റന്റ് കമ്മീഷണർ ഓഫ് പോലീസ് അല്ലെങ്കിൽ ഉയർന്ന റാങ്കിലുള്ള ഉദ്യോഗസ്ഥർ. **മറ്റ് കേസുകളിൽ:** ഡെപ്യൂട്ടി സൂപ്രണ്ട് ഓഫ് പോലീസ് അല്ലെങ്കിൽ തത്തുല്യമായ റാങ്കിൽ കുറയാത്ത ഉദ്യോഗസ്ഥർ.

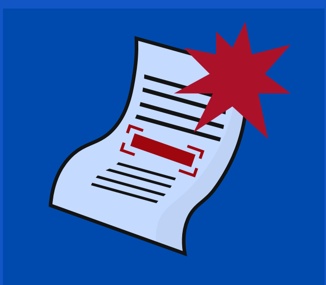
പിന്നണിയിൽ (BTS): പരിശോധനയ്ക്കും കണ്ടുകെട്ടലിനും അധികാരപ്പെട്ടവർ.

പരിശോധനയും കണ്ടുകെട്ടലും നടത്താൻ അധികാരമുള്ളവർ നിയമങ്ങളനുസരിച്ച് വ്യത്യാസപ്പെടുന്നു. പരിശോധനയ്ക്കുള്ള ഉത്തരവിടാനുള്ള അധികാരം ആർക്കാണ് എന്നതിനെക്കുറിച്ച് പൊതു വിവരം നൽകുക എന്നതാണ് ഈ വിഭാഗത്തിന്റെ ഉദ്ദേശ്യം. ഇത് പരിശോധിക്കുന്നതിലൂടെ, അന്വേഷണ അധികൃതരോട് ഉചിതമായ ചോദ്യങ്ങൾ ചോദിക്കാൻ നിങ്ങളെ സഹായിക്കും.

നിയമങ്ങളും സാഹചര്യങ്ങളും അനുസരിച്ച് പരിശോധനയും കണ്ടുകെട്ടലും നടത്തുന്ന രീതി മാറാം.

II. പരിശോധന നടത്താനുള്ള അധികാരം ആർക്കാണ്?

Income Tax Act	അസിസ്റ്റന്റ് കമ്മീഷണർ റാങ്കിൽ കുറയാത്ത അല്ലെങ്കിൽ ഉയർന്ന റാങ്കിലുള്ള ആദായ നികുതി ഉദ്യോഗസ്ഥർക്ക് മാത്രമേ അന്വേഷിക്കാൻ കഴിയൂ.
PMLA	ഡയറക്ടർ അല്ലെങ്കിൽ ഡെപ്യൂട്ടി ഡയറക്ടർ റാങ്കിൽ കുറയാത്ത മറ്റേതെങ്കിലും ഉദ്യോഗസ്ഥന് അന്വേഷിക്കാൻ അധികാരമുണ്ട്.
IT Act	ഇൻസ്പെക്ടർ റാങ്കിൽ കുറയാത്ത ഏതൊരു പോലീസ് ഉദ്യോഗസ്ഥനും. കൂടാതെ, കേന്ദ്ര/സംസ്ഥാന ഗവൺമെന്റിലെ മറ്റേതെങ്കിലും ഉദ്യോഗസ്ഥനെ, അന്വേഷിക്കാൻ കേന്ദ്ര ഗവൺമെന്റിന് അധികാരപ്പെടുത്താൻ കഴിയും കൂടാതെ, കൺട്രോളർക്കോ അവർ അധികാരപ്പെടുത്തിയ മറ്റേതെങ്കിലും ഉദ്യോഗസ്ഥനോ അന്വേഷിക്കാം.
2023-ലെ ടെലികമ്മ്യൂണിക്കേഷൻസ് നിയമം	അനധികൃതമായ ടെലികമ്മ്യൂണിക്കേഷൻ നെറ്റ്‌വർക്കോ ഉപകരണങ്ങളോ സൂക്ഷിച്ചിരിക്കുന്നതായോ മറച്ചുവെയ്ക്കുന്നതായോ സംശയമുണ്ടായാൽ, കേന്ദ്ര സർക്കാരിന്റെ അധികൃത ഉദ്യോഗസ്ഥന് ആ സ്ഥലം പരിശോധിക്കാനുള്ള അധികാരമുണ്ട് . [10]



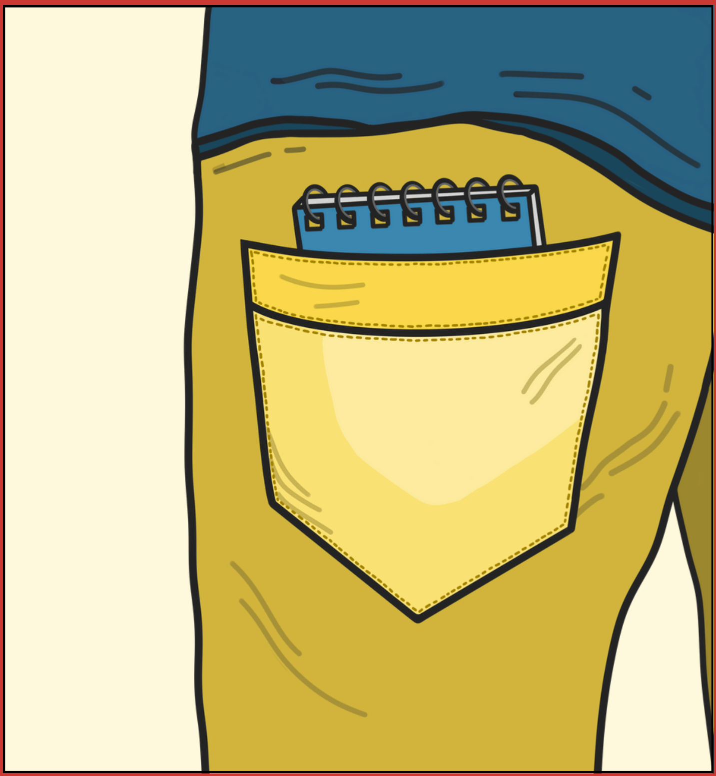
വിഭാഗം 2

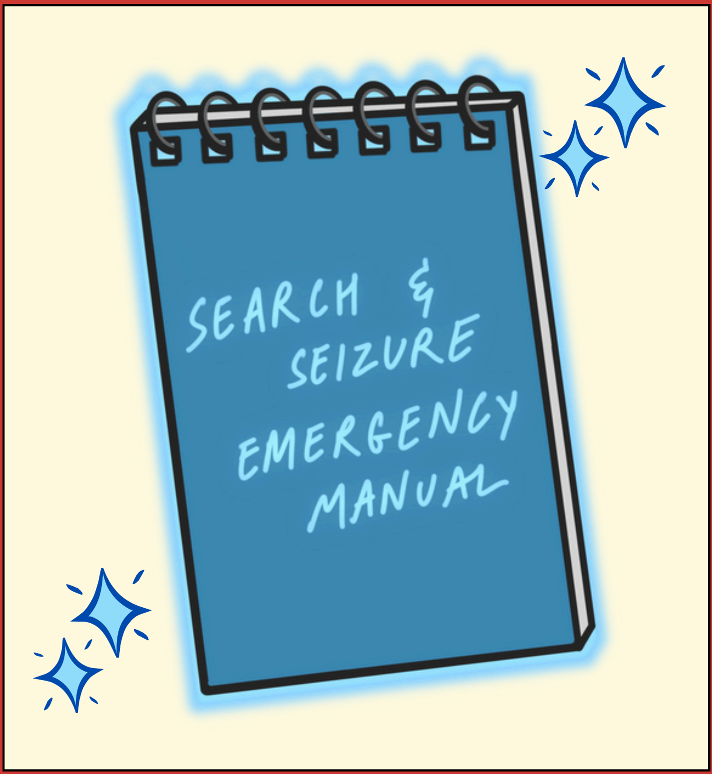
പരിശോധനാ സമയത്ത് എന്ത് ചെയ്യണം?

അന്വേഷണ പ്രക്രിയ സങ്കീർണവും അസ്വസ്ഥമാക്കുന്നതുമാകാം..

ഈ പ്രക്രിയ ശരിയായി കൈകാര്യം ചെയ്യാൻ, അതിന്റെ നടപടിക്രമങ്ങളും ആവശ്യമായ രേഖകളും മനസ്സിലാക്കേണ്ടത് അത്യാവശ്യമാണ്.

ഒരു അന്വേഷണം വിചാരണയിലേക്ക് നയിക്കുകയാണെങ്കിൽ, കോടതിയിൽ സ്വയം വാദിക്കാൻ പരിശോധനയുടെ നടപടിക്രമങ്ങളും അനുബന്ധ മാർഗനിർദേശങ്ങളും പൂർണമായി അറിഞ്ഞിരിക്കേണ്ടത് അനിവാര്യമാണ്.





പരിശോധന ആരംഭിക്കുമ്പോൾ, ഈ ചോദ്യങ്ങൾ പ്രയോജനപ്പെടും

1	**നിങ്ങൾക്ക് വാറന്റ് ഉണ്ടോ?**
2	**അത് ഇലക്ട്രോണിക്കായി സമർപ്പിക്കപ്പെട്ടിട്ടുണ്ടോ?**
3	**ഉണ്ടെങ്കിൽ, ഏത് വിധേനെയാണ്?**
4	**നിങ്ങൾ ഏത് അന്വേഷണ സ്ഥാപനത്തിന്റെ പ്രതിനിധിയാണ്?**
5	**നിങ്ങളുടെ പദവി എന്താണ്?**
6	**എനിക്കെതിരെയുള്ള ആരോപണങ്ങൾ എന്തൊക്കെയാണ്?**

അതോടൊപ്പം, ശ്രദ്ധിക്കുക – നിങ്ങളുടെ ചോദ്യങ്ങൾക്ക് ഉചിതമായ ഉത്തരം ലഭിക്കുന്നില്ലെന്ന് തോന്നുന്നുവെങ്കിൽ, ഉടനെ ഒരു അഭിഭാഷകനുമായി ബന്ധപ്പെടുക. നിങ്ങളുടെ നിയമ പ്രതിനിധി നിയമ പ്രതിനിധി എത്തുംവരെ കൂടുതൽ ചോദ്യങ്ങൾക്ക് ഉത്തരം നൽകുകയും ചെയ്യരുത്.

അധികാരികളിൽ നിന്ന് വിവരങ്ങൾ കൃത്യമായി ശേഖരിക്കുക.

- പോലീസിന് നിങ്ങളുടെ ഇലക്ട്രോണിക് ഉപകരണങ്ങൾ വാറന്റോടുകൂടിയോ അല്ലാതെയോ പരിശോധിക്കാം. **എന്നിരുന്നാലും, പരിശോധനയുടെയും കണ്ടുകെട്ടലിന്റെയും നടപടിക്രമങ്ങളുടെ റെക്കോർഡിന്റെ ഒരു പകർപ്പ്,** [11] **– പോലീസ് ഉദ്യോഗസ്ഥനിൽ നിന്ന് അത് ലഭിച്ചിട്ടുള്ള അടുത്തുള്ള മജിസ്ട്രേട്ടിനോട് എപ്പോഴും ആവശ്യപ്പെടണം.** [12]

- **നിങ്ങളുടെ കൈവശമുള്ള വേറൊരു വ്യക്തിയുടെ ഇലക്ട്രോണിക് രേഖകൾ, ആ വ്യക്തിയുടെ അനുവാദം ഇല്ലാതെ, നൽകരുത്.**

- പരിശോധനയും കണ്ടുകെട്ടാലും ഒരു അന്വേഷണത്തിന്റെ സാധാരണ നടപടിയാണ്. നിങ്ങളുടെ വീടോ ഉപകരണങ്ങളോ പരിശോധിക്കന്നതുകൊണ്ട് നിങ്ങൾ കുറ്റവാളിയാണെന്ന് **അർത്ഥമാക്കുന്നില്ല**. അന്വേഷണ സംഘത്തിന് പരിശോധന നടത്താൻ അനുവാദം നൽകുന്ന എല്ലാ രേഖകളുമുണ്ടെങ്കിൽ, അവരെ അവരുടെ ജോലി ചെയ്യാൻ അനുവദിക്കുക. നിങ്ങളുടെ അഭിഭാഷക/അഭിഭാഷകനുമായി ബന്ധപ്പെടുക, കാരണം പിന്നീട് അവരുടെ സഹായം ആവശ്യമായേക്കാം.

- ചില സമയങ്ങളിൽ അന്വേഷണ അധികാരികൾ നിങ്ങളുടെ ചോദ്യങ്ങൾക്ക് ഉത്തരം നൽകിയേക്കില്ല, അതുകൊണ്ട്, നിനിങ്ങളുടെ ചോദ്യങ്ങളും അവർ നൽകുന്ന മറുപടികളും ഒരു കടലാസിൽ രേഖപ്പെടുത്തി വെക്കുന്നതാണ് നല്ലതായിരിക്കും, അത് പിന്നീട് വിചാരണയിൽ ഉപയോഗിക്കാനാകും.

- നിങ്ങൾക്ക് അന്വേഷണ സംഘത്തിനെ പരിശോധനയിൽ സഹായിക്കേണ്ട യാതൊരു ബാധ്യതയുമില്ല, എന്നാൽ അവരുടെ ജോലിയിൽ തടസ്സം നിൽക്കരുത്. ഉദാഹരണമായി, ഉപകരണവുമായി കടന്നുകളയുകയോ അത് നശിപ്പിക്കുകയോ ചെയ്യരുത്.

പരിശോധനയും കണ്ടുകെട്ടലും നടക്കുന്ന സ്ഥലത്ത് വെച്ച്, ശേഖരിച്ച തെളിവുകളുടെ പ്രാധാന്യവും വിശ്വാസ്യതയും ഉറപ്പാക്കുന്നതിനായി ഉടനടിയുള്ള പരിശോധനയും വിലയിരുത്തലും വിശകലനത്തിന്റെ ഭാഗമാണ്..

ഇതിൽ സ്ഥലത്ത് ലഭിച്ച ഭൗതിക വസ്തുക്കളും ഡിജിറ്റൽ ഉപകരണങ്ങളും അവലോകനം ചെയ്യുകയും രേഖപ്പെടുത്തുകയും ചെയ്യുന്നു, ഡേറ്റ വീണ്ടെടുക്കലും ഫോറൻസിക് വിശകലനവും നടത്തി വിവരങ്ങൾ പരിശോധിക്കുകയും, കൃത്രിമത്വം തടയുകയും ചെയ്യുന്നു. പ്രധാന പാറ്റേണുകളും ബന്ധങ്ങളും കണ്ടെത്തുകയും, വ്യക്തമായ കസ്റ്റഡി ശൃംഖല ഉറപ്പാക്കാൻ വിശദമായ കുറിപ്പുകൾ രേഖപ്പെടുത്തുകയും ചെയ്യുന്നു.

1	**വിശകലനത്തിനായി ഉപയോഗിച്ച ഉപകരണങ്ങളുടെയും അക്കൗണ്ടുകളുടെയും ഒരു ലിസ്റ്റ് സൂക്ഷിക്കുക:** ഉദ്യോഗസ്ഥർ ശേഖരിച്ച എല്ലാ ഡേറ്റയും പിന്നീട് ക്രോസ്-റഫറൻസ് ചെയ്യുന്നത് എളുപ്പമാക്കാൻ വിശകലനത്തിനായി ഉപയോഗിച്ച ഉപകരണങ്ങളുടെയും അക്കൗണ്ടുകളുടെയും ഒരു ലിസ്റ്റ് സൂക്ഷിക്കുക.
2	**നിങ്ങളുടെ ഉപകരണങ്ങളിലെ ഫയലുകളുടെ സ്റ്റോറേജ് ലൊക്കേഷനുകൾ വെളിപ്പെടുത്തരുത്:** അധികാരികൾ പരിശോധനയും കണ്ടുകെട്ടലും നടത്തുമ്പോൾ, നിങ്ങളുടെ സ്വകാര്യതയും വിശ്വാസ്യതയും കാക്കാൻ ഡിവൈസിലെ ഫയലുകളുടെ സ്റ്റോറേജ് ലൊക്കേഷനുകൾ വെളിപ്പെടുത്താതിരിക്കുന്നതാണ് നല്ലത്. ഫയലുകൾ സൂക്ഷിച്ചിരിക്കുന്ന വിവരം നൽകുന്നത് അനുവദനീയമായ പരിധിക്കപ്പുറം പരിശോധനയുടെ വ്യാപ്തി വർദ്ധിപ്പിക്കാനും സെൻസിറ്റീവ് അല്ലെങ്കിൽ അപ്രസക്തമായ വ്യക്തിഗത വിവരങ്ങൾ പുറത്തുവരാനും ഇടയാക്കിയേക്കാം.
3	**Keep note of all IMEI, serial numbers, and specifications of all devices taken for analysis:** ഇത് ഡിവൈസിന്റെ ഐഡന്റിറ്റി സ്ഥിരീകരിക്കാൻ സഹായിക്കുകയും, മറ്റ് ഉപകരണങ്ങളുമായുള്ള ആശയക്കുഴപ്പം ഒഴിവാക്കി, ശരിയായ ഉപകരണമാണ് വിശകലനം ചെയ്യുന്നതെന്നും കോടതിയിൽ ഹാജരാക്കുന്നതെന്നും ഉറപ്പാക്കി തെളിവിന്റെ വിശ്വാസ്യത നിലനിർത്തും.

വിഭാഗം 3

ഇലക്ട്രോണിക് ഉപകരണങ്ങളും നിയമവും

K.S. പുട്ടസ്വാമി കേസിൽ, സുപ്രീം കോടതി വിവര സ്വകാര്യത ഉൾപ്പെടെ സ്വകാര്യതയെ മൗലികാവകാശമായി അംഗീകരിച്ചു. [13] - വീരേന്ദർ ഖന്ന v. കർണാടക സംസ്ഥാനം എന്ന കേസിൽ, കർണാടക ഹൈക്കോടതി ഇലക്ട്രോണിക് ഉപകരണങ്ങൾ പരിശോധിക്കുന്നതിനും കണ്ടുകെട്ടുന്നതിനും പ്രത്യേക മാർഗനിർദേശങ്ങൾ നിശ്ചയിച്ചു. ഒരു സ്മാർട്ട്ഫോൺ അല്ലെങ്കിൽ കമ്പ്യൂട്ടർ സിസ്റ്റം തുറക്കാൻ പാസ്വേഡ്, ബയോമെട്രിക്സ്, അല്ലെങ്കിൽ പാസ്കോഡ് നൽകുന്നത് ഒരു വ്യക്തിയുടെ സ്വയം കുറ്റസമ്മതത്തിനെതിരായ മൗലികാവകാശത്തിന് വിരുദ്ധമല്ലെന്ന് കോടതി വിധിച്ചു. [14]

എന്നിരുന്നാലും, ഫൗണ്ടേഷൻ ഓഫ് മീഡിയ പ്രൊഫഷണൽസ് സുപ്രീം കോടതിയെ സമീപിച്ച്, ഇലക്ട്രോണിക് ഉപകരണങ്ങളിൽ ഒരാളുടെ ധാരാളം വ്യക്തിഗത വിവരങ്ങൾ സൂക്ഷിക്കപ്പെടുന്നതിനാൽ, നിലവിലുള്ള നിയമം സ്വയം കുറ്റസമ്മതത്തിനെതിരായ മൗലികാവകാശങ്ങളും സ്വകാര്യതയും ലംഘിക്കപ്പെടുന്നതിൽ നിന്ന് ആളുകളെ സംരക്ഷിക്കാൻ പര്യാപ്തമല്ലെണ് വാദിച്ചു. [15] അന്വേഷണ ഏജൻസികൾ ഇലക്ട്രോണിക് ഉപകരണങ്ങളുടെ പരിശോധനയ്ക്കും കണ്ടുകെട്ടലിനും മാർഗനിർദേശങ്ങൾ വികസിപ്പിക്കാൻ ഒരു സമിതി രൂപീകരിച്ചു..[16]

വിവിധ നിയമങ്ങൾ പ്രകാരം പരിശോധനയും കണ്ടുകെട്ടലും എങ്ങനെ നടത്തുന്നു വെന്ന് അറിയാൻ അനുബന്ധങ്ങൾ വായിക്കുക.

വിഭാഗം 4

കണ്ടുകെട്ടിയതിന് ശേഷമുള്ള നടപടിക്രമം:

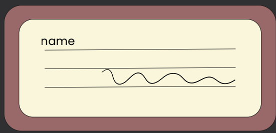
നിങ്ങളുടെ ഉപകരണം കണ്ടുകെട്ടിയ ശേഷം എന്ത് സംഭവിക്കുന്നു

കണ്ടുകെട്ടിയ ഉപകരണങ്ങൾക്കുള്ള ആവശ്യമായ രേഖകൾ

സർട്ടിഫിക്കറ്റുകൾ

[സെക്ഷൻ 63(4)(c) പ്രകാരം]:

ഉപകരണം പരിശോധനയ്ക്കും കണ്ടുകെട്ടലിനും വിധേയമാകുന്ന വ്യക്തിക്ക്, പരിശോധനയും കണ്ടുകെട്ടാലും നടത്തിയ വ്യക്തിയും നടപടിക്രമം നടത്തിയ വിദഗ്ധനും സമർപ്പിക്കേണ്ട സർട്ടിഫിക്കറ്റിന്റെ പകർപ്പ് ആവശ്യപ്പെടാം. [17][18] , ഇതിൽ ഇനിപ്പറയുന്നവ ഉണ്ടാവണം:



പരിശോധനയ്ക്കും കണ്ടുകെട്ടലിനും വിധേയമായ ഉപകരണത്തിന്റെ ഉടമയുടെ പേരും ഒപ്പും.

കണ്ടുകെട്ടിയ ദിവസവും സമയവും.

കണ്ടുകെട്ടിയ സ്ഥലം.

കണ്ടുകെട്ടിയ ഉപകരണങ്ങളുടെ വിവരങ്ങൾ (ബ്രാൻഡ്, മോഡൽ, സീരിയൽ നമ്പർ/IMEI/UIN/UID/MAC)

0000 1111
0000 2222

ഹാഷ് മൂല്യം (ഹാഷ് റിപ്പോർട്ടോടുകൂടി)

വിദഗ്ധൻ എല്ലാ ആവശ്യമായ വിവരങ്ങളോടും കൂടി ഒപ്പിട്ട സർട്ടിഫിക്കറ്റ് നൽകണം.

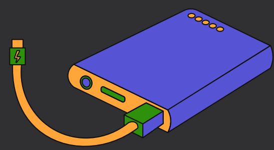
കണ്ടുകെട്ടിയ സമയത്ത് ഹാജരായിരുന്ന സാക്ഷികളുടെ പേര്

കണ്ടുകെട്ടലിന്റെ കാരണം.

പരിശോധനയും കണ്ടുകെട്ടലും ഇലക്ട്രോണിക് രീതിയിൽ, പ്രത്യേകിച്ച് മൊബൈൽ ഫോണിൽ റെക്കോർഡ് ചെയ്യണമെന്ന അഭ്യർത്ഥന.

മജിസ്ട്രേട്ടിന് ലഭിക്കുന്ന റെക്കോർഡിന്റെ ഒരു പകർപ്പ് ആവശ്യപ്പെടുക.

വസ്തുക്കളുടെ പട്ടിക



ചാർജറുകൾ, കേസുകൾ തുടങ്ങിയവ ഉൾപ്പെടെ കണ്ടുകെട്ടിയ എല്ലാ **വസ്തുക്കളുടെ പട്ടിക** [19] ആവശ്യപ്പെടുക.

കണ്ടുകെട്ടിയതിന്റെ കാരണങ്ങൾ

നിങ്ങളുടെ ഉപകരണങ്ങൾ **എന്തുകൊണ്ട് കണ്ടുകെട്ടിയെന്നും** ഏത് നിയമവ്യവസ്ഥ പ്രകാരം കണ്ടുകെട്ടൽ നടത്തിയെന്നും വ്യക്തമായി ചോദിക്കുക.

നിയമോപദേശകന്റെ സേവനം

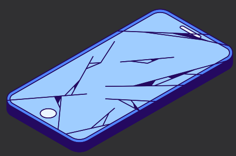
തിരച്ചിൽ നടക്കുന്ന സമയത്ത് **ഒരു വക്കീലുമായി ആലോചിക്കാനുള്ള** നിങ്ങളുടെ അവകാശം ഉറപ്പാക്കുക.

വാറന്റിന്റെ/ഉത്തരവിന്റെ രേഖകൾ

കണ്ടുകെട്ടൽ ഒരു വാറന്റിന്റെയോ മജിസ്ട്രേട്ടിന്റെ ഉത്തരവിന്റെയോ അടിസ്ഥാനത്തിലാണെങ്കിൽ, [20] **ആ രേഖകളുടെ പകർപ്പുകൾ** ആവശ്യപ്പെടുക. വാറന്റ്/ഉത്തരവിൽ ഉദ്ദേശിച്ച വ്യക്തികളുടെ ശരിയായ വിവരങ്ങളുണ്ടോയെന്നും, ബന്ധപ്പെട്ട ഉദ്യോഗസ്ഥൻ ഒപ്പിട്ടിട്ടുണ്ടോയെന്നും പരിശോധിക്കുക.

കണ്ടുകെട്ടലിന്റെ കാലാവധി

ഉപകരണങ്ങൾ എത്ര കാലം കൈവശം വയ്ക്കുമെന്നും തിരികെ നൽകുന്നതിനുള്ള നടപടികളെക്കുറിച്ചും ചോദിക്കുക.



അവസ്ഥയുടെ രേഖ

ഉപകരണങ്ങൾ കൈമാറുന്നതിന് മുമ്പ്, **അവയുടെ അവസ്ഥ** (ഉദാഹരണത്തിന്, പാടുകൾ, കേടുപാടുകൾ) ഫോട്ടോകളോ വീഡിയോകളോ എടുത്ത് രേഖപ്പെടുത്താൻ ആവശ്യപ്പെടുക.

അധിക രേഖകൾ

സന്ദർഭമനുസരിച്ച്, നിങ്ങൾക്ക് ഇനിപ്പറയുന്ന അധിക വിവരങ്ങൾ ആവശ്യപ്പെടാം:

- അന്വേഷണ ഉദ്യോഗസ്ഥന്റെ വിശദാംശങ്ങൾ.
- കണ്ടുകെട്ടലുമായി ബന്ധപ്പെട്ട പരാതിയുടെയോ കേസിന്റെയോ വിവരങ്ങൾ, കേസ് നമ്പർ ഉൾപ്പെടെ.
- അധികാരികൾ പാലിച്ച ബന്ധപ്പെട്ട നടപടിക്രമങ്ങളുടെയോ നയങ്ങളുടെയോ പകർപ്പുകൾ.

നിങ്ങളുടെ ഉപകരണം തിരികെ ലഭിക്കാൻ വളരെ സമയമെടുത്താൽ എന്താണ് സംഭവിക്കുക?

- ഉപകരണം തിരികെ നൽകുന്ന നടപടി, അത് കോടതിയിൽ ഹാജരാക്കിയോ എന്നതിനെ ആശ്രയിച്ചിരിക്കും. ഒരു അന്വേഷണത്തിനോ വിചാരണയ്ക്കോ വേണ്ടി കോടതിയിൽ ഹാജരാക്കിയ ഉപകരണമാണെങ്കിൽ, BNSS 2023-ലെ 497, 503 വകുപ്പുകൾ പ്രകാരം വിചാരണ അവസാനിച്ച ശേഷം കോടതിക്ക് അത് തിരികെ നൽകാൻ ഉത്തരവിടാം. 497-[illegible] വകുപ്പിൽ ഇപ്പോൾ സമയപരിധി വ്യക്തമാക്കിയിട്ടുണ്ട്.

- എന്നാൽ, ഉപകരണം കോടതിയിൽ ഹാജരാക്കിയിട്ടില്ലെങ്കിൽ, മജിസ്ട്രേറ്റ് സമ്മതിക്കുകയാണെങ്കിൽ, ആറ് മാസത്തിനുള്ളിൽ വാങ്ങാൻ ഉത്തരവിടും.അത് ശേഖരിക്കാൻ അവർ നിങ്ങൾക്ക് അനുമതി നൽകും. അതിനായി നിങ്ങൾക്ക് ആറ് മാസം വരെ സമയം നൽകും. **[21]**

ഏത് സാഹചര്യത്തിലും, പോലീസ് കണ്ടുകെട്ടിയ വസ്തു തിരികെ ലഭിക്കാനുള്ള നടപടിക്രമം നിങ്ങളുടെ കേസിന്റെ പ്രത്യേക സാഹചര്യങ്ങൾക്കനുസരിച്ച് വ്യത്യാസപ്പെടാം. നിന്റെ ഉപകരണം തിരികെ ലഭിക്കാൻ തയ്യാറാണെങ്കിലും അതിൽ പ്രശ്നങ്ങൾ നേരിടുകയാണെങ്കിൽ, പോലീസ് കണ്ടുകെട്ടിയ വസ്തു തിരികെ ലഭിക്കാനുള്ള പ്രക്രിയ കേസിന്റെ സാഹചര്യങ്ങൾക്കനുസരിച്ച് വ്യത്യാസപ്പെടുമെന്ന് ഓർക്കുക. എന്നിരുന്നാലും, നിങ്ങൾക്ക് സ്വീകരിക്കാവുന്ന പൊതുവായ ഘട്ടങ്ങളെക്കുറിച്ചുള്ള ഒരു വിവരണം ഇതാ:

വിവരങ്ങൾ ശേഖരിക്കുക: കണ്ടുകെട്ടിയ വസ്തുക്കളുടെ വിശദമായ ഒരു പട്ടിക തയ്യാറാക്കുക, അതിൽ സീരിയൽ നമ്പറുകളും, വിവരണങ്ങളും, സ്പെസിഫിക്കേഷനുകളും ഉൾപ്പെടുത്തുക. കൂടാതെ, വസ്തുവിന്റെ ഉടമസ്ഥത തെളിയിക്കുന്ന രേഖകൾ, ഉദാഹരണത്തിന് വാങ്ങൽ രസീതുകൾ, വിൽപ്പന രേഖകൾ, അല്ലെങ്കിൽ രജിസ്ട്രേഷൻ സർട്ടിഫിക്കറ്റുകൾ എന്നിവ ശേഖരിക്കുക.

പൊലീസ് സ്റ്റേഷനുമായി ബന്ധപ്പെടുക: ആവശ്യമായ എല്ലാ വിവരങ്ങളും ശേഖരിച്ചതിന് ശേഷം, കേസ് ഫയൽ ചെയ്ത പോലീസ് സ്റ്റേഷനിലേക്കോ നിങ്ങളുടെ വസ്തു കണ്ടുകെട്ടിയ സ്ഥലത്തെ അടുത്തുള്ള പോലീസ് സ്റ്റേഷനിലേക്കോ പോകുക. ഓഫീസർ-ഇൻ-ചാർജ്, അന്വേഷണ ഓഫീസർ അല്ലെങ്കിൽ പ്രോപ്പർട്ടി ഡിപ്പാർട്ട്മെന്റിലെ ഏതെങ്കിലും ഉദ്യോഗസ്ഥനുമായി സംസാരിക്കുക. നിങ്ങളുടെ സ്ഥിതി വിശദീകരിച്ച് നിന്റെ വസ്തു തിരികെ ലഭിക്കാൻ അഭ്യർത്ഥിക്കുക. ക്ഷമയോടെയും വിനയത്തോടെയും സഹകരിച്ച് പെരുമാറുകയും, ബന്ധപ്പെട്ട രേഖകൾ ഹാജരാക്കുകയും ചെയ്യുക.

നിയമ സഹായം തേടുക: പോലീസ് സഹകരിക്കുന്നില്ലെങ്കിലോ നടപടിക്രമങ്ങൾ സങ്കീർണമാണെന്ന് തോന്നുകയോ ചെയ്താൽ, വക്കീലിൽ നിന്ന് നിയമ സഹായം തേടുക.

പകരണം തിരികെ ലഭിക്കുമ്പോൾ പരിശോധിക്കേണ്ട പട്ടിക

1. പൊതു പരിശോധന

ഉപകരണങ്ങളും സേവനങ്ങളും	ഉദ്യോഗസ്ഥരിൽ നിന്ന്, പരിശോധിച്ചതോ കണ്ടുകെട്ടിയതോ ആയ ഉപകരണങ്ങളുടെയും, ഇമെയിൽ, ചാറ്റ് മുതലായവ പോലുള്ള പരിശോധിച്ച സേവനങ്ങളുടെയും ഒരു പട്ടിക ശേഖരിക്കുക, അത് കണ്ടുകെട്ടലിന് മുമ്പുള്ള ഡേറ്റാബേസുമായി പരിശോധിക്കാൻ സഹായിക്കും.
ആരംഭവും പ്രവർത്തനവും	ഉപകരണം ഓൺ ചെയ്ത് അത് സാധാരണ രീതിയിൽ പ്രവർത്തിക്കുന്നുണ്ടോ എന്ന് ഉറപ്പാക്കുക. ഇന്റർനെറ്റ് കണക്ഷൻ, ആപ്പ് യൂസേജ്, ക്യാമറ തുടങ്ങിയ അടിസ്ഥാന പ്രവർത്തനങ്ങളും ഫീച്ചറുകളും പരിശോധിക്കുക.
ഉപകരണം തിരികെ ലഭിക്കൽ	റെയ്ഡിന് ശേഷം, കണ്ടുകെട്ടാത്ത ഉപകരണങ്ങളെല്ലാം നിങ്ങൾക്ക് തിരികെ ലഭിച്ചിട്ടുണ്ടോ എന്ന് ഉറപ്പാക്കുക.
പുറമെയുള്ള നിലവാരം	ഉപകരണത്തിൽ ഏതെങ്കിലും ഭൗതിക കേടുപാടുകൾ ഉണ്ടോ എന്ന് പരിശോധിക്കുക, പ്രത്യേകിച്ച് സീലുകളിലോ സ്ക്രൂകളിലോ കൃത്രിമത്വത്തിന്റെ ലക്ഷണങ്ങൾ. ഉപകരണത്തിലെ സംശയാസ്പദമായ അടയാളങ്ങളോ കേടുപാടുകളോ ഫോട്ടോകളോ രേഖകളോ ആയി രേഖപ്പെടുത്തുക.
സെറ്റിങ്ങുകളും കൺഫിഗ്യുറേഷനുകളും	ഏതെങ്കിലും സെറ്റിങ്ങുകൾ, ആക്സസ് കൺട്രോളുകൾ അല്ലെങ്കിൽ കൺഫിഗ്യുറേഷനുകൾ മാറ്റിയിട്ടുണ്ടോ എന്ന് പരിശോധിക്കുക, പ്രത്യേകിച്ച് സെക്യൂരിറ്റി, പ്രൈവസി, ലൊക്കേഷൻ സേവനങ്ങളിൽ.

പകരണം തിരികെ ലഭിക്കുമ്പോൾ പരിശോധിക്കേണ്ട പട്ടിക

1. പൊതു പരിശോധന

ഇൻസ്റ്റാൾ ചെയ്ത സോഫ്റ്റ്‌വെയറുകൾ/ആപ്പുകൾ	നിങ്ങളുടെ ഫോണിൽ പുതിയ സോഫ്റ്റ്‌വെയർ അല്ലെങ്കിൽ ഓപ്പറേറ്റിംഗ് സിസ്റ്റം ഇൻസ്റ്റാൾ ചെയ്തിട്ടുണ്ടോ എന്ന് പരിശോധിക്കുക, കൂടാതെ ഇൻസ്റ്റാൾ ചെയ്ത ആപ്പുകളുടെ പട്ടിക കണ്ടുകെട്ടലിന് മുമ്പ് നിങ്ങൾക്ക് ഓർമയുള്ളവയുമായി താരതമ്യം ചെയ്യുക. അജ്ഞാതമോ സംശയാസ്പദമോ ആയ സോഫ്റ്റ്‌വെയറുകൾ അല്ലെങ്കിൽ ആപ്ലിക്കേഷനുകൾ സ്പൈവെയർ അല്ലെങ്കിൽ മാൽവെയർ ആയിരിക്കാം.
അസാധാരണ പ്രവർത്തനങ്ങൾ	ഉപകരണത്തിൽ വിശദീകരിക്കാനാകാത്തതോ അസാധാരണമോ ആയ പ്രവർത്തനങ്ങൾ, ഉദാഹരണത്തിന് ബാറ്ററി അമിതമായി കുറയുക,, ഡേറ്റാ ഉപഭോഗം, പ്രവർത്തനരഹിതമായ ഫീച്ചറുകൾ മുതലായവ, സ്പൈവെയർ അല്ലെങ്കിൽ മാൽവെയർ ആയേക്കാമെന്ന സൂചനകളാകാം.
ഓൺലൈൻ അക്കൗണ്ടുകൾ	ഇമെയിൽ, ഓൺലൈൻ സ്റ്റോറേജ്, സോഷ്യൽ മീഡിയ തുടങ്ങിയ ഓൺലൈൻ അക്കൗണ്ടുകളിൽ, നിങ്ങളുടെ ഉപയോഗത്തിലല്ലാത്ത മറ്റ് ഉപകരണങ്ങൾ ലോഗിൻ ചെയ്തിട്ടുണ്ടോ എന്ന് പരിശോധിക്കുക. അപരിചിതമായ ഉപകരണങ്ങൾ കണ്ടെത്തിയാൽ, അവ നീക്കം ചെയ്യാൻ ഉടനടി നടപടിയെടുത്ത് അക്കൗണ്ട് സുരക്ഷിതമാക്കുക. സാധാരണഗതിയിൽ ഇവ അക്കൗണ്ടിന്റെ സെക്യൂരിറ്റി സെറ്റിങ്ങിലൂടെ ചെയ്യാം.

പകരണം തിരികെ ലഭിക്കുമ്പോൾ പരിശോധിക്കേണ്ട പട്ടിക

2. ഡേറ്റാ സമഗ്രത

ഡേറ്റ പരിശോധന	നിങ്ങളുടെ എല്ലാ ഡേറ്റയും സുരക്ഷിതമാണോ എന്ന് പരിശോധിക്കുക. ഫയലുകൾ, ഫോട്ടോകൾ, ഡോക്യുമെന്റുകൾ, മെറ്റാഡേറ്റ, മറ്റ് ഡേറ്റ എന്നിവയിൽ ഒന്നും നഷ്ടമോ തകരാറോ ഇല്ലെന്ന് ഉറപ്പുവരുത്തുക.
ഫയൽ ടൈംസ്റ്റാമ്പുകൾ	നിങ്ങളുടെ ഉപകരണത്തിലെ പ്രധാന ഫയലുകളുടെയും ഡോക്യുമെന്റുകളുടെയും ടൈംസ്റ്റാമ്പുകൾ പരിശോധിക്കുക, കാരണം മാറ്റം വരുത്തിയ ടൈംസ്റ്റാമ്പുകൾ അനധികൃത പ്രവേശനമോ മാറ്റമോ സൂചിപ്പിക്കാം.
ഫയൽ ഹാഷുകൾ	പ്രധാന ഫയലുകളുടെ ക്രിപ്റ്റോഗ്രാഫിക് ഹാഷുകൾ കണ്ടുകെട്ടലിന് മുമ്പും ശേഷവും ഉണ്ടാക്കി താരതമ്യം ചെയ്യുക. വ്യത്യാസങ്ങൾ ഫയലിൽ മാറ്റമോ മാറ്റിസ്ഥാപനമോ ഉണ്ടായതിനെ സൂചിപ്പിക്കാം.
ഫോറൻസിക് ടൂൾ സ്കാനുകൾ	നിങ്ങളുടെ ഉപകരണത്തിൽ മറഞ്ഞിരിക്കുന്ന ഫയലുകൾ, സ്പൈവെയർ അടയാളങ്ങൾ, അല്ലെങ്കിൽ റൂട്ട്കിറ്റുകൾ എന്നിവ കണ്ടെത്താൻ ആന്റി-മാൽവെയർ, ഫോറൻസിക് സോഫ്റ്റ്‌വെയർ എന്നിവ ഉപയോഗിക്കാൻ ശ്രമിക്കുക. ഈ ഉപകരണങ്ങൾ സങ്കീർണമാകാം, അതിനാൽ ഡേറ്റാ റിക്കവറി അല്ലെങ്കിൽ സൈബർ സുരക്ഷാ വിദഗ്ധന്റെ സഹായം തേടുന്നത് നല്ലതാണ്.

പകരണം തിരികെ ലഭിക്കുമ്പോൾ പരിശോധിക്കേണ്ട പട്ടിക

3. അധിക പരിഗണനകൾ

ബാക്കപ്പ് ലോഗുകൾ	നിങ്ങളുടെ ഉപകരണം അനുവദിക്കുന്നുണ്ടെങ്കിൽ, ബാക്കപ്പ് ലോഗുകളിലോ സിസ്റ്റം ലോഗുകളിലോ കണ്ടുകെട്ടൽ കാലയളവിൽ അസാധാരണമോ അനധികൃതമോ ആയ പ്രവർത്തനങ്ങൾ കാണിക്കുന്നുണ്ടോ എന്ന് നോക്കുക.
ക്ലൗഡ് സ്റ്റോറേജ്	ഉപകരണവുമായി ലിങ്ക് ചെയ്ത നിങ്ങളുടെ ക്ലൗഡ് സ്റ്റോറേജ് അക്കൗണ്ടുകളിൽ ഏതെങ്കിലും അനധികൃത പ്രവേശനമോ മാറ്റങ്ങളോ ഉണ്ടോ എന്ന് പരിശോധിക്കുക.
ഡോക്യുമെന്റേഷൻ	നിങ്ങളുടെ കണ്ടെത്തലുകളെക്കുറിച്ച് വിശദമായ രേഖകൾ സൂക്ഷിക്കുക, ടൈംസ്റ്റാമ്പുകൾ, സ്ക്രീൻഷോട്ടുകൾ, സംശയാസ്പദ പ്രവർത്തനങ്ങളെക്കുറിച്ചുള്ള കുറിപ്പുകൾ എന്നിവ ഉൾപ്പെടുത്തി. നിയമനടപടികൾക്ക് ഈ രേഖകൾ നിർണായകമാണ്.
പാസ്‌വേഡ് മാനേജ്മെന്റ്	നിങ്ങളുടെ ഉപകരണവുമായും ഓൺലൈൻ അക്കൗണ്ടുകളുമായും ബന്ധപ്പെട്ട എല്ലാ നിലവിലുള്ള പാസ്‌വേഡുകളും മാറ്റുക, കാരണം അധികാരികൾ നിങ്ങളുടെ പാസ്‌വേഡുകളുടെ പകർപ്പ് എടുക്കാൻ സാധ്യതയുണ്ട്.

വിഭാഗം 5

തയ്യാറെടുപ്പ്:

നിങ്ങളുടെ ഉപകരണങ്ങൾ സുരക്ഷിതമാക്കൽ

ഇന്നത്തെ ഡിജിറ്റൽ യുഗത്തിൽ, ഉപകരണങ്ങളും അവയിലെ വിവരങ്ങളും അമൂല്യമാണ്.

ഈ വിവരങ്ങൾ സുരക്ഷിതമാക്കാൻ ഉപകരണങ്ങൾ സംരക്ഷിക്കേണ്ടത് അനിവാര്യമാണ്.

ഭീഷണികൾക്കെതിരെ മുൻകരുതൽ എടുക്കുന്നത് എളുപ്പവും അത്യാവശ്യവുമാണ്. നിങ്ങളുടെ ഫോൺ ഹാക്ക് ചെയ്യപ്പെട്ട് സ്വകാര്യ സന്ദേശങ്ങൾ പുറത്തുവന്നാൽ എന്താകും സ്ഥിതിയെന്ന് ഒന്ന് ചിന്തിക്കുക! ശക്തമായ പാസ്‌വേഡുകൾ, ഓൺലൈനിൽ പങ്കുവയ്ക്കുന്നതിൽ ജാഗ്രത, സോഫ്റ്റ്‌വേർ അപ്ഡേറ്റ് എന്നിവ നിങ്ങളുടെ ഡേറ്റയ്ക്ക് ശക്തമായ സുരക്ഷാ കവചം തീർക്കും. ചെറിയൊരു ജാഗ്രത പാലിച്ചാൽ നിങ്ങളുടെ ഓൺലൈൻ ജീവിതം സുരക്ഷിതമാക്കാൻ വലിയ പങ്കുവഹിക്കും. നിങ്ങളുടെ ഡേറ്റ സുരക്ഷിതമാക്കാനുള്ള ചില മികച്ച മാർഗ്ഗങ്ങൾ ചുവടെ കൊടുക്കുന്നു.

നിങ്ങളുടെ ഓൺലൈൻ പ്രവർത്തനങ്ങൾ സംരക്ഷിക്കുക | വഴികൾ:

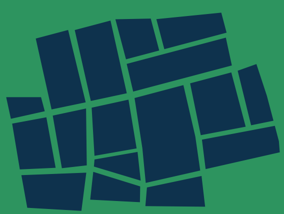
നിങ്ങളുടെ പ്രവർത്തനങ്ങൾ മറയ്ക്കുക

VPN-കളും ടോറും ഉപയോഗിച്ച് നിന്റെ ഓൺലൈൻ പ്രവർത്തനങ്ങൾ സംരക്ഷിക്കാം. ഇതൊരു സീക്രെട് ഏജന്റ് രഹസ്യ ദൗത്യത്തിനിടെ ആൾമാറാട്ടം നടത്തുന്ന പോലെയാണ്.

VPN-കൾ

നിങ്ങളുടെ ഇന്റർനെറ്റ് ട്രാഫിക്കിന് ഒരു സുരക്ഷിത തുരങ്കം ഉണ്ടെന്ന് സങ്കല്പിക്കുക. ഇത് നിങ്ങളുടെ യഥാർത്ഥ സ്ഥാനം മറയ്ക്കുകയും ഡേറ്റ എൻക്രിപ്റ്റ് ചെയ്യുകയും ചെയ്യുന്നു, അത് നിങ്ങൾക്കും VPN-നും മാത്രം മനസ്സിലാകുന്ന രഹസ്യ കോഡ് പോലെയാണ്. നിങ്ങളുടെ പ്രവർത്തനങ്ങൾ ലോഗ് ചെയ്യാത്ത വിശ്വസനീയമായ VPN സേവനം തിരഞ്ഞെടുക്കുക.

ടോർ (Tor)



ഒരു രഹസ്യ പാതകളുടെ കുരുക്കഴിച്ച മാർഗം സങ്കല്പിക്കുക. ടോർ നിങ്ങളുടെ ഇന്റർനെറ്റ് ട്രാഫിക്കിനെ എൻക്രിപ്റ്റ് ചെയ്ത റിലേകളുടെ പാളികളിലൂടെ കടത്തിവിടും, ഇത് ട്രാക്ക് ചെയ്യാൻ ഏറെക്കുറെ അസാധ്യമാണ്. അധിക സ്വകാര്യതയ്ക്കായി ടോർ ബ്രൗസർ ഡൗൺലോഡ് ചെയ്യുക.

ബുദ്ധിപൂർവം തിരഞ്ഞെടുക്കുക

എല്ലാ സെർച്ച് എൻജിനുകളും ഒരേ മാനദണ്ഡം പുലർത്തുന്നില്ല. ഡക്ക്ഡക്ക്ഗോ(DuckDuckGo) പോലുള്ളവ സ്വകാര്യതയെ മുൻനിർത്തി പ്രവർത്തിക്കുകയും നിങ്ങളുടെ സെർച്ചുകളെ ട്രാക്ക് ചെയ്യാതിരിക്കുകയും ചെയ്യുന്നു. ബ്രൗസർ ഹിസ്റ്ററി സൂക്ഷിക്കുന്നുണ്ടെങ്കിലും, POST അഭ്യർത്ഥനകൾ ഉപയോഗിക്കുന്ന സെർച്ച് എൻജിനുകൾ നിങ്ങളുടെ തിരയലുകളെ രഹസ്യമാക്കി നിലനിർത്തും.

ഇൻകോഗ്നിറ്റോ മോഡ്		"ഇൻകോഗ്നിറ്റോ മോഡ്" എന്നത് ഒരു സീക്രെട് ഏജന്റിന്റെ മുഖംമൂടി പോലെ കണക്കാക്കാം. ഇത് ബ്രൗസിംഗ് ഹിസ്റ്ററി, കുക്കികൾ, ഫോം ഡേറ്റ എന്നിവ സൂക്ഷിക്കപ്പെടുന്നതിൽ നിന്ന് തടയുന്നു, ഇത് നിങ്ങളുടെ ഓൺലൈൻ പ്രവർത്തനങ്ങൾ മറ്റുള്ളവർക്ക് കണ്ടെത്താനാകാത്തവിധം സുരക്ഷിതമാക്കുന്നു.
ജാഗ്രത പുലർത്തുക		ഈ ഉപകരണങ്ങൾ ഉപയോഗിച്ചാലും, പൂർണ സ്വകാര്യത ലഭ്യമല്ല. നിങ്ങൾ സന്ദർശിക്കുന്ന വെബ്സൈറ്റുകളിൽ ശ്രദ്ധിക്കുക, സുരക്ഷിത കണക്ഷനുകൾ (ലോക്ക് ഐക്കൺ!) ഉറപ്പുവരുത്തുക, അനാവശ്യമായി സ്വകാര്യ വിവരങ്ങൾ ഓൺലൈനിൽ പങ്കിടുന്നത് ഒഴിവാക്കുക.
വേഗതയും സ്വകാര്യതയും		VPN, TOR എന്നിവ എൻക്രിപ്ഷനും റീറൂട്ടിംഗും കാരണം നിങ്ങളുടെ ഇന്റർനെറ്റിന്റെ വേഗത കുറച്ചേക്കാം. ഇത് ഒരു വിട്ടുവീഴ്ചയാണ്: കുറഞ്ഞ വേഗതയ്ക്ക് പകരം കൂടുതൽ സ്വകാര്യത. നിങ്ങളുടെ ആവശ്യങ്ങൾക്ക് അനുയോജ്യമായത് തിരഞ്ഞെടുക്കുക.

ബോണസ് ടിപ്പ്:
നിങ്ങളുടെ ഡേറ്റ എങ്ങനെ കൈകാര്യം ചെയ്യപ്പെടുന്നുവെന്ന് അറിയാൻ, നിങ്ങൾ ഉപയോഗിക്കുന്ന ഏതൊരു ഉപകരണത്തിന്റെയും സ്വകാര്യതാ നയവും സേവന നിബന്ധനകളും എപ്പോഴും പരിശോധിക്കുക. ഈ ലളിതമായ നടപടികൾ പാലിച്ചാൽ, നിങ്ങളുടെ ഓൺലൈൻ സ്വകാര്യത നിങ്ങളുടെ കൈവശം നിലനിർത്താനും, നിങ്ങളുടെ ഓൺലൈൻ സ്വകാര്യതയുടെ നിയന്ത്രണം സ്വയം ഏറ്റെടുക്കാനും ഡിജിറ്റൽ ജീവിതം സുരക്ഷിതമാക്കാനും കഴിയും. ഓർമിക്കുക, ജെയിംസ് ബോണ്ടിന് പോലും ചിലസമയങ്ങളിൽ ആൾമാറാട്ടം നടത്തേണ്ടി വരാറുണ്ട്!

ജോലിയ്ക്ക് ആവശ്യമായ ഉപകരണങ്ങളും VS. വ്യക്തിപരമായ ആവശ്യങ്ങൾക്കുള്ള ഉപകരണങ്ങളും

നിങ്ങൾക്ക് രണ്ട് സ്യൂട്ട്കേസുകൾ ഉണ്ടെന്ന് കരുതുക: ഒന്ന് നിങ്ങളുടെ ജോലി ആവശ്യങ്ങൾക്കും മറ്റൊന്ന് വ്യക്തിപരമായ കാര്യങ്ങൾക്കും. ജോലിക്കുള്ള ലാപ്ടോപ്പും ഫോണും വേർതിരിച്ച് ഉപയോഗിക്കുന്നത് ഈ സ്യൂട്ട്കേസുകൾ വെവ്വേറെ സൂക്ഷിക്കുന്നതിന് തുല്യമാണ് – ഇത് നിങ്ങളുടെ ജീവിതത്തെ ക്രമപ്പെടുത്തുകയും തൊഴിൽ, വ്യക്തിപരമായ മേഖലകളെ സുരക്ഷിതമാക്കുകയും ചെയ്യുന്നു.

വ്യക്തിപരവും തൊഴിൽതൊഴിൽപരവുമായ ജീവിതങ്ങൾക്കായി വെവ്വേറെ ഉപകരണങ്ങൾ ഉപയോഗിക്കാൻ ശ്രമിക്കുക.

A. ഡേറ്റ ഡിറ്റക്ടീവ്: വെവ്വേറെ ഉപകരണങ്ങൾ ഉപയോഗിക്കുന്നത് വ്യക്തിപരവും തൊഴിൽ പരവുമായ ഡേറ്റകൾ കൂട്ടിക്കലരാനുള്ള അപകടസാധ്യത കുറയ്ക്കുന്നു, ഇത് സുരക്ഷ ശക്തിപ്പെടുത്തുകയും രണ്ടിന്റെയും സ്വകാര്യത സംരക്ഷിക്കുകയും ചെയ്യുന്നു. ജോലിക്കും വ്യക്തിപരമായ ആവശ്യങ്ങൾക്കും വെവ്വേറെ ഉപകരണങ്ങൾ ഉപയോഗിക്കുമ്പോൾ, നിങ്ങളൊരു ഡേറ്റ ഡിറ്റക്ടീവ് ആകുന്നു! നിങ്ങളുടെ ജോലി ഫയലുകൾ വ്യക്തിപരമായ ചിത്രങ്ങളിലേക്കോ, അല്ലെങ്കിൽ തിരിച്ചോ ഇടകലരുന്നത് തടഞ്ഞ്, വ്യത്യസ്ത താക്കോലുകളോടുകൂടിയ രണ്ട് പൂട്ടിയ സ്യൂട്ട്കേസുകൾ പോലെ ഇവയെല്ലാം സുരക്ഷിതവും രഹസ്യവുമായി സൂക്ഷിക്കുന്നു.

B. ആക്സസ് കണ്ട്രോൾ നിൻജ: നിങ്ങളുടെ ജോലി-സംബന്ധമായ സെൻസിറ്റീവ് വിവരങ്ങൾക്ക് ആക്സസ് നിയന്ത്രിക്കുന്നതിന്, ജോലിപരവും വ്യക്തിപരവുമായ ഉപകരണങ്ങൾ വേർതിരിക്കേണ്ടത് അത്യാവശ്യമാണ്. ഇത് നിങ്ങളുടെ ഓഫീസ് ബാഗിന് ഒരു രഹസ്യ കോഡ് നൽകുന്നത് പോലെയാണ്. അധികാരമുള്ളവർക്ക് മാത്രം (നിങ്ങൾക്കും നിങ്ങളുടെ മേലധികാരിക്കും) ജോലി-സംബന്ധമായ വിവരങ്ങൾ ആക്സസ് ചെയ്യാൻ കഴിയും. അതേസമയം, നിങ്ങളുടെ വ്യക്തിപരമായ ബാഗ് നിങ്ങളുടെ സ്വകാര്യതയ്ക്കായി സുരക്ഷിതമായിരിക്കും. ഇത് ആകസ്മികമായ വിവര ചോർച്ചയോ അനധികൃത ആക്സസോ തടയുകയും നിങ്ങളുടെ ജോലി ജീവിതം സുരക്ഷിതവും ക്രമീകൃതവുമാക്കുകയും ചെയ്യും.

C. ഉത്തരവാദിത്തം ഏറ്റെടുക്കുന്നയാൾ: ജോലി സംബന്ധമായ പ്രവർത്തനങ്ങൾക്കും ഡേറ്റകൾക്കും വ്യക്തമായ ഉടമസ്ഥതയും ഉത്തരവാദിത്തവും ഉറപ്പാക്കാൻ, ഉപകരണങ്ങൾ വേർതിരിക്കേണ്ടത് അത്യാവശ്യമാണ്. പ്രത്യേക ഉപകരണങ്ങൾ ഉപയോഗിക്കുന്നത് ഉത്തരവാദിത്തം ആർക്കാണെന്നത് വ്യക്തമാക്കും. ഇത് നിങ്ങളുടെ ബാഗുകൾ ലേബൽ ചെയ്യുന്നത് പോലെയാണ്. ഓഫീസിലെ ജോലി ബാഗ് നിങ്ങളുടേതാണെന്ന് എല്ലാവർക്കും അറിയാം, അതേസമയം വ്യക്തിപരമായ ബാഗിൽ നിങ്ങൾക്ക് ഇഷ്ടമുള്ളത് വയ്ക്കാം. ഇത് ജോലികൾ ട്രാക്ക് ചെയ്യാനും നിങ്ങൾക്കും നിങ്ങളുടെ സഹപ്രവർത്തകർക്കും ഉത്തരവാദിത്തം നിലനിർത്താനും എളുപ്പമാക്കും.

ഓർക്കുക, നിങ്ങളുടെ ജോലി/വ്യക്തിപരമായ ഉപകരണങ്ങൾ വേർതിരിക്കുന്നത് രണ്ട് ഗാഡ്ജറ്റുകൾ ഉണ്ടായിരിക്കുക എന്നതിനപ്പുറം ഇത് നിങ്ങളുടെ സ്വകാര്യത സംരക്ഷിക്കാനും, ഒതുക്കമൊക്കാനും ജീവിതം എളുപ്പമാക്കാനുമാണ്. അതിനാൽ, ഒരു ഡേറ്റ ഡിറ്റക്ടീവായും, ആക്സസ് കൺട്രോൾ നിൻജയായും, ഉത്തരവാദിത്തം ഏറ്റെടുക്കുന്നയാളുമായി മുന്നോട്ട് പോകുക! നിങ്ങളുടെ ബാഗുകൾ ലേബൽ ചെയ്യാൻ മറക്കരുത്!

ബോണസ് ടിപ്പ്: ഉപകരണങ്ങൾ വേർതിരിച്ചാലും, ഓൺലൈനിൽ എന്ത് പങ്കുവെക്കുന്നു, ആർക്ക് ആക്സസ് നൽകുന്നു എന്നതിൽ എപ്പോഴും ശ്രദ്ധപുലർത്തണം. ഒരു സിസ്റ്റവും പൂർണമായി സുരക്ഷിതമല്ല, അതിനാൽ ജാഗ്രതയോടെ നിങ്ങളുടെ ഡിജിറ്റൽ ലോകം ആസ്വദിക്കുക!

നിങ്ങളുടെ ഡേറ്റയെ ഒരു നിധിയെപ്പോലെ സംരക്ഷിക്കുക: എൻക്രിപ്ഷൻ ലേയറുകടെ ഒരു മാർഗ്ഗനിർദ്ദേശം

നിങ്ങളുടെ ഡേറ്റ എന്നത് വളരെ പ്രധാനപ്പെട്ട രഹസ്യങ്ങൾ അടങ്ങിയ ഒരു ശേഖരം ആണെന്ന് കരുതുക. ഈ രഹസ്യങ്ങൾ സംരക്ഷിക്കാൻ പലതരം സുരക്ഷാ സംവിധാനങ്ങൾ വേണ്ടിവരും, അല്ലേ?

അതുപോലെയാണ് എൻക്രിപ്ഷൻ ലേയറുകളും പ്രവർത്തിക്കുന്നത്!

ഹോൾ ചെസ്റ്റ് ലോക്ക് (FDE):

- നിങ്ങളുടെ ഹാർഡ് ഡ്രൈവ് മൊത്തത്തിൽ എൻക്രിപ്റ്റ് ചെയ്യുക, അത് ഒരു വലിയ നിധി പെട്ടിയിൽ ശക്തമായ ഒരു പൂട്ടിടുന്നത് പോലെയാണ്.
- BitLocker (Windows), FileVault (macOS), അല്ലെങ്കിൽ VeraCrypt (തേർഡ് പാർട്ടി) പോലുള്ള ഉപകരണങ്ങൾ ഉപയോഗിക്കുക.

സീക്രെട് കമ്പാർട്മെന്റ് ലോക്കുകൾ (OS-തലത്തിൽ):

- macOS-ൽ എൻക്രിപ്റ്റ് ചെയ്ത ഡിസ്ക് ഇമേജുകൾ (നിധി പെട്ടിക്കുള്ളിലെ രഹസ്യ പെട്ടികൾ) ഉണ്ടാക്കുക.
- ചില ഓപ്പറേറ്റിംഗ് സിസ്റ്റങ്ങളിൽ എൻക്രിപ്റ്റ് ഫയൽ സിസ്റ്റങ്ങൾ (മറഞ്ഞിരിക്കുന്ന അറകൾ പോലെ) ഉപയോഗിക്കുക.

ഓരോ ജം പൗഞ്ചുകൾ (ആപ്പ് തലത്തിൽ)

- പാസ്‌വേഡുകൾ, നോട്ടുകൾ, മെസേജുകൾ തുടങ്ങിയ പ്രധാനപ്പെട്ട വിവരങ്ങളെ എൻക്രിപ്ഷൻ സൗകര്യങ്ങളുള്ള ആപ്ലിക്കേഷനുകൾ ഉപയോഗിച്ച് സുരക്ഷിതമാക്കുക.
- ഇതിൽ പാസ്‌വേഡ് മാനേജർമാർ, സുരക്ഷിതമായ നോട്ടുകൾ സൂക്ഷിക്കുന്ന ആപ്ലിക്കേഷനുകൾ, എൻഡ്-ടു-എൻഡ് എൻക്രിപ്ഷനോടുകൂടിയ സന്ദേശമയയ്ക്കാനുള്ള ആപ്ലിക്കേഷനുകൾ

പ്രധാന ഓർമ്മകൾ:

- ഓരോ ലോക്കിനും (എൻക്രിപ്ഷൻ ലെയർ) ശക്തവും വ്യത്യസ്തവുമായ പാസ്‌വേഡുകളോ കീകളോ ഉപയോഗിക്കുക.
- നിങ്ങളുടെ സുരക്ഷ ഉറപ്പാക്കുന്നതിന് സോഫ്റ്റ്‌വെയർ അപ്‌ഡേറ്റുകൾ പതിവായി ചെയ്യുക.
- നിന്റെ എൻക്രിപ്റ്റ് ചെയ്ത ഡേറ്റ (നിധി ഭൂപടങ്ങൾ!) ആവശ്യമായി വരുമ്പോൾ വീണ്ടെടുക്കുന്നതിനായി ബാക്കപ്പ് ചെയ്യുക.

ഈ എൻക്രിപ്ഷൻ പൂട്ടുകൾ അടുക്കുന്നതിലൂടെ, നിങ്ങളുടെ ഡേറ്റയ്ക്ക് ഒരു കോട്ട നിങ്ങൾ സൃഷ്ടിക്കും, അത് നിങ്ങളുടെ ഡിജിറ്റൽ നിധികൾ ആർക്കും മോഷ്ടിക്കാൻ വളരെ പ്രയാസകരമാക്കും!

സ്വകാര്യതയും സൈബർസുരക്ഷയും ഉറപ്പാക്കുന്നു: ഓൺലൈനിലും ഓഫ്‌ലൈനിലും

- സന്ദേശങ്ങൾ വായിച്ചതിന് ശേഷമോ മുൻകൂട്ടി നിശ്ചയിച്ച സമയത്തിന് ശേഷമോ സ്വയം ഇല്ലാതാകുന്ന മെസേജിംഗ് സേവനങ്ങളോ ആപ്ലിക്കേഷനുകളോ ഉപയോഗിക്കുക. Signal, Telegram, WhatsApp തുടങ്ങിയ ആപ്പുകൾ അപ്രത്യക്ഷമാകുന്ന മെസേജിങ് ഫീച്ചറുകൾ നൽകുന്നു, ആശയവിനിമയം താൽക്കാലികമായിരിക്കുകയും വായനയ്ക്ക് ശേഷമോ നിശ്ചിത കാലയളവിന് ശേഷമോ ചാറ്റുകളിലോ ഹിസ്റ്റോറിയിലോ തുടരുന്നില്ലായെന്ന് ഉറപ്പാക്കുന്നു.

- ഫിംഗർപ്രിന്റ് അല്ലെങ്കിൽ ഫേസ് ഐഡിറെക്കഗ്നിഷൻ പകരം, ബോധപൂർവമായ ശ്രദ്ധയോ വ്യക്തമായ സമ്മതമോ ആവശ്യമില്ലാത്തതിനാൽ, ഓഥന്റിക്കേഷനായി പാസ്‌വേഡ് അല്ലെങ്കിൽ പിൻ ഉപയോഗിക്കുക. പാസ്‌വേഡ് അല്ലെങ്കിൽ പിൻ ഉപയോഗിക്കുന്നത്, സുരക്ഷിത വിവരങ്ങളിലേക്കോ ഉപകരണങ്ങളിലേക്കോ പ്രവേശനം ഉപയോക്താവിന്റെ അറിവിനെ മാത്രം ആശ്രയിക്കുന്നതിനാൽ, ബോധപൂർവമായ പ്രവർത്തനവും വ്യക്തമായ സമ്മതവും വഴി നിയന്ത്രണവും സുരക്ഷയും ഉറപ്പാക്കുന്നു.

- നിങ്ങളുടെ പാസ്‌വേഡുകളുടെ ഒരു ഭാഗം ഒരു പാസ്‌വേഡ് മാനേജറിൽ സുരക്ഷിതമായി സൂക്ഷിക്കുകയും ബാക്കി ഭാഗം മനഃപാഠമാക്കുകയും ചെയ്യുന്നത് നിങ്ങളുടെ അക്കൗണ്ടുകളുടെ സുരക്ഷ വർദ്ധിപ്പിക്കുന്നതിനുള്ള ഒരു മികച്ച തന്ത്രമാണ്.

- ഒരു പാസ്‌വേഡ് മാനേജറിൽ, ഉദാഹരണത്തിന്, "12345" എന്ന ഭാഗം സുരക്ഷിതമായി സംഭരിക്കുകയും "fdsjrie" എന്ന ബാക്കി ഭാഗം ഓർമ്മയിൽ സൂക്ഷിക്കുകയും ചെയ്യുന്നതിലൂടെ, "12345fdsjrie" എന്ന പൂർണ്ണ പാസ്‌വേഡ് രൂപപ്പെടുത്താം. ഈ രീതി പാസ്‌വേഡ് മാനേജറിന്റെ എൻക്രിപ്ഷൻ സുരക്ഷയും നിങ്ങളുടെ ഓർമ്മശക്തിയും സംയോജിപ്പിച്ച്, അനധികൃത പ്രവേശനം തടയുന്നതിന് സുരക്ഷയും സൗകര്യവും സന്തുലിതമാക്കുന്നു.

- 2FA (റ്റു-ഫാക്ടർ ഓഥന്റിക്കേഷൻ) നടപ്പിലാക്കുന്നത് അക്കൗണ്ടിന്റെ സുരക്ഷയെ ഗണ്യമായി വർദ്ധിപ്പിക്കുന്നു. SMS അല്ലെങ്കിൽ ഇമെയിൽ അടിസ്ഥാനമാക്കിയ 2FA-യെ അപേക്ഷിച്ച്, TOTP (ടൈം-ബേസ്ഡ് വൺ-ടൈം പാസ്സ്‌വേർഡ്) അടിസ്ഥാനമാക്കിയ 2FA ഉപയോഗിക്കുന്നത് ഉയർന്ന സുരക്ഷ ഉറപ്പാക്കുന്നതിനാൽ കൂടുതൽ ശുപാർശ ചെയ്യപ്പെടുന്നു. TOTP സാധാരണയായി ഓരോ 30 സെക്കൻഡിലും മാറുന്ന ഒരു പ്രത്യേകമായ കോഡ് നിമ്മിച്ച്, അനധികൃത പ്രവേശനത്തിനെതിരെ അധിക സംരക്ഷണം ഉറപ്പാക്കുന്നു.

- ഗൂഗിൾ ഓഥന്റിക്കേറ്റർ, ഓഥി, അല്ലെങ്കിൽ മൈക്രോസോഫ്റ്റ് ഓഥന്റിക്കേറ്റർ പോലുള്ള ഓഥന്റിക്കേറ്റർ ആപ്പുകൾ TOTP കോഡുകൾ നിർമ്മിക്കുന്നതിനായി, അത്യന്തം സുരക്ഷിതമായ ഒരു മാർഗമാണ്.. ഈ ആപ്പുകൾ നിങ്ങളുടെ അക്കൗണ്ടുകളുമായി ബന്ധപ്പെട്ട, ടൈം-സെൻസിറ്റീവ് കോഡുകൾ നിർമ്മിക്കുന്നു, മാത്രമല്ല SMS അല്ലെങ്കിൽ ഇമെയിൽ പോലുള്ള ആശയവിനിമയ ചാനലുകളെ ആശ്രയിക്കാത്തതിനാൽ, SMS-അടിസ്ഥാനമാക്കിയ 2FA-യെ അപകടപ്പെടുത്താൻ കഴിയുന്ന ഇന്റർസെപ്ഷൻ അല്ലെങ്കിൽ SIM സ്വാപ്പിംഗ് ആക്രമണങ്ങളുടെ സാധ്യത കുറയ്ക്കുന്നു.

- TOTP-അടിസ്ഥാനമാക്കിയ 2FA ഉപയോഗിക്കുന്നതിലൂടെ, നിങ്ങളുടെ അക്കൗണ്ടുകളിലേക്കുള്ള അനധികൃത പ്രവേശനത്തിന്റെ സാധ്യത ഗണ്യമായി കുറയ്ക്കുന്ന ഒരു അധിക സുരക്ഷാ ലെയർ നിങ്ങൾ ചേർത്ത്, വിവിധ സൈബർ ഭീഷണികൾക്കെതിരെ കൂടുതൽ ശക്തമായ സംരക്ഷണം നൽകുന്നു.

- ഫയലുകൾ ഡിലീറ്റ് ചെയ്യുന്നത് നിങ്ങളുടെ സ്വകാര്യതയെ പൂർണ്ണമായി സംരക്ഷിക്കാൻ പര്യാപ്തമല്ല. "ഡിലീറ്റ്" ബട്ടൺ ക്ലിക്ക് ചെയ്യുന്നത് ഫയലുകളെ എന്നെന്നേക്കുമായി ഇല്ലാതാക്കുന്നില്ല; അവ നിങ്ങളുടെ ഉപകരണത്തിൽ മറഞ്ഞിരിക്കുകയും പ്രത്യേക ഉപകരണങ്ങൾ ഉപയോഗിച്ച് കണ്ടെത്താനാകുകയും ചെയ്യും. സ്വകാര്യത ഉറപ്പാക്കാൻ, ഫയലുകൾ "ഷ്രെഡ് (Shred)" ചെയ്യേണ്ടതുണ്ട്. ഇത് കടലാസ് രേഖകൾ ഷ്രെഡ് ചെയ്യുന്നത് പോലെയാണ്. അവ വീണ്ടും ചേർക്കുന്നത് ഏതാണ്ട് അസാധ്യമാണ്. ഷ്രെഡിംഗ് സോഫ്റ്റ്‌വെയർ ഫയലുകളെ ക്രമരഹിതമായ അക്ഷരങ്ങളും അക്കങ്ങളും ഉപയോഗിച്ച് ഓവർറൈറ്റ് ചെയ്ത്, അവയെ വായിക്കാനാകാത്തവിധം കുഴപ്പിക്കും. ഇത് ഷ്രെഡ് ചെയ്ത കടലാസ് വലിച്ചെറിഞ്ഞ് ഭൂമിയിൽ ആഴത്തിൽ കുഴിച്ചിടുന്നത് പോലെയാണ്. ആർക്കും അത് കുഴിച്ചെടുത്ത് നിങ്ങളുടെ രഹസ്യങ്ങൾ വായിക്കാനാകില്ല. അതിനാൽ, സെൻസിറ്റീവ് ഫയലുകൾ നീക്കം ചെയ്യുമ്പോൾ, "ഡിലീറ്റ്" ബട്ടൺ ഒഴിവാക്കി ഷ്രെഡിംഗ് സോഫ്റ്റ്‌വെയർ ഉപയോഗിക്കുക. ഇത് നിന്റെ ഡിജിറ്റൽ ജീവിതത്തെ സ്വകാര്യവും സുരക്ഷിതവുമാക്കാനുള്ള ഏറ്റവും മികച്ച മാർഗമാണ്.

- ടോർ (Tor) ഉപയോഗിച്ച് വെബ്സൈറ്റുകൾ ആക്സസ് ചെയ്യുന്നത് സ്വകാര്യതയും സുരക്ഷയും വർദ്ധിപ്പിക്കും. ഉദാഹരണത്തിന്, ദ ഗാർഡിയൻ പോലുള്ള വാർത്താ സൈറ്റുകളോ X (മുമ്പത്തെ ട്വിറ്റർ) പോലുള്ള സോഷ്യൽ മീഡിയ പ്ലാറ്റ്ഫോമുകളോ ടോർ വഴി സന്ദർശിക്കുന്നത് അധിക അജ്ഞാതത്വം ഉറപ്പാക്കുന്നു.

കാര്യങ്ങൾ മറയ്ക്കുക: ഓൺലൈനിലും ഓഫ്‌ലൈനിലും

ഓൺലൈനിൽ:

- **Crypt.ee**: അജ്ഞാതമായി സൈൻ അപ്പ് ചെയ്യാനുള്ള സൗകര്യവും, എൻഡ്-ടു-എൻഡ് എൻക്രിപ്ഷനും, കൂടാതെ അധിക സ്വകാര്യതയ്ക്കായി ഹിഡൻ ഫോൾഡറുകൾ ഉണ്ടാക്കുന്ന ഓപ്ഷനും നൽകുന്നു.
- **Cryptomator**: ഫയലുകളെ വ്യക്തിഗത സെർവറുകളിൽ എൻക്രിപ്റ്റ് ചെയ്ത് സൂക്ഷിക്കുന്നു, ആപ്പ് അൺഇൻസ്റ്റാൾ ചെയ്തതിന് ശേഷം ഫയൽ ലൊക്കേഷനുകൾ കണ്ടെത്താനാകാത്തവിധം സുരക്ഷിതമാക്കുന്നു.

ഓഫ്‌ലൈൻ:

- **Veracrypt**: ഡ്രൈവുകളിലോ സ്റ്റോറേജ് ഡിവൈസുകളോ ഡേറ്റ സുരക്ഷിതമാക്കുന്നതിനായി ഹിഡൻപാർട്ടീഷനുകൾ നിർമ്മിക്കുന്നു.
- ***രഹസ്യ അറകൾ:*** ഫർണിച്ചറുകളിലോ വസ്തുക്കളിലോ ഉള്ള മറഞ്ഞ അറകളിൽ വിലപിടിപ്പുള്ള സാധനങ്ങൾ ഒളിപ്പിക്കാനുള്ള സൗകര്യം.
- ***സൈഫർ സിസ്റ്റങ്ങൾ:*** എഴുതപ്പെട്ട വിവരങ്ങളോ സ്വത്തുക്കളോ എൻക്രിപ്റ്റ് ചെയ്ത് സുരക്ഷിതമാക്കുന്നതിനായി വ്യക്തിഗത കോഡുകളോ സൈഫറുകളോ നിർമ്മിക്കുന്നു.

ഈ രീതികൾ ഡിജിറ്റൽ, ഫിസിക്കൽ മേഖലകളിൽ സ്വകാര്യതയും സുരക്ഷയും ഉയർത്തി, സെൻസിറ്റീവ് വിവരങ്ങൾ സംരക്ഷിക്കാനുള്ള മാർഗങ്ങൾ പ്രദാനം ചെയ്യുന്നു.

നിങ്ങൾ അപൂർവ്വമായി ഉപയോഗിക്കുന്ന ഫയലുകൾ ഒരു സുരക്ഷിത സ്ഥലത്തിൽ (എൻക്രിപ്റ്റഡ് ഡ്രൈവിലോ ക്ലൗഡിലോ) സൂക്ഷിക്കുകയും നിങ്ങളുടെ ഡിജിറ്റൽ ഡെസ്ക് പതിവായി വൃത്തിയാക്കുകയും ചെയ്യുക, ഇപ്പോൾ ആവശ്യമുള്ളവ മാത്രം നിലനിർത്തുക. പഴയ പതിപ്പുകൾ കോപ്പികൾ ഉണ്ടാക്കുന്നതിനുപകരം ആർക്കൈവ് ചെയ്യുക, ഇത് നിങ്ങളുടെ ഡിജിറ്റൽ ജീവിതത്തെ സംഘടിതവും സുരക്ഷിതവുമാക്കുന്നു.

നിങ്ങളുടെ ഡിജിറ്റൽ ഹിസ്റ്ററി അവശേഷിപ്പിക്കാതെ ഒരു സൈറ്റിൽ ജോയിൻ ചെയ്യാൻ ആഗ്രഹിക്കുന്നുണ്ടോ? ഇനിപ്പറയുന്നവ തിരഞ്ഞെടുക്കുക:

- കുറഞ്ഞ വിവരങ്ങൾ മാത്രം ആവശ്യപ്പെടുന്നവ: ഒരു യൂസർനെയിം, ഒരുപക്ഷേ ഒരു ഇമെയിൽ മാത്രം, ഒരു രഹസ്യ ഹാൻഡ്ഷേക്കിന് സമാനമായി.
- അജ്ഞാതത്വം അനുവദിക്കുന്നവ: പേര് വേണ്ടേ? പ്രശ്നമില്ല! ചില സൈറ്റുകളിൽ നിങ്ങളുടെ ഐഡന്റിറ്റി വെളിപ്പെടുത്താതെ സൈൻ അപ്പ് ചെയ്യാനാകും.
- വ്യാജ ഇമെയിൽ നൽകുന്നവ: സൈൻ അപ്പ് ചെയ്യാൻ ഒരു "ത്രോ-എവേ" ഇമെയിൽ ഉപയോഗിച്ച്, നിങ്ങളുടെ യഥാർത്ഥ ഇമെയിൽ സ്വകാര്യമായി സൂക്ഷിക്കുക.

വാക്കുകളുടെ നിഘണ്ടു:

ഓഡിയോ-വിഡിയോ ഇലക്ട്രോണിക്: എന്നത്, വീഡിയോ കോൺഫറൻസിംഗ്, റെക്കോർഡിങ് ഐഡന്റിഫിക്കേഷൻ പ്രോസസ്സ്, പരിശോധനയും കണ്ടുകെട്ടലും, ഇലക്ട്രോണിക് ആശയവിനിമയം അയയ്ക്കൽ എന്നിവയ്ക്കും, സംസ്ഥാന സർക്കാർ ചട്ടങ്ങൾ പ്രകാരം നിർദ്ദേശിക്കപ്പെട്ട മറ്റ് ആവശ്യങ്ങൾക്കും ഉപയോഗിക്കാവുന്ന ആശയവിനിമയ ഉപകരണങ്ങളെ സൂചിപ്പിക്കുന്നു.

അറസ്റ്റ്: എന്നാൽ, ഒരു വ്യക്തിയെ നിയമപരമായി കസ്റ്റഡിയിൽ എടുക്കുകയും അവരെ തടങ്കലിൽ വയ്ക്കുകയോ നിയന്ത്രിക്കുകയോ ചെയ്യുന്ന പ്രക്രിയയാണ്. അവർക്കെതിരെ കുറ്റം ആരോപിക്കപ്പെട്ടിട്ടില്ലെങ്കിലും, അല്ലെങ്കിൽ ഒരു വാറന്റ് ഇല്ലാതെ പോലും ഒരു വ്യക്തിയെ അറസ്റ്റ് ചെയ്യാം. (കോഗ്നിസബിൾ കുറ്റങ്ങൾ നോക്കുക)

ജാമ്യം ലഭിക്കുന്ന കുറ്റങ്ങൾ: എന്നാൽ, അതിഗൗരവമോ ഗുരുതരമോ അല്ലാത്ത കുറ്റങ്ങളെ സൂചിപ്പിക്കുന്നു, ഇവയിൽ അറസ്റ്റ് ചെയ്യപ്പെട്ടവർക്കോ പ്രതിക്കോ ജാമ്യം ആവശ്യപ്പെടാൻ അവകാശമുണ്ട്.[22] പലപ്പോഴും ജാമ്യ ബോണ്ട് നൽകുക എന്ന വ്യവസ്ഥയോടെ ഇത്തരം കുറ്റങ്ങൾക്ക് അന്വേഷണ ഉദ്യോഗസ്ഥൻ ജാമ്യം നൽകാൻ ബാധ്യസ്ഥനാണ്, എന്നിരുന്നാലും, ജാമ്യം ലഭിച്ചാലും പ്രതി പൂർണമായി മോചിതനായി എന്നല്ല, കാരണം അവർക്ക് ഇപ്പോഴും ജുഡീഷ്യൽ വിചാരണ നേരിടേണ്ടി വരും.

കുറ്റാരോപണം: ഒരു വ്യക്തി കുറ്റകൃത്യം ചെയ്തുവെന്നുള്ള ഔപചാരികമായ ആരോപണമാണ് കുറ്റാരോപണം. ഇത് ഒരു പ്രോസിക്യൂട്ടർ അല്ലെങ്കിൽ പോലീസ്/അന്വേഷണ ഉദ്യോഗസ്ഥരാണ് മുന്നോട്ടുവയ്ക്കുന്നത്.[23] കുറ്റാരോപണത്തിന്റെ അടിസ്ഥാനം വ്യക്തിയെ അറിയിക്കേണ്ടതാണ്.

കോഗ്നിസബിൾ കുറ്റങ്ങൾ: പോലീസ് ഉദ്യോഗസ്ഥന് വാറന്റോ മജിസ്ട്രേട്ടിന്റെ മുൻകൂർ അനുമതിയോ ഇല്ലാതെ അറസ്റ്റ് ചെയ്യാൻ കഴിയുന്ന കുറ്റകൃത്യങ്ങളാണ് കോഗ്നിസബിൾ കുറ്റങ്ങൾ. [24] FIR (ഫസ്റ്റ് ഇൻഫർമേഷൻ റിപ്പോർട്ട്) ഫയൽ ചെയ്താലും ചെയ്യാതിരുന്നാലും ഇത് ബാധകമാണ്, സാധാരണയായി ഇത് ഗൗരവമുള്ള കുറ്റകൃത്യങ്ങളിലാണ് ബാധകമാകുന്നത്.

കമ്പ്യൂട്ടർ: ഇലക്ട്രോണിക്, മാഗ്നറ്റിക്, ഒപ്റ്റിക്കൽ അല്ലെങ്കിൽ മറ്റ് ഉയർന്ന വേഗതയുള്ള ഡേറ്റ പ്രോസസ്സിംഗ് ഉപകരണമോ സിസ്റ്റമോ ആണ് കമ്പ്യൂട്ടർ. ഇത് ഇലക്ട്രോണിക്, മാഗ്നറ്റിക് അല്ലെങ്കിൽ ഒപ്റ്റിക്കൽ ഇംപൾസുകളുടെ കൃത്രിമത്വത്തിലൂടെ ലോജിക്കൽ, അരിത്മറ്റിക്, മെമ്മറി പ്രവർത്തനങ്ങൾ നടത്തുന്നു. കമ്പ്യൂട്ടർ സിസ്റ്റത്തിലോ നെറ്റ്‌വർക്കിലോ ബന്ധപ്പെട്ട എല്ലാ ഇൻപുട്ട്, ഔട്ട്പുട്ട്, പ്രോസസ്സിംഗ്, സ്റ്റോറേജ്, കമ്പ്യൂട്ടർ സോഫ്റ്റ്‌വെയർ അല്ലെങ്കിൽ ആശയവിനിമയ സൗകര്യങ്ങളും ഇതിൽ ഉൾപ്പെടുന്നുണ്ട്.

ആശയവിനിമയ ഉപകരണം: ഇതൊരു സെൽ ഫോൺ, വ്യക്തിപരമായ ഡിജിറ്റൽ സഹായത്തിനുള്ള ഉപകരണം, അല്ലെങ്കിൽ ഇവ രണ്ടിന്റെയും സംയോജനമോ ആകാം. ടെക്സ്റ്റ്, വീഡിയോ, ഓഡിയോ, അല്ലെങ്കിൽ ചിത്രങ്ങൾ ആശയവിനിമയം ചെയ്യാനോ അയയ്ക്കാനോ പ്രക്ഷേപണം ചെയ്യാനോ ഉപയോഗിക്കുന്ന മറ്റേതൊരു ഉപകരണവും ഇതിൽ ഉൾപ്പെടുന്നുണ്ട്.

കുക്കീസ്: വെബ് ബ്രൗസറിൽ നിങ്ങളുടെ പ്രവർത്തനങ്ങളെ ട്രാക്ക് ചെയ്യുകയും രേഖപ്പെടുത്തുകയും ചെയ്യുന്ന ചെറിയ വിവര/ഡേറ്റ ഫയലുകളാണ് കുക്കീസ്. പരസ്യങ്ങൾക്കും വിശകലന സേവനങ്ങൾക്കും ഉപയോക്താവിന്റെ പ്രവർത്തനങ്ങൾ രേഖപ്പെടുത്താൻ ഇവ ഉപയോഗിക്കാം. കുക്കീസിൽ ഉപയോക്താവിന്റെ യൂസർനെയിം, പാസ്‌വേഡ്, കസ്റ്റമൈസേഡ് ക്രമീകരണങ്ങൾ, വെബ് പ്രവർത്തനങ്ങൾ തുടങ്ങിയ വ്യക്തിപരമായ വിവരങ്ങൾ അടങ്ങിയിരിക്കാം. ഇവ സുരക്ഷിതമല്ലെങ്കിൽ, ഉപയോക്താക്കൾക്ക് സുരക്ഷാ, സ്വകാര്യതാ അപകടസാധ്യതകൾ ഉണ്ടാകാം.

വാക്കുകളുടെ നിഘണ്ടു:

ഇലക്ട്രോണിക് ആശയവിനിമയം: ഫോണുകൾ, കമ്പ്യൂട്ടറുകൾ, ഓഡിയോ-വീഡിയോ പ്ലെയറുകൾ, ക്യാമറകൾ, മറ്റ് ഇലക്ട്രോണിക് ഉപകരണങ്ങൾ, അല്ലെങ്കിൽ കേന്ദ്ര സർക്കാർ നിർദ്ദേശിക്കുന്ന മറ്റേതെങ്കിലും ഇലക്ട്രോണിക് രൂപങ്ങൾ ഉപയോഗിച്ച്, വ്യക്തികൾക്കിടയിലോ ഉപകരണങ്ങൾക്കിടയിലോ ഇലക്ട്രോണിക് മാർഗത്തിൽ പങ്കിടുന്ന എഴുതപ്പെട്ട, വാചിക, ചിത്ര, അല്ലെങ്കിൽ വീഡിയോ വിവരങ്ങളെ സൂചിപ്പിക്കുന്നു..

എൻക്രിപ്ഷൻ: വ്യക്തിപരമോ സെൻസിറ്റീവോ ആയ ഡേറ്റ യെ ഒരു രഹസ്യ/കോഡ് രൂപത്തിൽ സംഭരിക്കുന്ന പ്രക്രിയയാണ് എൻക്രിപ്ഷൻ. ഇത് ഡീക്രിപ്ഷൻ കീ ഉള്ള വ്യക്തിക്ക് മാത്രമേ ഡീകോഡ് ചെയ്യാൻ കഴിയൂ. ഇതിലൂടെ വ്യക്തിപരവും, സെൻസിറ്റീവുമായ വിവരങ്ങളുടെ പ്രോസസ്സിംഗ്, സ്റ്റോറേജ്, കൈമാറ്റം എന്നിവ കൂടുതൽ സംരക്ഷിതവുമാകുന്നു, കാരണം അനധികൃത വ്യക്തികൾക്ക് ഡേറ്റ ആക്സസ് ചെയ്യാനോ മനസ്സിലാക്കാനോ കഴിയില്ല.

രേഖ: ഒരു അന്വേഷണത്തിനോ അന്വേഷണവുമായോ ബന്ധപ്പെട്ട വാമൊഴിയോ രേഖാമൂലമോ (എഴുത്തോ ഇലക്ട്രോണിക് രൂപമോ, ഡിജിറ്റൽ ഉപകരണങ്ങൾ ഉൾപ്പെടെ) ആയ ഏതൊരു പ്രസ്താവനയും രേഖയാണ്. ഇത്തരം രേഖകളെ രേഖാതെളിവ് എന്ന് വിളിക്കുന്നു. രേഖ തെളിവിൽ നിന്ന് വ്യത്യസ്തമാണ്, കാരണം അത് നിർണായകമല്ല, മാത്രമല്ല കോടതിയുടെ വിവേചനാധികാരത്തിന് വിധേയവുമാണ്.

ഇന്വെസ്റ്റിഗെറ്റിംഗ് ഓഫീസർ (IO): ഒരു കുറ്റകൃത്യത്തെ അന്വേഷിക്കാൻ ചുമതലപ്പെടുത്തപ്പെട്ട പോലീസ് ഉദ്യോഗസ്ഥനാണ് ഇന്വെസ്റ്റിഗെറ്റിംഗ് ഓഫീസർ (അന്വേഷണ ഉദ്യോഗസ്ഥൻ).

മൂവബിൾ പ്രോപ്പർട്ടി: BNSS പ്രകാരം, ജനാല, വാതിൽ, മരങ്ങൾ തുടങ്ങി എല്ലാത്തരം സ്വത്തുക്കളും മൂവബിൾ പ്രോപ്പർട്ടിയായി കണക്കാക്കപ്പെടുന്നു, പക്ഷേ ഭൂമിയിൽ ഉറപ്പിച്ചതോ ഭൂമിയിൽ ഘടിപ്പിച്ചവയോട് സ്ഥിരമായി ബന്ധിപ്പിച്ചതോ ആയ വസ്തുക്കൾ ഇതിൽ ഉൾപ്പെടുന്നില്ല. ഭൂമിയിൽ ഘടിപ്പിക്കാത്ത എല്ലാ ഇലക്ട്രോണിക്, ഡിജിറ്റൽ ഉപകരണങ്ങളും മൂവബിൾ പ്രോപ്പർട്ടിയിൽ ഉൾപ്പെടും. [25]

ജാമ്യം ലഭിക്കാത്ത കുറ്റകൃത്യങ്ങൾ: കൂടുതൽ ഗുരുതരമോ ഗൗരവമേറിയതോ ആയ കുറ്റകൃത്യങ്ങളാണ് ജാമ്യം ലഭിക്കാത്ത കുറ്റകൃത്യങ്ങൾ. ഇത്തരം കുറ്റങ്ങൾക്ക് കുറ്റാരോപിതനോ അറസ്റ്റ് ചെയ്യപ്പെട്ട വ്യക്തിയോ ജാമ്യം ആവശ്യപ്പെടാനുള്ള അവകാശം ഉണ്ടായിരിക്കില്ല. എന്നിരുന്നാലും, കുറ്റാരോപിതൻ ഒളിവിൽ പോകാനോ നിയമനടപടികളോട് സഹകരിക്കാതിരിക്കാനോ ഉള്ള സാധ്യതകൾ പരിഗണിച്ച്, കോടതിക്ക് അതിന്റെ വിവേചനാധികാരത്തിൽ ജാമ്യം അനുവദിക്കാം.

നോൺ-കോഗ്നിസബിൾ കുറ്റകൃത്യങ്ങൾ: പോലീസ് ഉദ്യോഗസ്ഥന് വാറന്റോ മജിസ്ട്രേട്ടിന്റെ മുൻകൂർ അനുമതിയോ ഇല്ലാതെ അറസ്റ്റ് ചെയ്യാൻ കഴിയാത്ത കുറ്റകൃത്യങ്ങളാണ് നോൺ-കോഗ്നിസബിൾ കുറ്റകൃത്യങ്ങൾ. [26] FIR ഫയൽ ചെയ്ത ശേഷവും വാറന്റ് ലഭിച്ച ശേഷവും മാത്രമേ ഇത് സാധ്യമാകൂ. സാധാരണയായി അത്ര ഗൗരവമില്ലാത്ത കുറ്റകൃത്യങ്ങൾക്കാണ് ഇവ ബാധകമാകുന്നത്..

സ്ഥലം: BNSS പ്രകാരം, ഒരു സ്ഥലം എന്നത് വീട്, കെട്ടിടം, കൂടാരം, വാഹനം, അല്ലെങ്കിൽ പാത്രം എന്നിവ ആകാം.[27]

പൊതു സ്ഥലം: പൊതുഗതാഗതത്തിനുള്ള സ്ഥലങ്ങൾ, ഹോട്ടലുകൾ, കടകൾ, അല്ലെങ്കിൽ പൊതുജനങ്ങൾക്ക് ഉപയോഗിക്കാനോ പ്രവേശിക്കാനോ ഉദ്ദേശിച്ചിട്ടുള്ള മറ്റേതൊരു സ്ഥലവും പൊതു സ്ഥലത്തിൽ ഉൾപ്പെടുന്നു.[28]

വാക്കുകളുടെ നിഘണ്ടു:

കണ്ടുകെട്ടൽ മെമ്മോ: ഒരു കുറ്റാരോപിതനിൽ നിന്ന് അന്വേഷണ ഉദ്യോഗസ്ഥൻ അന്വേഷണ ആവശ്യങ്ങൾക്കായി ഏതെങ്കിലും വസ്തു (മൂല്യവത്തോ മൂല്യമില്ലാത്തതോ) കണ്ടുകെട്ടുകയാണെങ്കിൽ, അത് രജിസ്റ്റർ ചെയ്യുകയും കണ്ടുകെട്ടൽ മെമ്മോയിൽ രേഖപ്പെടുത്തുകയും ചെയ്യുന്നു. ഇതിൽ വസ്തുവിന്റെ വിശദാംശങ്ങൾ/സ്പെസിഫിക്കേഷനുകൾ, സൂക്ഷിച്ച സ്ഥലം, കണ്ടുകെട്ടലുമായി ബന്ധപ്പെട്ട കേസിന്റെ വിശദാംശങ്ങൾ തുടങ്ങിയവ ഉൾപ്പെടുന്നു.

വാറന്റ്: ഒരു ജഡ്ജി ഒപ്പിട്ട ഒരു രേഖയാണ് വാറന്റ്, ഇത് പോലീസിന് നിങ്ങളെ അറസ്റ്റ് ചെയ്യാനോ നിങ്ങളുടെ വസ്തു പരിശോധിക്കാനോ അല്ലെങ്കിൽ അതിൽ നിന്ന് ചിലത് കണ്ടുകെട്ടാനോ അനുമതി നൽകുന്നു. നിങ്ങൾക്ക് വാറന്റ് കാണാനും, അത് സാധുവാണോ എന്ന് പരിശോധിക്കാനും അനുവാദമുണ്ട്.

അനുബന്ധം:

പരിശോധനയും കണ്ടുകെട്ടലും സംബന്ധിച്ച കുറച്ച് കുറിപ്പുകൾ:

1. നിയമവിരുദ്ധവും അനുചിതവുമായ മാർഗങ്ങളിലൂടെ ലഭിച്ച തെളിവുകൾ: മുമ്പ്, കോടതികൾ വിധിച്ചിട്ടുണ്ട്, നിയമവിരുദ്ധമോ അനുചിതമോ ആയ മാർഗങ്ങളിലൂടെ ലഭിച്ച തെളിവുകൾ സ്വീകരിക്കപ്പെടാവുന്നതാണ്. എന്നിരുന്നാലും, അത്തരം തെളിവുകൾ യഥാർത്ഥവും കൃത്രിമം ചെയ്യപ്പെടാത്തതുമാണെന്ന് തെളിയിക്കപ്പെടണം. തെളിവിന്റെ സ്വീകാര്യത കോടതികൾക്ക് മാത്രമേ നിർണ്ണയിക്കാൻ കഴിയൂ, അത് ഓരോ കേസിന്റെയും വസ്തുതകളെയും സാഹചര്യങ്ങളെയും ആശ്രയിച്ചിരിക്കും. [ഉമേഷ് കുമാർ വി. സ്റ്റേറ്റ് ഓഫ് എ.പി., (2013) 10 എസ്.സി.സി. 169]

2. എന്നിരുന്നാലും, കേരള ഹൈക്കോടതിയുടെ തീരുമാന പ്രകാരം, സിആർപിസിയിലെ (ഇപ്പോൾ ബിഎൻഎസ്എസ്) നിയമപരമായ നടപടിക്രമങ്ങൾ കൃത്യമായി പാലിക്കാതെ ഒരു പോലീസ് ഉദ്യോഗസ്ഥന് ഒരു പത്രപ്രവർത്തകന്റെ മൊബൈൽ ഫോൺ കണ്ടുകെട്ടാൻ അനുവാദമില്ല. ഏതെങ്കിലും കുറ്റകൃത്യത്തിന്റെ അന്വേഷണത്തിന് ഈ ഉപകരണം അനിവാര്യമാണെങ്കിൽ പോലും, പോലീസ് ഉദ്യോഗസ്ഥർ നിയമങ്ങൾക്കനുസൃതമായി മാത്രമേ അത് പരിശോധിക്കാനും കണ്ടുകെട്ടാനും ചെയ്യാവൂ. **[29]**

3. ഡൽഹി ഹൈക്കോടതിയുടെ വിധി പ്രകാരം, ഭരണഘടനയുടെ ആർട്ടിക്കിൾ 20(3) പ്രകാരം സ്വയം കുറ്റാരോപണത്തിൽ നിന്നുള്ള സംരക്ഷണം കണക്കിലെടുത്ത്, ഒരു വ്യക്തിയെ പാസ്‌വേഡോ മറ്റു വിശദാംശങ്ങളോ നൽകാൻ നിർബന്ധിക്കാൻ കഴിയില്ല എന്നാണ്.**[30]**

4. അതുപോലെ, ഡൽഹിയിലെ റൗസ് അവന്യൂ ജില്ലാ കോടതിയിലെ പ്രത്യേക സിബിഐ കോടതി വിധി പ്രകാരം, ഭരണഘടനയുടെ ആർട്ടിക്കിൾ 20(3) ഉം ബിഎൻഎസ്എസ്ന്റെ സെക്ഷൻ 180(2) ഉം നൽകുന്ന സംരക്ഷണത്തിന്റെ അടിസ്ഥാനത്തിൽ, പ്രതിയെ അത്തരം വിശദാംശങ്ങൾ വെളിപ്പെടുത്താൻ ബലമായി നിർബന്ധിക്കാനാവില്ല. **[31]**

5. പരിശോധനയും കണ്ടുകെട്ടലും സംബന്ധിച്ച നടപടിക്രമങ്ങൾ മനസ്സിലാക്കുന്നത്, ഇത്തരം തീവ്രമായ സാഹചര്യങ്ങളിൽ പരിഭ്രാന്തി ഒഴിവാക്കാൻ സഹായിക്കുക മാത്രമല്ല, അധികാരികളുമായി മെച്ചപ്പെട്ട രീതിയിൽ സഹകരിക്കാനും സഹായിക്കും. കൂടാതെ, ഇത്തരം നടപടിക്രമങ്ങൾ അറിയുന്നത് നിയമപാലകരിൽ നിന്നുള്ള തെറ്റായ പെരുമാറ്റത്തിൽ നിന്ന് വ്യക്തികളെ സംരക്ഷിക്കും.

ഇലക്ട്രോണിക് ഉപകരണങ്ങളും നിയമവും

ഇലക്ട്രോണിക് ഉപകരണങ്ങളും നിയമവും സംബന്ധിച്ച വിഷയത്തിൽ ജുഡീഷ്യൽ നിലപാട് ഇപ്പോഴും വ്യക്തമായിട്ടില്ല. എന്നിരുന്നാലും, ബിഎൻഎസ്എസ്, ബിഎസ്എ, യുഎപിഎ, ഇൻകം ടാക്സ് ആക്ട്, പിഎംഎൽഎ, ഐടി ആക്ട് എന്നിവയിൽ പരിശോധന നടത്തലും കണ്ടുകെട്ടലും സംബന്ധിച്ച പൊതുവായ മാർഗനിർദേശങ്ങൾ നിലവിലുണ്ട്. ഈ നിയമങ്ങളിലെ പരിശോധന കണ്ടുകെട്ടൽ നടപടിക്രമങ്ങൾ വ്യത്യസ്തമാണെന്ന് ശ്രദ്ധിക്കേണ്ടതാണ്.

അനുബന്ധം:

ഭാരതീയ നാഗരിക് സുരക്ഷാ സംഹിത വാറന്റിനോടെ	**വകുപ്പ് 96-** ഈ വ്യവസ്ഥയനുസരിച്ച്, ഒരു പോലീസ് ഉദ്യോഗസ്ഥൻ കോടതിയിൽ നിന്ന് പ്രത്യേക അനുമതി നേടേണ്ടതുണ്ട്. പരിശോധന നടത്താൻ തക്കതായ കാരണങ്ങളുണ്ടെന്ന് കോടതിക്ക് ബോധ്യമാകുന്ന പക്ഷം, പരിശോധ വാറണ്ട് നൽകുന്നതിനുള്ള വ്യവസ്ഥകൾ കോടതി വ്യക്തമാക്കും. പരിശോധന/കണ്ടുകെട്ടൽ നടത്തുന്ന ഉദ്യോഗസ്ഥൻ, വാറണ്ട് നൽകപ്പെട്ട പ്രത്യേക മേഖലയിൽ മാത്രം പ്രവർത്തനം പരിമിതപ്പെടുത്തണം. **വകുപ്പ് 103:** വസ്തു പരിശോധന നടത്തുന്നതിനും കണ്ടുകെട്ടുന്നതിനുമുള്ള അടിസ്ഥാന വ്യവസ്ഥയാണിത്. പോലീസ് ഉദ്യോഗസ്ഥർ വസ്തു പരിശോധികല്ലോ കണ്ടുകെട്ടലോ നടത്തുമ്പോൾ ഈ നിയമങ്ങൾ പാലിക്കേണ്ടതാണ്.
ഭാരതീയ നാഗരിക് സുരക്ഷാ സംഹിത വാറന്റില്ലാതെ	**വകുപ്പ് 185:** പോലീസിന്, ഒരു കുറ്റകൃത്യം ഉടൻ സംഭവിക്കാനിടയുണ്ടെന്ന് തോന്നുകയോ അ ന്വേഷണത്തിന് നിർണായകമാണെന്ന് കരുതുകയോ ചെയ്യുന്ന സാഹചര്യത്തിൽ, പ്രത്യേക അനുമതി (വാറണ്ട്) ഇല്ലാതെ ഒരു സ്ഥലത്ത് പ്രവേശിച്ച് പരിശോധന നടത്താം. കൂടാതെ, ഈ വ്യവസ്ഥ ഇപ്പോൾ പരിശോധന നടത്തുന്ന പോലീസ് ഉദ്യോഗസ്ഥൻ ആ പ്രക്രിയ രേഖപ്പെടുത്തണമെന്ന് നിർദ്ദേശിക്കുന്നു. പരിശോധന നടത്താൻ കഴിയാത്ത സാഹചര്യത്തിൽ, ഉദ്യോഗസ്ഥൻ കാരണങ്ങൾ രേഖാമൂലം രേഖപ്പെടുത്തിയ ശേഷം തന്റെ കീഴുദ്യോഗസ്ഥനെ ആ ജോലി ഏൽപ്പിക്കാം. പരിശോധനയുടെ രേഖകളുടെ പകർപ്പുകൾ നാൽപ്പത് മണിക്കൂറിനുള്ളിൽ അടുത്തുള്ള മജിസ്ട്രേട്ടിന് കൈമാറണം. **അന്വേഷണ സമയത്തെ പ്രസ്താവനകൾ: വകുപ്പ് 180, 181 എന്നിവയിലെ വ്യവസ്ഥകൾ** പ്രകാരം, ഒരു വ്യക്തി അന്വേഷണ സമയത്ത് നൽകുന്ന പ്രസ്താവനകൾ സത്യവാങ്മൂലമായി സാക്ഷ്യപ്പെടുത്തേണ്ടതില്ല. കൂടാതെ, ഇന്ത്യൻ ഭരണഘടന പ്രകാരം, തങ്ങളെ കുറ്റവാളിയാക്കാൻ സാധ്യതയുള്ള കാര്യങ്ങൾ പറയാതിരിക്കാനുള്ള അവകാശവും വ്യക്തികൾക്കുണ്ട്.[32] **വാറന്റ് ഇല്ലാതെയുള്ള അറസ്റ്റ്: വകുപ്പ് 35** പ്രകാരം, ഒരു വ്യക്തി ഗുരുതരമായ കുറ്റകൃത്യത്തിൽ ഉൾപ്പെട്ടിട്ടുണ്ടെന്ന് പോലീസ് സംശയിക്കുന്നുവെങ്കിലോ, ആ വ്യക്തിക്കെതിരെ പരാതി ലഭിച്ചിട്ടുണ്ടെങ്കിലോ, അല്ലെങ്കിൽ അവർ കുറ്റകൃത്യത്തിൽ ഉൾപ്പെട്ടതായി വിശ്വസിക്കാൻ കാരണമുണ്ടെങ്കിലോ, വാറന്റ് ഇല്ലാതെ അറസ്റ്റ് ചെയ്യാം. എന്നിരുന്നാലും, മൂന്ന് വർഷത്തിൽ താഴെ ശിക്ഷ ലഭിക്കാവുന്ന കുറ്റകൃത്യങ്ങളിൽ, അവശനിലയിലുള്ള വ്യക്തിയെയോ അറുപത് വയസ്സിന് മുകളിലുള്ള വ്യക്തിയെയോ ഡിഎസ്പിയുടെ മുൻകൂർ അനുമതി ഇല്ലാതെ അറസ്റ്റ് ചെയ്യാൻ പാടില്ല.
	സെക്ഷൻ 105-ലെ പുതിയ വ്യവസ്ഥ അനുസരിച്ച്, പോലീസ് ഉദ്യോഗസ്ഥർ തിരച്ചിലും പിടിച്ചെടുക്കലും നടപടികൾ, മുൻഗണനാക്രമത്തിൽ മൊബൈൽ ഫോൺ ഉപയോഗിച്ച്, രേഖപ്പെടുത്തണം. പിടിച്ചെടുത്ത വസ്തുക്കളുടെ ഒരു പട്ടിക സാക്ഷികളുടെ ഒപ്പോടുകൂടി തയ്യാറാക്കണം. ഈ പട്ടിക ഉടനടി ജില്ലാ മജിസ്ട്രേറ്റിനോ അല്ലെങ്കിൽ ഒന്നാം ക്ലാസ് ജുഡീഷ്യൽ മജിസ്ട്രേറ്റിനോ അയച്ചുകൊടുക്കുകയും വേണം. **സെക്ഷൻ 106** അനുസരിച്ച്, മോഷ്ടിക്കപ്പെട്ടതാണെന്ന് സംശയിക്കുന്ന ഏത് വസ്തുവും പോലീസിന് കണ്ടുകെട്ടാം. എന്നാൽ, ചിലപ്പോൾ ഈ വ്യവസ്ഥ ദുരുപയോഗം ചെയ്യപ്പെടുകയും എല്ലാം ഉൾപ്പെടുത്തി പൊതുവായ പരിശോധനയ്ക്ക് ഉപയോഗിക്കാറുണ്ട്. ഏത് പോലീസ് ഉദ്യോഗസ്ഥനും മോഷണവുമായോ കുറ്റകൃത്യവുമായോ ബന്ധപ്പെട്ടതെന്ന് സംശയിക്കുന്ന വസ്തുക്കൾ കണ്ടുകെട്ടാൻ അധികാരമുണ്ട്. കണ്ടുകെട്ടിയ വസ്തുക്കളെക്കുറിച്ച് അടുത്തുള്ള മജിസ്ട്രേറ്റിന് റിപ്പോർട്ട് ചെയ്യണം. കൂടാതെ, പിടിച്ചെടുത്ത വസ്തു കോടതിയിൽ ആവശ്യമുള്ളപ്പോൾ ഹാജരാക്കാമെന്ന ഉറപ്പിൽ ഒരു ബോണ്ടിൽ ഒപ്പുവെച്ചാൽ, ആ വ്യക്തിക്ക് അതിന്റെ സംരക്ഷണാവകാശം ലഭിക്കും.

അനുബന്ധം:

ഭാരതീയ സാക്ഷ്യ അധിനിയം	**Section 168-** The judge has the authority to do the following - • പ്രസക്തമോ അപ്രസക്തമോ ആയ വസ്തുതകളുമായി ബന്ധപ്പെട്ട് ഏത് രീതിയിൽ വേണമെങ്കിലും ചോദ്യങ്ങൾ ചോദിക്കാം. • ഏത് സമയത്തും കക്ഷികളോടോ സാക്ഷികളോടോ ചോദ്യങ്ങൾ ചോദിക്കാം. • തെളിവായി ഏതെങ്കിലും രേഖകളോ വസ്തുക്കളോ ഹാജരാക്കാൻ ആവശ്യപ്പെടാം. പ്രധാനമായി, ഈ വ്യവസ്ഥ പ്രകാരം, ജഡ്ജിയുടെ ആവശ്യങ്ങൾക്കോ നിർദ്ദേശങ്ങൾക്കോ എതിർപ്പ് ഉന്നയിക്കാൻ ആർക്കും അനുവാദമില്ല. [പരിശോധനയും കണ്ടുകെട്ടലും ഉൾപ്പെട്ട കേസുകളിൽ, പ്രത്യേക രേഖകളോ വസ്തുക്കളോ തെളിവായി ഉപയോഗിക്കപ്പെടാവുന്നതിനാൽ ഇത് നിർണായകമാകാം.]
PMLA	**വകുപ്പുകൾ 16, 17:** ഈ വകുപ്പുകൾ പരിശോധനയുടെയും കണ്ടുകെട്ടലിന്റെയും നടപടിക്രമങ്ങൾ വ്യക്തമാക്കുന്നു. പരിശോധനയോ കണ്ടുകെട്ടലോ നടക്കുന്നതിന്റെ കാരണങ്ങൾ എഴുതി രേഖപ്പെടുത്തണമെന്നും, കണ്ടുകെട്ടിയ വസ്തുക്കളുടെ പട്ടിക സഹിതം ഒരു റിപ്പോർട്ട് തയ്യാറാക്കണമെന്നും ഇവ നിർദ്ദേശിക്കുന്നു. [ഇത് പരിശോധന, കണ്ടുകെട്ടൽ പ്രക്രിയയും അതിനാവശ്യമായ രേഖീകരണ ആവശ്യകതകളും തമ്മിലുള്ള ബന്ധം വെളിപ്പെടുത്തുന്നു.]
UAPA	**വകുപ്പ് 43A:** ഈ വകുപ്പ് ഉദ്യോഗസ്ഥർക്ക് കീഴുദ്യോഗസ്ഥർക്ക് പരിശോധന നടത്താൻ അനുമതി നൽകുന്നതാണ്. കൂടാതെ 'വിശ്വാസത്തിന്റെ അടിസ്ഥാനം' സ്വന്തം അറിവിന്റെ അടിസ്ഥാനത്തിലോ മൂന്നാമതൊരാൾ നൽകിയ എഴുത്തുമൂലമുള്ള വിവരത്തിന്റെ അടിസ്ഥാനത്തിലോ ആയിരിക്കണമെന്ന് നിർദ്ദേശിക്കുന്നു. **വകുപ്പ് 43B:** പരിശോധനയ്ക്കോ കണ്ടുകെട്ടലിനോ വിധേയനാകുന്ന വ്യക്തിയുടെ അവകാശങ്ങൾ വിശദീകരിക്കുന്നു. ഈ വകുപ്പുകൾ ഉറപ്പാക്കുന്നത്, പരിശോധനയോ അല്ലത് കണ്ടുകെട്ടൽ സമയത്തോ, പരിശോധിക്കപ്പെടുന്ന വ്യക്തിയോട് പരിശോധിനയുടെ കാരണങ്ങൾ അറിയിക്കണമെന്നും, കണ്ടുകെട്ടിയ വസ്തുക്കൾ അടുത്തുള്ള പോലീസ് സ്റ്റേഷനിലേക്ക് കൊണ്ടുവരണമെന്നുമാണ്. അവിടെയുള്ള ഉത്തരവാദപ്പെട്ട ഉദ്യോഗസ്ഥൻ CrPC (ഇപ്പോൾ BNSS) ൽ വ്യക്തമാക്കിയ നിയമങ്ങൾക്കനുസൃതമായി ആവശ്യമായ നടപടികൾ കൈക്കൊള്ളണം.
വരുമാന നികുതി നിയമം	**വകുപ്പ് 132:** ഈ വകുപ്പ്, നിയമപ്രകാരം ആവശ്യപ്പെട്ട രേഖകളോ വസ്തുക്കളോ ആരെങ്കിലും നൽകാത്തപക്ഷം അവ കണ്ടുകെട്ടാൻ അധികാരികൾക്ക് അനുമതി നൽകുന്നു. പരിശോധനയുടെയും കണ്ടുകെട്ടലിന്റെയും പശ്ചാത്തലത്തിൽ, അന്വേഷണത്തിലോ നിയമനടപടികളിലോ സ്വമേധയാ രേഖകളോ വസ്തുക്കളോ ഹാജരാക്കാത്ത സാഹചര്യത്തിൽ അവ പിടിച്ചെടുക്കാൻ അധികാരികൾക്ക് നിയമപരമായ പിന്തുണ ഇവ ഉറപ്പാക്കുന്നു. കൂടാതെ, പ്രതികൾക്ക് ന്യായമായ അവസരം നൽകണമെന്നും ഈ വകുപ്പ് നിർദ്ദേശിക്കുന്നു, അതായത്, കണ്ടുകെട്ടിയ വസ്തുക്കളെക്കുറിച്ചുള്ള അവരുടെ വിശദീകരണത്തെ പിന്തുണയ്ക്കുന്ന തെളിവുകൾ നൽകാൻ പ്രതിക്ക് അവസരം ലഭിക്കേണ്ടതാണ്.
ഐടി നിയമം	**വകുപ്പ് 80:** ഈ വകുപ്പനുസരിച്ച്, അധികൃത ഉദ്യോഗസ്ഥർക്ക് [33] ഏതൊരു പൊതുസ്ഥലത്തും പരിശോധന നടത്താനും, അവിടെ കണ്ടെത്തുന്ന ഒരു വ്യക്തിയെ, ഐടി നിയമപ്രകാരം കുറ്റകൃത്യം കുറ്റകൃത്യം മുൻകാലത്തോ വർത്തമാനത്തോ ഭാവിയിലോ ചെയ്തതായോ ചെയ്യാൻ സാധ്യതയുണ്ടെന്നോ ന്യായമായി സംശയിക്കപ്പെടുന്നുവെങ്കിൽ, വാറന്റ് ഇല്ലാതെ അറസ്റ്റ് ചെയ്യാനും അനുമതി നൽകുന്നു.

അനുബന്ധം:

THE SCHEDULE

[*See* section 63(*4*)(*c*)]

CERTIFICATE

PART A

(To be filled by the Party)

I, ____________________ (Name), Son/daughter/spouse of __________________ residing/employed at _________________________ do hereby solemnly affirm and sincerely state and submit as follows:—

I have produced electronic record/output of the digital record taken from the following device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: ____

Make & Model: ______________ Color: ______________
Serial Number: ______________
IMEI/UIN/UID/MAC/Cloud ID____________________ (as applicable)
and any other relevant information, if any, about the device/digital record____(specify).

The digital device or the digital record source was under the lawful control for regularly creating, storing or processing information for the purposes of carrying out regular activities and during this period, the computer or the communication device was working properly and the relevant information was regularly fed into the computer during the ordinary course of business. If the computer/digital device at any point of time was not working properly or out of operation, then it has not affected the electronic/digital record or its accuracy. The digital device or the source of the digital record is:—

Owned ☐ Maintained ☐ Managed ☐ Operated ☐

by me (select as applicable).

I state that the HASH value/s of the electronic/digital record/s is ________________, obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other_________________ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name and signature)

Date (DD/MM/YYYY): _____

Time (IST): ________hours (In 24 hours format)

Place: ____________

ചിത്രം 1:
സർട്ടിഫിക്കറ്റ്

അനുബന്ധം:

PART B

(To be filled by the Expert)

I, ____________________ (Name), Son/daughter/spouse of _____________________ residing/employed at _________________________ do hereby solemnly affirm and sincerely state and submit as follows:—

The produced electronic record/output of the digital record are obtained from the following device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: ____

Make & Model: _______________ Color: _______________
Serial Number: _______________
IMEI/UIN/UID/MAC/Cloud ID_____________________ (as applicable)
and any other relevant information, if any, about the device/digital record_______(specify).

I state that the HASH value/s of the electronic/digital record/s is _____________________, obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other__________________ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name, designation and signature)

Date(DD/MM/YYYY): _____

Time (IST): ________hours (In 24 hours format)

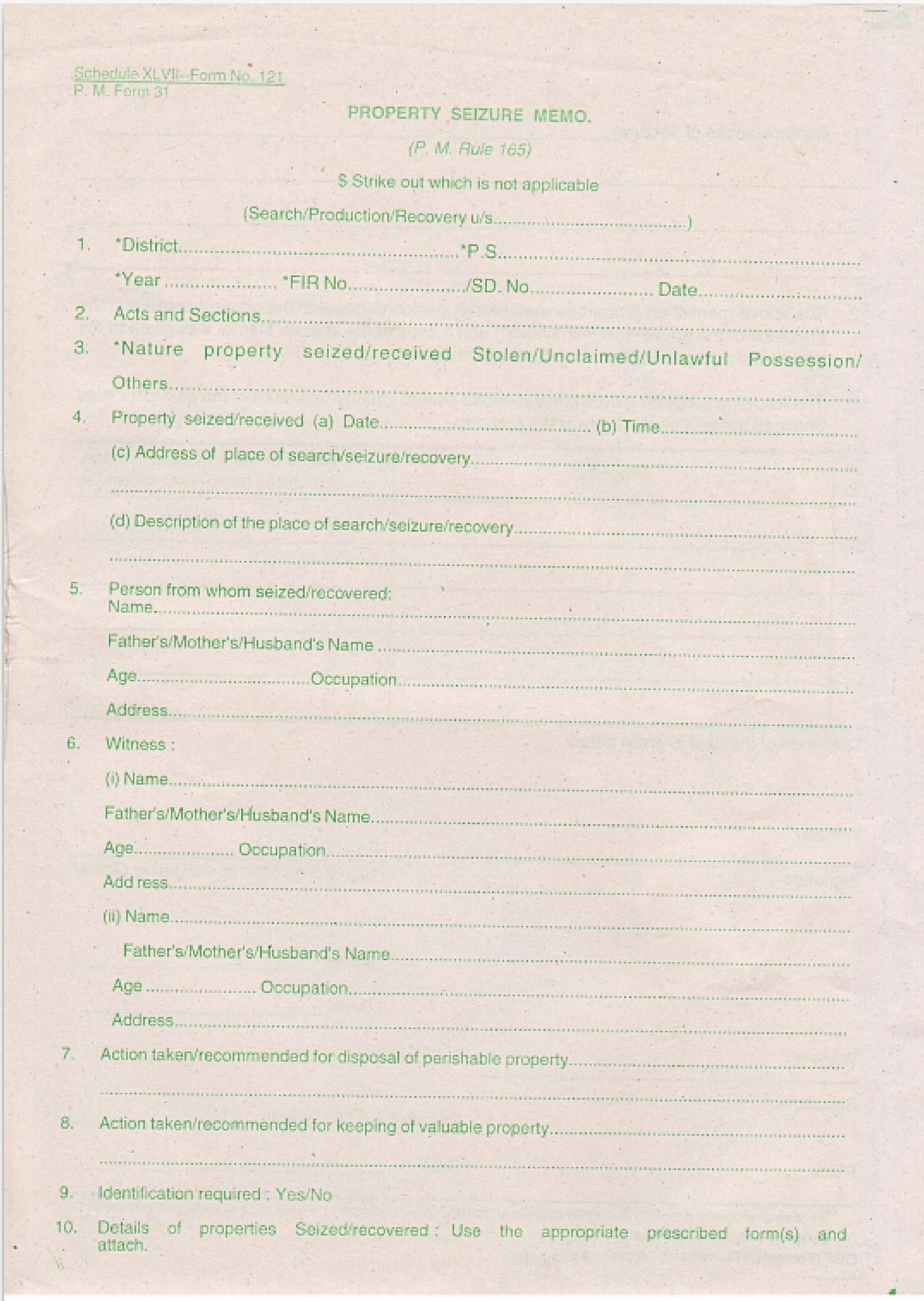
Place: ____________

____

DIWAKAR SINGH,
Joint Secretary & Legislative Counsel to the Govt. of India.

ചിത്രം 2:
സർട്ടിഫിക്കറ്റ് (വിദഗ്ധൻ സമർപ്പിക്കേണ്ടത്)

അനുബന്ധം:



Schedule XLVII--Form No. 121
P. M. Form 31

PROPERTY SEIZURE MEMO.

(P. M. Rule 165)

$ Strike out which is not applicable

(Search/Production/Recovery u/s.......................................)

1. *District...*P.S...

   *Year .... *FIR No....................../SD. No...................... Date..............................

2. Acts and Sections...

3. *Nature property seized/received Stolen/Unclaimed/Unlawful Possession/ Others...

4. Property seized/received (a) Date.. (b) Time..

   (c) Address of place of search/seizure/recovery..

   ....

   (d) Description of the place of search/seizure/recovery..

   ....

5. Person from whom seized/recovered:
   Name...

   Father's/Mother's/Husband's Name ....

   Age..................................Occupation..

   Address..

6. Witness :

   (i) Name..

   Father's/Mother's/Husband's Name...

   Age.................... Occupation...

   Add ress...

   (ii) Name...

   Father's/Mother's/Husband's Name...

   Age .... Occupation..

   Address..

7. Action taken/recommended for disposal of perishable property..

   ....

8. Action taken/recommended for keeping of valuable property..

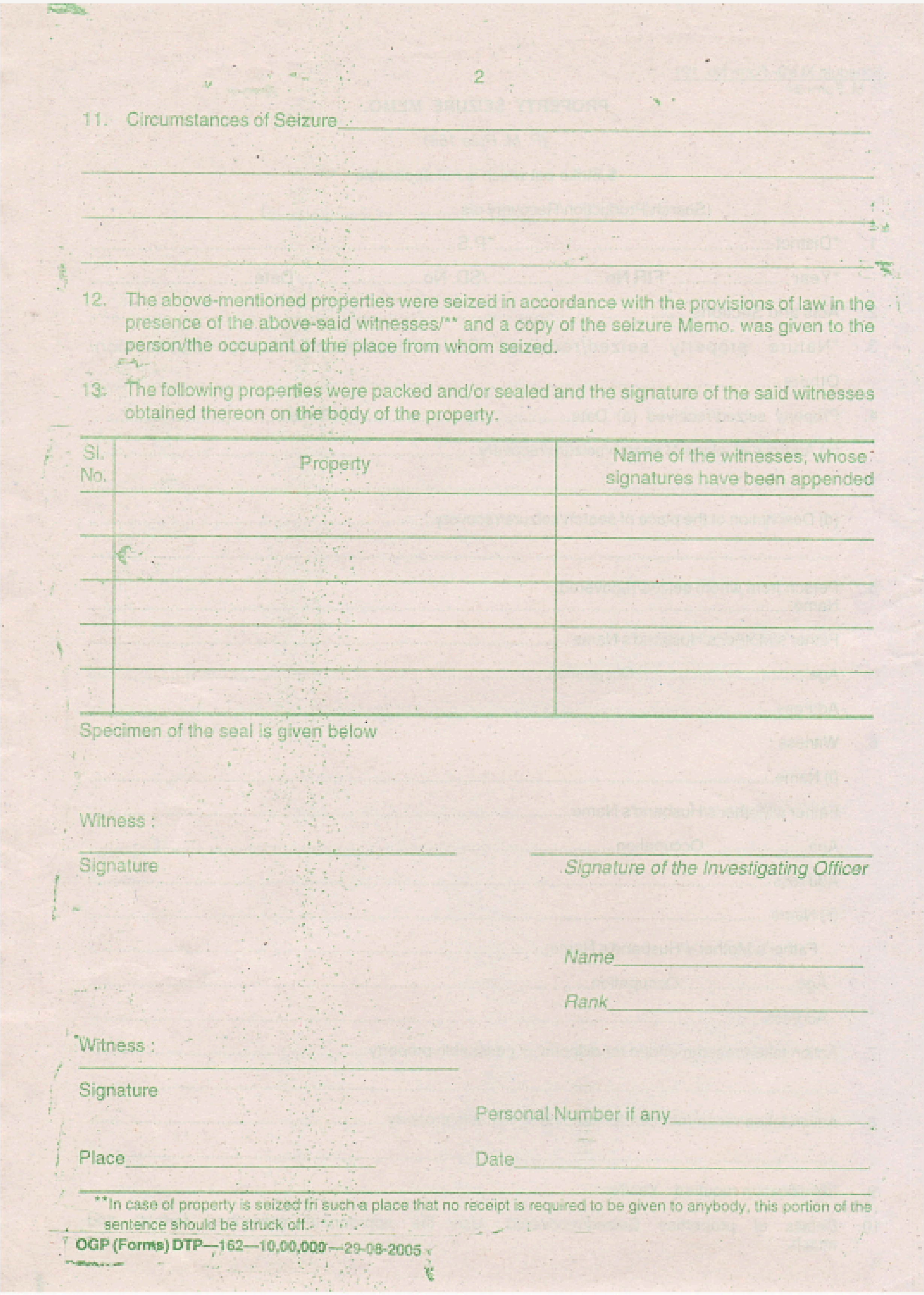
   ....

9. Identification required : Yes/No

10. Details of properties Seized/recovered : Use the appropriate prescribed form(s) and attach.

ചിത്രം *3:*
ഉപകരണങ്ങൾ പിടിച്ചെടുക്കൽ മെമ്മോ

അനുബന്ധം:



2

11. Circumstances of Seizure ____________________

____

____

____

12. The above-mentioned properties were seized in accordance with the provisions of law in the presence of the above-said witnesses/** and a copy of the seizure Memo. was given to the person/the occupant of the place from whom seized.

13. The following properties were packed and/or sealed and the signature of the said witnesses obtained thereon on the body of the property.

Sl. No.	Property	Name of the witnesses, whose signatures have been appended

Specimen of the seal is given below

Witness : ____________________

Signature

Signature of the Investigating Officer

Name ____________________

Rank ____________________

Witness : ____________________

Signature

Personal Number if any ____________________

Place ____________________ Date ____________________

**In case of property is seized in such a place that no receipt is required to be given to anybody, this portion of the sentence should be struck off.

OGP (Forms) DTP—162—10,00,000—29-08-2005

ചിത്രം *3.1:*

ഉപകരണങ്ങൾ പിടിച്ചെടുക്കൽ മെമ്മോ

അനുബന്ധം:

SEIZURE LIST

Case Reference :

1. Date and Hours of Seizure :

2. Place of Seizure / Person from whom seized :

3. Name and Address of Witnesses :
   (i) (ii)

4. Description of articles seized :
   (Appropriate PF and / or space on reverse may be used)

5. Circumstances of Seizure :

6. Signature of Witnesses & Police Officer

ചിത്രം *4:*
കണ്ടുകെട്ടൽ പട്ടിക

അനുബന്ധം:

FORM No. 3

WARRANT OF ARREST

(*See* section 72)

To .... (*name and designation of the person or persons who is or are to execute the warrant*).

WHEREAS (*name of accused*) of (*address*) stands charged with the offence of .... (*state the offence*), you are hereby directed to arrest the said ...., and to produce him before me. Herein fail not.

Dated, this... day of.. , 20 ....

(*Seal of the Court*) (*Signature*)

(*See* section 73)

This warrant may be endorsed as follows:—

If the said... shall give bail himself in the sum of rupees.. with one surety in the sum of rupees.. (or two sureties each in the sum of rupees..) to attend before me on the.. day of.. and to continue so to attend until otherwise directed by me, he may be released.

Dated, this... day of.. , 20 ....

(*Seal of the Court*) (*Signature*)

ചിത്രം 5:
അറസ്റ്റ് വാറന്റ് ഫോർമാറ്റ് (ബിഎൻഎസ്എസിന്റെ രണ്ടാം പട്ടികയിൽ നൽകിയിരിക്കുന്നത്, അധികൃത വാണിഭ വിജ്ഞാപനത്തിൽ പ്രസിദ്ധീകരിച്ച നിയമത്തിന്റെ *192-*[illegible] പേജിൽ*)*

REFERENCES:

[1] See glossary for the meaning of the word

[2] For explanation of search within the BNSS, see Section 49;97.

[3] Section 44 of the BNSS.

[4] Section 185(1) of the BNSS.

[5] For explanation of seizure within BNSS, see Sec 106, 117.

[6] This is not an exhaustive list of the laws. There are other laws as well which provide for search and seizure.

[7] Code of Criminal Procedure, 1973 (CrPC).

[8] Indian Evidence Act, 1872.

[9] Indian Penal Code, 1860

[10] See Section 42 and 43 of The Telecommunications Act, 2023

[11] Please note that such a recording can be provided to only Judicial Magistrate of the First Class, District Magistrate and Sub-divisional Magistrate.

[12] Sections 94, 185 of BNSS, 2023.

[13] K.S. Puttuswamy v Union of India (2017) 10 SCC 1.

[14] Virender Khanna v. State of Karnataka, Writ Petition No. 11759 of 2020 (GM-RES).

[15] Foundation of Media Professionals v. Union of India, Writ Petition (Crim) No, 395 of 2022, Supreme Court of India, pg 1.

[16] Awstika Das, Committee Constituted To Frame Guidelines For Seizure Of Digital Devices : Centre Tells Supreme Court, (December 6th, 2023 12:05 PM) https://www.livelaw.in/top-stories/supreme-court-seizure-journalists-digital-devices-centre-243831

[17] Certificate has been provided under Section 63(4)(c) of BSA, 2023.

REFERENCES:

[18] A sample of the seizure memo is provided in the Annexure as Figure 3 & Figure 3.1. The source of this sample is https://odishapolice.gov.in/sites/default/files/PDF/PROPERTY-SEIZURE-MEMO.pdf

[19] A sample of such an inventory list (can be identified as the seizure list in Figure 4) is provided in the Annexure below.

[20] A sample of the warrant of the arrest is provided in the Annexure as Figure 5.

[21] BNSS Section 503(2).

[22] See BNSS Section 2(c).

[23] See BNSS Section 2(f), charge is defined under Section 2(b); See also (for better understanding of the contents of a charge) Section. 234.

[24] See BNSS, Section 2(g). See also First Schedule, Point (2) of Explanatory Notes, page 158 of Act published in Gazette notification.

[25] BNS Section 2(21).

[26] See BNSS Section 2(o). See also First Schedule, Point (2) of Explanatory Notes, page 158 of Act published in Gazette notification.

[27] BNSS, Section 2(s).

[28] IT Act, Explanation to section 80(1).

[29] G. Vishakan v. State of Kerala & Ors., WP(C) No. 22328 of 2023 (10.07.2023 - KERHC) : MANU/KE/1872/2023.

[30] Sanket Bhadresh Modi vs CBI, BA No. 3754/23.

[31] CBI vs. Mahesh Kumar Sharma, CBI 31/2021

[32] This right is enshrined within Part III of the Constitution of India, under art. 20(3).

[33] Authorised officers here means either a police officer (not below Inspector) or any other officer of the Central or State Government authorised by the Central Government.

Email: mail@sflc.in

Website: https://www.sflc.in