I/49561/2023

ഭരണഭാഷ-
മാതൃഭാഷ

നം.TRY/2400/2023-T1-ISO

ട്രഷറി ഡയറക്ടറേറ്റ്
തിരുവനന്തപുരം,
തീയതി: 01-08-2023

സർക്കുലർ നം. 09/2023

വിഷയം:- ട്രഷറി വകുപ്പിൽ ISO 27001 നടപ്പിലാക്കുന്നതുമായി ബന്ധപ്പെട്ട് ജീവനക്കാർ പാലിക്കേണ്ട പൊതുനിർദ്ദേശങ്ങൾ-സംബന്ധിച്ച്

സൂചന:- ഇല്ല

ആധുനിക കാലഘട്ടത്തിൽ Information and Communication Technology (ICT)-യിലധിഷ്ഠിതമായ വികസന മുന്നേറ്റങ്ങളാണ് നടന്നുകൊണ്ടിരിക്കുന്നത്. എല്ലാ സ്ഥാപനങ്ങളുടെയും വിവരങ്ങൾ (DATA/Information) ഒരു മൂല്യവത്തായ ആസ്തിയായി മാറിയിരിക്കുന്നു. Business Continuity ഉറപ്പുവരുത്തികൊണ്ടും തന്ത്രപ്രധാനമായ വിവരങ്ങൾ (Sensitive Information) സംരക്ഷിച്ചുകൊണ്ടും സൈബർ ആക്രമണങ്ങൾ, ഡാറ്റാ ലംഘനങ്ങൾ, അനധികൃത ആക്സസ്, പ്രകൃതി ദുരന്തങ്ങൾ, റെഗുലേറ്ററി കംപ്ലയിൻസ് പരാജയങ്ങൾ എന്നിങ്ങനെയുള്ളതായ ഭീഷണികളിൽ നിന്ന് വിവരങ്ങൾ സംരക്ഷിക്കുകയെന്നത് അനിവാര്യവും ശ്രമകരവുമായ ദൗത്യമാണ്. കൂട്ടായ പരിശ്രമം ഇക്കാര്യത്തിൽ ആവശ്യമാണ്. ഇവിടെയാണ് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി മാനേജ്മെന്റ് സിസ്റ്റം (ISMS) പ്രധാന പങ്ക് വഹിക്കുന്നത്. **തന്ത്രപ്രധാനമായ വിവരങ്ങൾ കൈകാര്യം ചെയ്യുന്നതിനും അതിന്റെ രഹസ്യാത്മകത (Confidentiality), സമഗ്രത (Integrity), ലഭ്യത (Availability) എന്നിവ ഉറപ്പാക്കുന്നതിനുമുള്ള ചിട്ടയായ സമീപനമാണ് ISMS.** സംസ്ഥാനത്തിന്റെ സാമ്പത്തിക ഇടപാടുകളുടെ സമഗ്രമായ വിവരങ്ങളും ട്രഷറി സേവിംഗ് ബാങ്ക് ഇടപാടുകാരും ഇതിന്റെ ഭാഗമാണ്. ട്രഷറി വകുപ്പിൽ ഫലപ്രദമായ ഒരു ISMS നടപ്പിലാക്കുന്നത് വഴി വിവരങ്ങൾ സംരക്ഷിക്കാനും മുകളിൽപ്പറഞ്ഞ അപകട സാധ്യതകൾ ഫലപ്രദമായി ലഘൂകരിക്കാനും ബിസിനസ്സ് തുടർച്ച ഉറപ്പാക്കാനും അതിലൂടെ ഇടപാടുകാരുടെ വിശ്വാസം നേടാനും വകുപ്പിനെ പ്രാപ്തമാക്കുന്നു. ഇൻഫർമേഷൻ സെക്യൂരിറ്റി മാനേജ്മെന്റ് സിസ്റ്റങ്ങളിൽ പ്രചുര പ്രചാരത്തിലുള്ള മാനദണ്ഡമായ ISO 27001 സർട്ടിഫിക്കേഷൻ നേടുന്നതിനാണ് വകുപ്പ്

ശ്രമിക്കുന്നത്. വകുപ്പ് നാളിതുവരെ ആർജ്ജിച്ച വൈജ്ഞാനിക ശേഷിയുടെയും തൽഫലമായി കൈവരിച്ച നേട്ടങ്ങളുടെയും പൊതുസ്വീകാര്യതയും അംഗീകാരവുമായി ഇത് മാറും. കാര്യക്ഷമമായ ഒരു ISMS നടപ്പിലാക്കുന്നതിനായി വകുപ്പിലെ എല്ലാ ജീവനക്കാരും ഒത്തൊരുമയോടെ, ആത്മാർഥമായി പരിശ്രമിക്കേണ്ടതാണ്. ഇതിലേക്കായി താഴെ പറയുന്ന നിർദ്ദേശങ്ങൾ കർശനമായി പാലിക്കേണ്ടതാണ്.

1. വകുപ്പിൽ നടപ്പിലാക്കി വരുന്ന ഐ.എസ്.ഒ 27001 മാനദണ്ഡങ്ങളെപ്പറ്റിയും അതിനായി നൽകിയിട്ടുള്ള മാർഗ്ഗ നിർദ്ദേശങ്ങളെക്കുറിച്ചും ഐ.ടി അധിഷ്ഠിതമായി പ്രവർത്തിക്കുന്ന ഒരു വകുപ്പെന്ന നിലയിൽ പാലിക്കേണ്ട വിവര സുരക്ഷാ മാർഗ്ഗങ്ങളെപ്പറ്റിയും വകുപ്പിലെ എല്ലാ ജീവനക്കാരും അവബോധം നേടേണ്ടതാണ്.
2. തങ്ങളുടെ ഓഫീസ് മികച്ച നിലവാരത്തിലുള്ള സേവനം നൽകുന്നുണ്ടെന്നും അവയ്ക്ക് ആധാരമായ സംവിധാനങ്ങൾ തികവുറ്റ സുരക്ഷാ ശൃംഖലയുടെ കീഴിലാണെന്ന് മനസ്സിലാക്കുകയും അക്കാര്യം ഓരോത്തരും ഉറപ്പു വരുത്തേണ്ടതുമാണ്.
3. വകുപ്പിന്റെ ISMS പോളിസികൾ, പ്രോസിഡീയറുകൾ, സർക്കുലറുകൾ തുടങ്ങിയവ Treasury Docs (http://www.docs.treasury.kerala.gov.in)-ൽ ലഭ്യമാക്കിയിട്ടുള്ളതും ഇത് ജീവനക്കാർ ഡൌൺലോഡ് ചെയ്ത് ഉപയോഗിക്കേണ്ടതുമാണ്. ഓഫീസ് മേധാവി ഇത് സംബന്ധിച്ച വിവരം ജീവനക്കാരെ അറിയിക്കേണ്ടതാണ്.
4. പുതിയതായി സർവ്വീസിൽ പ്രവേശിക്കുന്ന ജൂനിയർ അക്കൗണ്ടന്റ് മുതലുള്ളവർ വകുപ്പ് പുറത്തിറക്കിയിട്ടുള്ള ഐ.എസ്.ഒ 27001 പോളിസി ആൻഡ് പ്രോസിഡീയർ വായിച്ചു മനസ്സിലാക്കി സേവന-സുരക്ഷാ വിഷയങ്ങളിൽ അറിവ് നേടേണ്ടതും പ്രസ്തുത വ്യവസ്ഥകൾ പാലിച്ചുകൊണ്ട് സേവനം നിർവ്വഹിക്കേണ്ടതുമാണ്. ഇത് സംബന്ധിച്ച ഒരു Declaration ജീവനക്കാരിൽ നിന്നും വാങ്ങാവുന്നതാണ്. (മാതൃക ഉള്ളടക്കം ചെയ്യുന്നു). ISO Certification- നുമായി ബന്ധപ്പെട്ട പരിശോധന നടത്തുമ്പോൾ ജീവനക്കാർക്ക് ISMS-ൽ മതിയായ അവബോധം നൽകിയിട്ടുണ്ട് എന്നുള്ളതിന് evidence ആയും ഇത് ഉപയോഗിക്കാവുന്നതാണ്.
5. ലാസ്റ്റ് ഗ്രേഡ് ജീവനക്കാർ, പാർട്ട് ടൈം കണ്ടിൻജന്റ് ജീവനക്കാർ, ദിവസ വേതനക്കാർ, താൽക്കാലിക ജീവനക്കാർ എന്നിവർക്കെല്ലാം ഓഫീസ് മേധാവി ഐ.എസ്.ഒ 27001 പോളിസി ആൻഡ് പ്രോസിഡീയർ വിശദീകരിച്ചു നൽകേണ്ടതും ഐ.എസ്.ഒ മാനദണ്ഡങ്ങളെപ്പറ്റി ബോധവാന്മാരാക്കേണ്ടതുമാണ്. ഇത് സംബന്ധിച്ച ഒരു സത്യപ്രസ്താവന ജീവനക്കാരിൽ നിന്നും വാങ്ങാവുന്നതാണ്. (മാതൃക ഉള്ളടക്കം ചെയ്യുന്നു).
6. എല്ലാ ജീവനക്കാരും ഓഫീസ് സമയത്ത് തിരിച്ചറിയൽ കാർഡ് ധരിക്കേണ്ടതാണ്. നിലവിൽ ഐഡി കാർഡ് ലഭിച്ചിട്ടില്ലാത്തവർക്ക് സ്പാർക്കിൽ നിന്നുള്ള ഐഡി കാർഡ് താൽക്കാലികമായി പ്രിന്റെടുത്ത് നൽകേണ്ടതാണ്.
7. സർവ്വീസ് എഞ്ചിനീയർമാർക്ക് അവരുടെ സ്ഥാപനം നൽകിയിട്ടുള്ള തിരിച്ചറിയൽ കാർഡ് ധരിച്ചിട്ടുണ്ടെങ്കിൽ മാത്രം പ്രവേശനം അനുവദിക്കേണ്ടതും സർവ്വീസ് സംബന്ധമായ വിവരങ്ങൾ ലോഗ് ബുക്കിൽ രേഖപ്പെടുത്തേണ്ടതുമാണ്.
8. സസ്പെൻഷനിലാകുന്നവർ/സ്ഥലംമാറി പോകുന്നവർ/വകുപ്പിൽ നിന്നും വിടുതൽ

വാങ്ങിയ ജീവനക്കാർ, ദീർഘകാല അവധി/എൽ.പി.ആർ തുടങ്ങിയ അവധിയിൽ പ്രവേശിച്ചവർ എന്നിവരിൽ നിന്നും ഐ.ഡി കാർഡ് (SPARK-ൽ നിന്നുള്ള താൽക്കാലിക കാർഡുൾപ്പെടെ) മടക്കി വാങ്ങേണ്ടതാണ്.

9. ഒരു ഓഫീസിലെ നിലവിലുള്ള ജീവനക്കാർ അല്ലാത്തവർ പബ്ലിക് ഏരിയക്ക് പുറമേ ഓഫീസിന്റെ മറ്റു സ്ഥലങ്ങളിലേക്ക്/ സെക്ഷനുകളിലേക്ക് പ്രവേശിക്കണമെന്നുണ്ടെങ്കിൽ സന്ദർശന വിവരം സന്ദർശക രജിസ്റ്ററിൽ രേഖപ്പെടുത്തി ഓഫീസ് മേധാവിയുടെ അനുമതിയോടെ മാത്രം പ്രവേശനം അനുവദിക്കാവുന്നതാണ്.
10. ഒരു ഓഫീസ് കെട്ടിടത്തിൽ നടത്തുന്ന പൊതുവായ meeting/ Program എന്നിവയ്ക്ക് ഓഫീസ് മേധാവിയുടെ മുൻകൂർ അനുമതി ആവശ്യമാണ്.
11. കമ്പ്യൂട്ടറിലും അനുബന്ധ ഉപകരണങ്ങളിലും Asset ID രേഖപ്പെടുത്തിയിട്ടുണ്ടെന്നും FMS പോർട്ടലിൽ ഉള്ള എല്ലാ ഉപകരണങ്ങളും ഓഫീസിൽ ഉണ്ടെന്നും ഉറപ്പ് വരുത്തേണ്ടതുമാണ്. FMS പോർട്ടലിൽ ഉള്ള ഉപകരണങ്ങൾ ഓഫീസിൽ ഇല്ലെങ്കിലോ ഓഫീസിൽ ഉള്ള ഉപകരണങ്ങൾക്ക് Asset ID ലഭ്യമായിട്ടില്ലെങ്കിലോ ഡയറക്ടറേറ്റിലെ ISMC സെക്ഷനിൽ റിപ്പോർട്ട് ചെയ്യേണ്ടതാണ്.
12. System login, Treasury application login പാസ്സ്വേർഡുകൾ തുടങ്ങിയവ സൂക്ഷിക്കേണ്ടുന്ന ഉത്തരവാദിത്വം അതാത് ജീവനക്കാരനാണ്. ഒരു ജീവനക്കാരന്റെ PEN നമ്പരിൽ രേഖപ്പെടുന്ന എല്ലാ ഇടപാടുകളുടെയും നിയമപരമായ ഉത്തരവാദി PEN നമ്പരിന്റെ ഉടമസ്ഥൻ ആയതിനാൽ ടി പാസ്സ് വേർഡുകൾ, അതാത് ദിവസം ലഭിക്കുന്ന OTP തുടങ്ങിയവ യാതൊരു കാരണവശാലും മറ്റുജീവനക്കാർക്ക് കൈമാറുകയോ മറ്റുള്ളവർക്ക് ലഭിക്കുന്ന വിധത്തിൽ രേഖപ്പെടുത്തി വയ്ക്കുകയോ ചെയ്യരുത്.
13. വകുപ്പ് നിലവിൽ പൂർണ്ണമായും ഇ-ഗവേർണൻസിൽ അധിഷ്ഠിതമായി പ്രവർത്തിച്ചുകൊണ്ടിരിക്കുന്നതിനാൽ നിയമപരമായ എല്ലാ ഇടപാടുകളും PEN Login അധിഷ്ഠിതവും ആയതിന് ഐ.ടി ആക്ട്-2000 ബാധകവുമാണ്. ആയതിനാൽ തങ്ങളുടെ ജോലിയുടെ ഭാഗമായുള്ള ഡേറ്റയുടെ സുരക്ഷ ഓരോ ജീവനക്കാരും ഉറപ്പു വരുത്തേണ്ടതാണ്.
14. ലൈസൻസ് ഇല്ലാത്ത സോഫ്റ്റവെയറുകൾ സിസ്റ്റത്തിൽ ഉപയോഗിക്കുവാൻ പാടില്ല. ഇവ സിസ്റ്റം അഡ്മിന്റെ സഹായത്തോടെ സിസ്റ്റത്തിൽ നിന്നും നീക്കം ചെയ്യേണ്ടതാണ്.
15. ബ്രൌസറുകളിൽ Password-കൾ ഒരു കാരണവശാലും Auto save ചെയ്ത് വയ്ക്കാൻ പാടുള്ളതല്ല. Auto save ഓപ്ഷൻ സിസ്റ്റം അഡ്മിന്റെ സഹായത്തോടെ നീക്കം ചെയ്യേണ്ടതാണ്.
16. External Hard Disk, Pen drive, CD drive മുതലായ Storage devices ഓഫീസിൽ കൊണ്ടുവരാനോ ഡാറ്റകൾ പകർത്താനോ ഓഫീസ് കമ്പ്യൂട്ടറുകൾ/CCTV ഉപകരണങ്ങൾ എന്നിവയിൽ ഉപയോഗിക്കാനോ പാടുള്ളതല്ല.
17. സ്വകാര്യ വിവരങ്ങൾ ഓഫീസ് കമ്പ്യൂട്ടറുകളിൽ സൂക്ഷിക്കാൻ പാടില്ല.
18. ഓഫീസ് മേധാവിയുടെ അനുമതിയോടുകൂടി മാത്രമേ സ്വകാര്യ Laptop

ഓഫീസിനുള്ളിൽ കൊണ്ടുവരാവൂ. ഇത് ബന്ധപ്പെട്ട രജിസ്റ്ററിൽ രേഖപ്പെടുത്തേണ്ടതുമാണ്.

19. Laptop, External Hard Disk, Pen drive, CD drive മുതലായ Storage devices-മായി സന്ദർശകരെ Public Area ഒഴികെയുള്ള ഇടങ്ങളിൽ പ്രവേശിപ്പിക്കാൻ പാടുള്ളതല്ല. പ്രത്യേക സാഹചര്യങ്ങളിൽ ഓഫീസ് മേധാവിയുടെ മുൻകൂർ അനുമതി ആവശ്യമാണ്.
20. ജീവനക്കാർ തങ്ങളുടെ കമ്പ്യൂട്ടറിന്റെ USB Port-ലെ Media Access Disable ചെയ്തിട്ടുണ്ടെന്ന് ഉറപ്പ് വരുത്തേണ്ടതാണ്. Media Access ആവശ്യമുള്ളവർ Annexure 7 പ്രകാരമുള്ള ഫോം പൂരിപ്പിച്ച് നൽകേണ്ടതും അർഹരായിട്ടുള്ളവർക്ക് മാത്രം ഓഫീസ് മേധാവി ഇത് അനുവദിച്ചു കൊടുക്കേണ്ടതുമാണ്.
21. ജീവനക്കാർ എല്ലാ ദിവസവും തങ്ങളുടെ ഔദ്യോഗിക മെയിൽ (gov.in) ലോഗിൻ ചെയ്ത് Inbox പരിശോധിക്കേണ്ടതും മറുപടി നൽകേണ്ടതുമാണ്. Gmail ഉപയോഗിക്കുവാനോ ഉറവിടം അറിയാത്ത ലിങ്ക് ഓപ്പൺ ചെയ്യാനോ പാടുള്ളതല്ല.
22. Spam mail–കൾ ഓപ്പൺ ചെയ്യരുത്. മെയിൽ വഴി വരുന്ന വകുപ്പ് നല്കിയിട്ടുള്ളതല്ലാത്ത ലിങ്കുകളിലേക്ക് പ്രവേശിക്കാൻ പാടില്ല.
23. എല്ലാ ജീവനക്കാരും Clear Screen പോളിസി കൃത്യമായും പാലിക്കേണ്ടതാണ്. സീറ്റ് വിട്ട് പോകുമ്പോൾ കമ്പ്യൂട്ടർ സ്ക്രീൻ ലോക്ക് (Windows Key+L) ചെയ്തിട്ടുണ്ടെന്ന് ഉറപ്പ് വരുത്തേണ്ടതാണ്.
24. Digital Signature Device ഉപയോഗിക്കുന്നവർ അതിന്റെ പാസ്സ്വേർഡ് സുരക്ഷിതമായും ഉത്തരവാദിത്വത്തോടുകൂടിയും സൂക്ഷിക്കേണ്ടതാണ്.
25. പേപ്പർ അസെറ്റുകൾ Confidential, Restricted, Internal, Public എന്നിങ്ങനെ തരം തിരിച്ചു സൂക്ഷിക്കേണ്ടതാണ്.
26. Whatsapp, facebook ഉൾപ്പെടെയുള്ള സാമൂഹ്യ മാധ്യമങ്ങൾ കൈകാര്യം ചെയ്യുമ്പോൾ ജീവനക്കാർ അതീവ സൂക്ഷ്മത പുലർത്തേണ്ടതാണ്. വകുപ്പിന്റെ പോളിസികൾക്കും സർക്കാർ ഉത്തരവുകൾക്കും അനുസൃതമല്ലാത്ത വിധത്തിലുള്ള വിവരം പങ്കുവയ്ക്കുന്ന തരത്തിൽ സോഷ്യൽ മീഡിയയിൽ പോസ്റ്റുകൾ ഇടാനോ ഷെയർ ചെയ്യാനോ പാടുള്ളതല്ല. ഇത് ഒഫീഷ്യൽ ഗ്രൂപ്പുകൾക്കും ബാധകമാണ്.
27. CCTV Footage ഒരു കാരണവശാലും പുറമേയുള്ള ഏജൻസികൾക്കോ, വ്യക്തികൾക്കോ കൈമാറാൻ പാടുള്ളതല്ല. പോലീസ് ആവശ്യപ്പെടുന്ന പക്ഷം അനുമതിയോടുകൂടി നൽകാവുന്നതാണ്.
28. ഓഫീസ് റെക്കോർഡുകൾ, സീലുകൾ, മറ്റു പ്രധാന രേഖകൾ എന്നിവ അതീവ സുരക്ഷയോടെ കൈകാര്യം ചെയ്യേണ്ടതാണ്. അവയെല്ലാം നിർബന്ധമായും അടച്ചുറപ്പുള്ള സ്ഥലങ്ങളിൽ മാത്രം സൂക്ഷിക്കേണ്ടതാണ്.
29. Clean Desk Policy നിർബന്ധമായും നടപ്പാക്കേണ്ടതാണ്. ഫയലുകൾ, മറ്റു രജിസ്റ്ററുകൾ എന്നിവ മേശപ്പുറത്ത് അലക്ഷ്യമായി വയ്ക്കരുത്. അവ ശരിയായ വിധം കൈകാര്യം ചെയ്യുകയും ആവശ്യത്തിനുശേഷം അലമാരയിൽ സൂക്ഷിക്കുകയും ചെയേണ്ടതാണ്.
30. ഫയലുകൾ സെക്ഷൻ, സീറ്റ് എന്നിങ്ങനെ തരം തിരിച്ച് അലമാരകളിൽ / storage

I/49561/2023

space-ൽ അടുക്കി സൂക്ഷിക്കേണ്ടതാണ്.

31. ഓരോ സെക്ഷനുകളിലേയും സീറ്റുകളിലെ വർക്ക് കൃത്യമായി വിവരിച്ചിട്ടുള്ളതായ ഓഫീസ് ഓർഡർ ഓഫീസിലും ബന്ധപ്പെട്ട സെക്ഷനുകളിലും സൂക്ഷിക്കേണ്ടതാണ്.
32. തങ്ങളുടെ ഓഫീസും പരിസരവും വൃത്തിയായി സൂക്ഷിക്കുവാൻ ഓരോ ജീവനക്കാരും പരിശ്രമിക്കേണ്ടതാണ്.
33. വകുപ്പിന്റെ ISMS പോളിസികൾക്കനുസൃതമായി പ്രവർത്തിക്കുവാൻ എല്ലാ ജീവനക്കാരും ബാധ്യസ്ഥരാണ്.

Signed by V Sajan
Date: 01-08-2023 22:26:14
Reason: Approved

V SAJAN
DIRECTOR

സ്വീകർത്താവ്

എല്ലാ ജീവനക്കാർക്കും

Directorate of Treasuries, Pattom, Pattom Palace. P.O, Thiruvananthapuram, Kerala 695004
Website: www.treasury.kerala.gov.in, Email:treasury@kerala.gov.in
Ph: 0471-2323963,2322712 , FAX:0471-2324229

ISO 27001:2013

Information Security Management System (*ISMS*)

DECLARATION

1) I have received a copy of ISMS policies and procedures of the Department of Treasuries and have kept the same with me for ready reference.
2) I have read and understood the ISMS policies and procedures of the Department of Treasuries and will follow the same.
3) I assure that any breach of the policy will be reported immediately to the head of office / controlling officer by following the procedures outlined in the relevant document.
4) I am aware that I will be responsible for all transactions using my PEN.

Place :

Date :

Signature :

Name :

PEN :

Designation :

Name of Office :

സത്യപ്രസ്താവന

ട്രഷറി വകുപ്പിന്റെ ISO 27001 സർട്ടിഫിക്കേഷനുമായി ബന്ധപ്പെട്ട് ഓഫീസിൽ അനുവർത്തിക്കേണ്ട കാര്യങ്ങളെക്കുറിച്ച് ഓഫീസ് മേധാവിയിൽ നിന്ന് എന്റെ ജോലിയുമായി ബന്ധപ്പെട്ട കാര്യങ്ങൾ മനസ്സിലാക്കിയിട്ടുണ്ട്. ആയതിനനുസരിച്ച് ഞാൻ പ്രവർത്തിക്കുന്നതാണ്.

സ്ഥലം:

തീയതി

ഒപ്പ് :

പേര് :

PEN :

തസ്തിക :

ട്രഷറി / ഓഫീസ്: