ചീഫ് എഞ്ചിനീയറുടെ കാര്യാലയം
ജലസേചനവും ഭരണവും
തിരുവനന്തപുരം
തീയതി : 14-02-2025

CEIA/646/2025-IT

സർക്കുലർ

വിഷയം: - ജലസേചനം - E-Governance സംവിധാനങ്ങളുടെ ഉപയോഗം - ജാഗ്രത പുലർത്തുന്നത് - നിർദ്ദേശങ്ങൾ പുറപ്പെടുവിക്കുന്നു.

ജലസേചന വകുപ്പിലെ ചില ഓഫീസുകളിൽ ഓഫീസ് മേധാവികളുടെ eOffice, PRICE, eTENDER Portal, BIMS, BAMS, SPARK, EMLI തുടങ്ങിയ e-Governance സങ്കേതങ്ങൾ ഉപയോഗിക്കുന്നതിനുള്ള user credentials-ഉം [User ID & Password], ഈ സോഫ്റ്റ്വെയറുകളിൽ അധിക സെക്യൂരിറ്റിക്ക് ഏർപ്പെടുത്തിയിട്ടുള്ള Digital Signer Token [DSC]-ഉം സൗകര്യാർത്ഥം ഓഫീസിലെ കീഴുദ്യോഗസ്ഥരെ ഏല്പിച്ചിരിക്കുന്നതായി ശ്രദ്ധയിൽപ്പെട്ടിട്ടുണ്ട്. ഇത്തരം നടപടികൾ ബോധപൂർവ്വമോ അല്ലാതെയോ ഉള്ള ക്രമക്കേടുകൾക്കും കൃത്യവിലോപത്തിനും ഇടയാക്കുന്നതാണ്. ആയതിനാൽ e-Governance സോഫ്റ്റ്വെയറുകളുടെ Password കൈകാര്യം ചെയ്യുന്നതിനെ സംബന്ധിച്ച നിർദ്ദേശങ്ങൾ ചുവടെ ചേർക്കുന്നു.

1. ഓരോ അക്കൗണ്ടിനും വ്യത്യസ്തവും, സങ്കീർണ്ണവുമായ [unique and complex] പാസ്സ്വേർഡുകൾ തിരഞ്ഞെടുക്കുവാൻ ശ്രദ്ധിക്കുക.
2. Social Engineering മുഖേന എളുപ്പത്തിൽ കണ്ടെത്താനാവുന്ന പാസ്സ്വേർഡുകളോ, പൊതുപദങ്ങളോ, നിഘണ്ടു പദങ്ങളോ (Dictionary words) തിരഞ്ഞെടുക്കാതിരിക്കുക. ഉദാ: പേര്, ജനനത്തീയതി, തസ്തികയുടെ പേര് തുടങ്ങിയവ.
3. പൊതുവായി ഉപയോഗിക്കുന്ന കംപ്യൂട്ടറുകളിൽ Password സേവ് ചെയ്ത് സൂക്ഷിക്കാതിരിക്കുക. ആധുനിക വെബ് ബ്രൗസറുകളിൽ ഇമെയിൽ അനുബന്ധിത പ്രൊഫൈലുകൾ സൃഷ്ടിക്കുന്നതിനാൽ സേവ് ചെയ്യപ്പെടുന്ന Password അതേ email പ്രൊഫൈൽ ഉപയോഗിക്കുന്ന എല്ലാ കമ്പ്യൂട്ടറുകളിലും ലഭ്യമാകും (sync ചെയ്യപ്പെടും).
4. പാസ്വേഡുകൾ പ്രദർശിപ്പിക്കാനോ, പ്രിന്റ് ചെയ്യാനോ, പങ്കിടാനോ പാടില്ല.
5. Password ക്രൃത്യമായ ഇടവേളകളിൽ (60 ദിവസത്തിൽ ഒരിക്കലെങ്കിലും) നിർബന്ധമായും മാറ്റുക.
6. ഒരിക്കൽ ഉപയോഗിച്ച പാസ്വേഡ് വീണ്ടും ഉപയോഗിക്കുന്നത് പരമാവധി ഒഴിവാക്കുക.

7. കമ്പ്യൂട്ടർ സങ്കേതങ്ങൾ ഓരോ യൂസറെയും തിരിച്ചറിയുന്നത് പാസ്വേഡ് മുഖേനയാണ്. ആയതിനാൽ തന്നെ Password സഹപ്രവർത്തകരുമായോ മറ്റു വ്യക്തികളുമായോ പങ്കുവയ്ക്കാതിരിക്കുക. തങ്ങളുടെ അക്കൗണ്ട് ഉപയോഗിച്ച് മറ്റുള്ളവരെക്കൊണ്ട് പ്രവർത്തി ചെയ്യാൻ അനുവദിക്കാതിരിക്കുക. A password represents a shared secret and the primary means of authentication between the end user and the system. The system cannot differentiate the real user from an impersonator who also knows the password. Thus, it is essential that users keep their password private.
8. ഏതെങ്കിലും പ്രത്യേക സാഹചര്യത്തിൽ സ്വന്തം അക്കൗണ്ട് ഉപയോഗിച്ച് ഏതെങ്കിലും സവിശേഷ task ചെയ്യുന്നതിനായി മറ്റൊരാളെ അനുവദിക്കേണ്ടി വന്നാൽ പ്രസ്തുത പ്രവർത്തി അവസാനിച്ച ഉടൻ തന്നെ Password മാറ്റേണ്ടതാണ്.
9. തങ്ങളുടെ അക്കൗണ്ട് ഉപയോഗിച്ച് അനുവാദത്തോടെയോ അല്ലാതെയോ മറ്റുള്ളവർ ചെയ്യുന്ന പ്രവൃത്തിയുടെയും ഉത്തരവാദിത്വം അക്കൗണ്ട് ഉടമസ്ഥന് തന്നെ ആയിരിക്കും. Users are accountable for all actions carried out using user IDs allotted to them. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users. The Officer holding the account shall be held responsible for all activities performed by others with or without consent using the account.
10. പാസ്സ്വേഡിനു പുറമെ അധിക സുരക്ഷിതത്വത്തിനായാണ് DSC Signing ഏർപ്പെടുത്തിയിരിക്കുന്നത്. ആയതിനാൽ തന്നെ DSC Token അതീവ ഗൗരവത്തോടെയും ഉത്തരവാദിത്വത്തോടെയും കൈകാര്യം ചെയ്യേണ്ടതാണ്.

മുകളിൽ പ്രതിപാദിച്ചിരിക്കുന്ന നിർദ്ദേശങ്ങൾ ഗൗരവപൂർവ്വം പാലിക്കേണ്ടതാണ്. ഇതിൽ വീഴ്ച വരുത്തുന്നതുമൂലം സംഭവിക്കുന്ന ക്രമക്കേടുകൾക്ക് ബന്ധപ്പെട്ട account holder വ്യക്തിപരമായി ഉത്തരവാദി ആയിരിക്കുന്നതാണ്.

ചീഫ് എഞ്ചിനീയർ
Signed by Sivadasan M
Date: 17-02-2025 05:30:50

പകർപ്പ്:- എല്ലാ ജീവനക്കാർക്കും വകുപ്പ് വെബ്സൈറ്റ് മുഖേന