കേരള സ്റ്റേറ്റ് സിവിൽ സപ്ലൈസ് കോർപ്പറേഷൻ

SUPPLYCO

ഇൻഫർമേഷൻ ടെക്നോളജി
ഉപയോഗ നയങ്ങളും മാർഗ്ഗനിർദ്ദേശങ്ങളും
പതിപ്പ് 1.0

ഡിസംബർ 2020

കുറിപ്പ്

സാമൂഹ്യ ജീവിതത്തിന്റെ സമസ്ത മേഖലകളിലും വിവര സാങ്കേതിക വിദ്യയുടെ ഉപയോഗം അതിവേഗം വ്യാപിച്ചുകൊണ്ടിരിക്കുകയാണ്. ആധുനിക സമൂഹത്തിൽ ഇവയുടെ ഉപയോഗം അനിവാര്യമാണ്. വിവര സാങ്കേതിക വിദ്യയുടെ അജ്ഞത അല്ലെങ്കിൽ ദുരുപയോഗം അനാവശ്യമായ അപകടസാധ്യതകൾക്കും ബാധ്യതകൾക്കും കാരണമാകും. ദി കേരളാ സ്റ്റേറ്റ് സിവിൽ സപ്ലൈസ് കോർപ്പറേഷൻ ലിമിറ്റഡ് (സപ്ലൈകോ) വിവര സാങ്കേതിക വിദ്യകൾ ഉപയോഗിക്കുന്നവർക്കുള്ള ഉപയോഗ മാർഗ്ഗനിർദ്ദേശങ്ങളും, സ്വകാര്യതയും ഈ നയരേഖയിലൂടെ ആലേഖനം ചെയ്യുന്നു. സാധാരണക്കാർക്ക് മനസ്സിലാക്കാൻ പറ്റുന്ന വിധത്തിലാണ് നയങ്ങൾ വ്യക്തമാക്കിയിരിക്കുന്നത്. ആയതിനാൽ നയങ്ങളുടെ ചുരുക്ക രൂപമാണ് മലയാളം പതിപ്പിൽ അടങ്ങിയിട്ടുള്ളത്. സമ്പൂർണ രൂപത്തിനായി ഈ നയരേഖയുടെ ഇംഗ്ലീഷ് പതിപ്പ് കാണുകയോ അല്ലെങ്കിൽ സപ്ലൈകോ ഹെഡ് ഓഫീസിലെ എംഐഎസ് ഡിവിഷനുമായി ബന്ധപ്പെടുകയോ ചെയ്യുക.

ഒപ്പ്

മാനേജർ (എം.ഐ.എസ്.)

വിഷയങ്ങൾ

1. ആമുഖം 4
2. ഐടി ഉപയോഗ നയത്തിന്റെ ഉദ്ദേശ്യം 5
3. പ്രയോഗികതലം 6
4. നിർവചനങ്ങൾ 7
4.1. ഇൻഫർമേഷൻ വർഗ്ഗീകരണം 7
4.2. ഐടി റിസോഴ്സുകൾ (വിവര സാങ്കേതിക ഉറവിടങ്ങൾ) 8
4.3. ഉപയോക്താവ് 9
4.4. സിസ്റ്റംസ് അതോറിറ്റി 9
4.5. ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ (ISO) 9
4.6. നെറ്റ്വർക്ക് / സിസ്റ്റം അഡ്മിനിസ്ട്രേറ്റർ 9
4.7. സിസ്റ്റം സപ്പോർട്ട് ഓഫീസർമാർ (SSO) 10
4.8. നെറ്റ്വർക്ക് ഓപ്പറേഷൻസ് സെന്ററർ (NOC) 10
4.9. ഹെൽപ്പ് ഡെസ്ക് 10
5. വിവര സാങ്കേതിക വിദ്യയുടെ (ഐടി) ഉപയോഗ നയം 10
5.1. ഇൻഫർമേഷൻ ടെക്നൊളജിയുടെ പൊതുവായ ഉപയോഗ നയം 11
5.1.1. പാസ്വേഡ് നയം 11
5.1.2. സുരക്ഷ / ഉപയോഗ നിയന്ത്രണം 12
5.1.3. നെറ്റ്വർക്ക് /സിസ്റ്റങ്ങളിൽ വരുത്തുന്ന മാറ്റങ്ങൾ 13
5.2. സോഫ്റ്റ്വെയർ ലൈസൻസിംഗ് പോളിസി 13
5.3. ഇൻറർനെറ്റ്, ഇൻട്രാനെറ്റ് ഉപയോഗ നയം 14
5.4. ഇ-മെയിൽ ഉപയോഗ നയം 16
5.5. ലാപ്ടോപ്പ് പോളിസി 17
5.5.1. ലാപ്ടോപ്പ് ഉപയോഗ പൊതുനിയമങ്ങൾ 18
6. ഡാറ്റാ ബാക്കപ്പ് പോളിസി 19
7. ലംഘനങ്ങൾ 21

1. ആമുഖം

കംപ്യൂട്ടർ അടിസ്ഥാനമാക്കിയുള്ള ഇൻഫർമേഷൻ സിസ്റ്റംസിന്റെ പഠനം, രൂപകല്പന, നിർമ്മാണം, അതിന്റെ നടപ്പിലാക്കൽ, നിയന്ത്രണം എന്നിവക്കു പൊതുവെ പറയുന്ന പേരാണ് **ഇൻഫർമേഷൻ ടെക്നൊളജി (ഐടി) അഥവാ വിവര സാങ്കേതിക വിദ്യ**.

ഇൻഫർമേഷൻ റിസോഴ്സ്സ് അഥവാ വിവര ഉറവിടങ്ങൾ എന്നത് ഡാറ്റ, ഡെസ്ക്ടോപ്പ് ഉപകരണങ്ങൾ, പോർട്ടബിൾ, മൊബൈൽ ഉപകരണങ്ങൾ, വയർലെസ് നെറ്റ്വർക്കുകൾ, ഇന്റർനെറ്റ് കണക്റ്റിവിറ്റി, ബാഹ്യ സംഭരണ ഉപകരണങ്ങൾ (External Storage Devices), പ്രിന്ററുകൾ, സ്കാനറുകൾ എന്നിവ പോലുള്ള അനുബന്ധ ഉപകരണങ്ങളും അതുമായി ബന്ധപ്പെട്ട സോഫ്റ്റ്വെയറും ഉൾപ്പെടുന്നു.

ജീവനക്കാരുടെ കാര്യക്ഷമതയും ഉൽപാദനക്ഷമതയും വർദ്ധിപ്പിക്കുന്നതിന് വേണ്ടി ഐടി റിസോഴ്സുകൾ നൽകുന്നു. ഇവ ജീവനക്കാരുടെ ജോലി മേഖലകളുമായി ബന്ധപ്പെട്ട വിവരങ്ങൾ കൈകാര്യം ചെയ്യുന്നതിനുള്ള ഉപകരണങ്ങളാണ്. ഉദ്യോഗസ്ഥർക്ക് അവരുടെ പ്രവർത്തനങ്ങൾ കാര്യക്ഷമമായും ഫലപ്രദമായും നടപ്പാക്കാൻ ഐടി റിസോഴ്സുകൾ സഹായിക്കുന്നു.

ഐടി റിസോഴ്സുകൾ ദുരുപയോഗം ചെയ്യുന്നത് അനാവശ്യമായ അപകടസാധ്യതകൾക്കും ബാധ്യതകൾക്കും കാരണമാകും. അതിനാൽ, ഇവ ജോലിയുമായി ബന്ധപ്പെട്ട ആവശ്യങ്ങൾക്ക് വേണ്ടി നിയമപരവും ധാർമ്മികവുമായ രീതിയിൽ ഉപയോഗിക്കണമെന്നത് ഓരോ ജീവനക്കാരന്റെയും ഉത്തരവാദിത്തമാണ്.

ഐടി റിസോഴ്സുകളിലേക്ക് ശരിയായ പ്രവേശനവും ഉപയോഗവും ഉറപ്പുവരുത്തുകയും ഉപയോക്താക്കൾ അവ ദുരുപയോഗം ചെയ്യുന്നത് തടയുകയുമാണ് ഈ നയത്തിന്റെ ലക്ഷ്യം. അനുചിതമായ ഉപയോഗം വൈറസ് ആക്രമണങ്ങൾ, രഹസ്യാത്മക ഡാറ്റ നഷ്ടപ്പെടുന്നത്, നെറ്റ്വർക്ക് സിസ്റ്റങ്ങളുടെയും സേവനങ്ങളുടെയും വിട്ടുവീഴ്ച, നിയമപരമായ പ്രശ്നങ്ങൾ എന്നിങ്ങനെയുള്ള അപകടസാധ്യതകളിലേക്ക് സപ്ലൈകോയെ നയിക്കുന്നു.

ഇൻഫർമേഷന്റെ സുരക്ഷ എല്ലാവരുടെയും ഉത്തരവാദിത്തമാണ്. സപ്ലൈകോയുടെ ഇൻഫർമേഷൻ സിസ്റ്റങ്ങളുമായി ഇടപെടുന്ന ഓരോ ജീവനക്കാരന്റെയും

പങ്കാളിത്തം, പിന്തുണ എന്നിവ സപ്ലൈകോ ആവശ്യപ്പെടുന്നു. സപ്ലൈകോയുടെ ഇൻഫർമേഷൻ സിസ്റ്റങ്ങൾ ഉപയോഗിക്കുന്നതിന് മുൻപ് എല്ലാ ജീവനക്കാരും ഈ ഉപയോഗ നയം പാലിക്കേണ്ടതുണ്ട്.

2. ഐടി ഉപയോഗ നയത്തിന്റെ ഉദ്ദേശ്യം

സപ്ലൈകോയിലെ എല്ലാ ജീവനക്കാർക്കും ഇൻഫർമേഷൻ ടെക്നൊളജി റിസോഴ്സുകളുടെ ഉപയോഗക്ഷമതയും ലഭ്യതയും ഉറപ്പുവരുത്തുന്നതിനായി ഇൻഫർമേഷന്റെയും ഇൻഫർമേഷൻ ടെക്നൊളജി റിസോഴ്സുകളുടെയും സംരക്ഷണമാണ് ഈ നയത്തിന്റെ പ്രാഥമിക ഉദ്ദേശ്യം. സപ്ലൈകോയുടെ ഇൻഫർമേഷൻ ടെക്നൊളജി റിസോഴ്സുകൾ ഉപയോഗിക്കുന്നവർക്കുള്ള ഉപയോഗ മാർഗ്ഗനിർദ്ദേശങ്ങളും, സ്വകാര്യതയും നയം വ്യക്തമാക്കുന്നു.

സപ്ലൈകോയുടെ സിസ്റ്റങ്ങളിൽ ഏതെല്ലാം പ്രവർത്തനങ്ങൾ അനുവദനീയമാണെന്നും അസ്വീകാര്യമായത് എന്താണെന്നും വ്യക്തമായി നിർവചിക്കേണ്ടതിന്റെ ആവശ്യകതയുണ്ട്. സപ്ലൈകോ ഇൻഫർമേഷൻ സിസ്റ്റവുമായി ബന്ധപ്പെട്ടിരിക്കുന്ന ഉദ്യോഗസ്ഥർക്ക് (സ്റ്റാഫ്, ഉപഭോക്താക്കൾ, കരാറുകാർ, മറ്റുള്ളവർ) അവരുടെ സുരക്ഷാ ഉത്തരവാദിത്തങ്ങളെക്കുറിച്ച് ബോധവാന്മാരാണെന്നും അപകടസാധ്യതകൾ ലഘൂകരിക്കുന്നതിന് ഉചിതമായ നിയന്ത്രണങ്ങൾ നിലവിലുണ്ടെന്നും ഉറപ്പാക്കുകയാണ് ഈ നയത്തിന്റെ ലക്ഷ്യം.

കമ്പനി ബിസിനസിനെ സ്വാധീനിക്കുന്നതിൽ ഇൻഫർമേഷൻ ടെക്നൊളജി വഹിക്കുന്ന പ്രധാന പങ്കും ഇൻഫർമേഷൻ സംരക്ഷിക്കുന്നതിന്റെ പ്രാധാന്യവും സപ്ലൈകോ മനസ്സിലാക്കുന്നു. സപ്ലൈകോയുടെ അംഗീകൃത ജീവനക്കാർ ഇൻഫർമേഷൻ ടെക്നൊളജി റിസോഴ്സുകളിൽ നിന്നുമുള്ള ഇൻഫർമേഷനുകൾ ഡിജിറ്റൽ രൂപത്തിൽ ഉപയോഗിക്കുകയും പങ്കിടുകയും ചെയ്യുന്നതിനാൽ, ഇൻഫർമേഷനും അതിനെ പിന്തുണയ്ക്കുന്ന ടെക്നൊളജി റിസോഴ്സുകളും സംരക്ഷിക്കേണ്ടതിന്റെ ആവശ്യകത സപ്ലൈകോയ്ക്ക് ഉണ്ട്.

ഡാറ്റ, കമ്പ്യൂട്ടറുകൾ, പ്രിന്ററുകൾ, ഇ-മെയിൽ, ഇൻറർനെറ്റ് ഉപയോഗം എന്നിവയുടെ പരിമിതമായ അളവിലുള്ള ഉപയോഗം സപ്ലൈകോ അനുവദിക്കുന്നതിനാൽ, ഈ സൗകര്യങ്ങൾ ജീവനക്കാർ ഉത്തരവാദിത്തത്തോടെ ഉപയോഗിക്കേണ്ടത് അത്യാവശ്യമാണ്. ഏതെങ്കിലും തരത്തിലുള്ള ദുരുപയോഗം കമ്പനി ബിസിനസിനെ തടസ്സപ്പെടുത്താനും മറ്റ് ജീവനക്കാരുടെ ജോലിയെ ബാധിക്കാനും സാധ്യതയുണ്ട്.

ഇൻഫർമേഷൻ ടെക്നൊളജിയുടെ അനുചിതമായ ഉപയോഗം സപ്ലൈകോയെ കുഴപ്പങ്ങളിലേക്കും വിവാദങ്ങളിലേക്കും നയിച്ചേക്കാം. അതിനാൽ സപ്ലൈകോയുടെ ഇൻഫർമേഷൻ ടെക്നോളജി സൗകര്യങ്ങൾ ഉപയോഗിക്കുമ്പോൾ എല്ലാ ജീവനക്കാരും ധാർമ്മികബോധത്തോടെയും ഉത്തരവാദിത്തത്തോടെയും പെരുമാറേണ്ടതാണ്.

ഇനിപ്പറയുന്ന ലക്ഷ്യങ്ങൾ പ്രോത്സാഹിപ്പിക്കുകയാണ് ഈ നയം ലക്ഷ്യമിടുന്നത്:

- ഐടി സിസ്റ്റങ്ങളുടെ വിശ്വാസ്യത, ലഭ്യത, മികച്ച പ്രകടനം എന്നിവ ഉറപ്പാക്കുക.
- ഐടി ആപ്ലിക്കേഷനുകളുടെയും സിസ്റ്റങ്ങളുടെയും സംരക്ഷണത്തിന്റെ ആവശ്യകതയെ കുറിച്ച് ബോധവൽക്കരണം നൽകുക.
- വ്യക്തികളുടെ ഉത്തരവാദിത്തങ്ങൾ ബോധ്യപ്പെടുത്തുക.
- ദുരുപയോഗം, ഡാറ്റ നഷ്ടപ്പെടൽ അല്ലെങ്കിൽ അനധികൃത വെളിപ്പെടുത്തൽ എന്നിവയ്ക്ക് സ്വീകരിക്കേണ്ട നടപടികൾ ബോധ്യപ്പെടുത്തുക.
- പരിശീലനം പ്രോത്സാഹിപ്പിക്കുകയും എല്ലാ ജീവനക്കാർക്കും ഇൻഫർമേഷന്റെ സുരക്ഷയെക്കുറിച്ചുള്ള അവബോധം വർദ്ധിപ്പിക്കുകയും ചെയ്യുക.
- ഉദ്ദേശിച്ച ആവശ്യങ്ങൾക്കായി മാത്രം ഐടി സിസ്റ്റങ്ങൾ ഉപയോഗിക്കുന്നുവെന്ന് ഉറപ്പാക്കുക.

3. പ്രയോഗികതലം

ഈ നയം സപ്ലൈകോയുടെ ഇൻഫർമേഷൻ സിസ്റ്റം / റിസോഴ്സസ് ഉപയോഗിക്കുന്ന എല്ലാവർക്കും ബാധകമാണ്. ഈ നയം എല്ലാ ഉപയോക്താക്കളും വ്യക്തമായി മനസ്സിലാക്കുകയും പിന്തുടരുകയും ചെയ്യുന്നുവെന്ന് ഉറപ്പാക്കേണ്ടത് എല്ലാ ഔട്ട്ലെറ്റ് / ഡിപ്പോ / റീജിയണൽ മാനേജർമാരുടെയും ഹെഡ് ഓഫീസിലെ എംഐഎസ് ഡിവിഷൻ / നെറ്റ്വർക്ക് അഡ്മിനിസ്ട്രേറ്ററുടെയും ഉത്തരവാദിത്തമാണ്.

സപ്ലൈകോയുടെ ഇൻഫർമേഷൻ ടെക്നോളജി റിസോഴ്സുകളുമായി സമ്പർക്കം പുലർത്തുന്ന എല്ലാ സാധാരണ ജീവനക്കാർക്കും കരാർ ജീവനക്കാർക്കും ദൈനംദിന വേതന സ്റ്റാഫുകൾക്കും സപ്ലൈകോയ്ക്ക് സേവനങ്ങൾ നൽകുന്ന വെണ്ടർമാർ /വിതരണക്കാർക്കും ഈ നയം ബാധകമാണ്.

ഈ നയങ്ങൾ ബാധകമായിട്ടുള്ള ഇൻഫർമേഷൻ ടെക്നൊളജി റിസോഴ്സുകൾ താഴെ പറയുന്നു:

- പേഴ്സണൽ കമ്പ്യൂട്ടറുകൾ (പിസി), ലാപ്ടോപ്പ്, വർക്ക്സ്റ്റേഷനുകൾ, ടാബ്ലറ്റുകൾ, വയർലെസ് കമ്പ്യൂട്ടിംഗ് ഉപകരണങ്ങൾ, നെറ്റ്വർക്കുകൾ, ഡാറ്റാബേസുകൾ, പ്രിന്ററുകൾ, സെർവറുകൾ, സുരക്ഷാ സംവിധാനങ്ങൾ, തുടങ്ങിയവ കണക്റ്റുചെയ്തിരിക്കുന്ന എല്ലാ നെറ്റ്വർക്കുകളും ഹാർഡ്വെയറും ഉൾപ്പെടെ കമ്പ്യൂട്ടറുമായി ബന്ധപ്പെട്ട എല്ലാ ഉപകരണങ്ങളും.
- സപ്ലൈകോ സ്വയം വികസിപ്പിച്ചെടുത്ത, വാങ്ങിയ അല്ലെങ്കിൽ ലൈസൻസുള്ള ബിസിനസ്സ് സോഫ്റ്റ്വെയർ ആപ്ലിക്കേഷനുകൾ, സപ്ലൈകോയുടെ വെബ്സൈറ്റ് /പോർട്ടൽ, കമ്പ്യൂട്ടർ ഓപ്പറേറ്റിംഗ് സിസ്റ്റങ്ങൾ, സപ്ലൈകോയുടെ ഉടമസ്ഥതയിലുള്ള ഉപകരണങ്ങളിലുള്ള ഫേംവെയർ, മറ്റേതെങ്കിലും സോഫ്റ്റ്വെയർ എന്നിവയുൾപ്പെടെ എല്ലാ സോഫ്റ്റ്വെയറുകളും.
- സപ്ലൈകോയുടെ ഇൻഫർമേഷൻ ടെക്നോളജി ഉപകരണങ്ങളിൽ സൂക്ഷിക്കുന്ന ഡാറ്റ.

4. നിർവചനങ്ങൾ

ഈ നയത്തിൽ, ഇനിപ്പറയുന്ന വാക്കുകൾക്ക് ഇനിപ്പറയുന്ന അർത്ഥങ്ങൾ നൽകുന്നു.

4.1. ഇൻഫർമേഷൻ വർഗ്ഗീകരണം

ഓർഗനൈസേഷനിൽ ബാധകമായ ഇൻഫർമേഷനുകളെ ഇനിപ്പറയുന്ന വിഭാഗങ്ങളായി തരം തിരിക്കാം:

- **പ്രധാന രഹസ്യം:**

  പ്രധാന രഹസ്യം എന്നത് ഓർഗനൈസേഷന്റെ ഏറ്റവും അടുത്ത രഹസ്യങ്ങളായും മാത്രമല്ല ചില സാഹചര്യങ്ങളിൽ മാത്രം ഉപയോഗിക്കാനുള്ളതുമാണ്. ഈ ഇൻഫർമേഷനുകളുടെ ദുരുപയോഗം / വെളിപ്പെടുത്തൽ സപ്ലൈകോയുടെ പ്രവർത്തനത്തെ ഗുരുതരമായി ബാധിക്കും. ഉദാ. വെയർഹൗസിലെ ചരക്കിന്റെ ഡാറ്റ ലഭ്യത, സുരക്ഷിതമായ സിസ്റ്റങ്ങളിലേക്കുള്ള പാസ്വേഡുകൾ, അതീവ രഹസ്യാത്മക രേഖകൾ തുടങ്ങിയവ.

- **രഹസ്യം:**

ഈ ഇൻഫർമേഷനുകളുടെ അനധികൃത വെളിപ്പെടുത്തൽ ഓർഗനൈസേഷന് നാശനഷ്ടമുണ്ടാക്കും. ഉദാ. ഔട്ട്ലെറ്റുകളുടെ സ്റ്റോക്ക് വിവരം, വെണ്ടർ സംഭരണ വില വിശദാംശങ്ങൾ, ഡാറ്റാ സെന്ററുകളിലെ സെർവറുകളുടെ കോൺഫിഗറേഷൻ വിശദാംശങ്ങൾ പോലുള്ള നിർണായക ഇൻഫ്രാസ്ട്രക്ചറുമായി ബന്ധപ്പെട്ട ഇൻഫർമേഷനുകൾ.

- **സ്വകാര്യമായവ**

  ഒരു കൂട്ടം വ്യക്തികൾക്ക് മാത്രം ലഭ്യമാവുന്ന വിവരങ്ങൾ. ഉദാ. ബോർഡ്/എക്സിക്യൂട്ടീവ്/മിനിസ്റ്റർ ലെവൽ മാനേജ്മെന്റ് എന്നിവയിലെ മാറ്റങ്ങൾ, സാമ്പത്തിക വിശദാംശങ്ങൾ, തന്ത്രപരമായ തീരുമാനങ്ങൾ തുടങ്ങിയവ.

- **പരിമിതപ്പെടുത്തിയവ:**

  ഇത് ഔദ്യോഗിക ഉപയോഗത്തിന് മാത്രമുള്ളതാണ് ഉദാ. എച്ച്ആർ ഡാറ്റ, സുരക്ഷാ നയങ്ങൾ, ഔദ്യോഗിക സർക്കുലറുകൾ തുടങ്ങിയവ.

- **തരംതിരിക്കാത്തവ / പൊതുവായവ:**

  ഇൻഫർമേഷനുകൾ ഇൻറർനെറ്റിൽ / വിവിധ മാധ്യമങ്ങളിൽ / നോട്ടീസ് ബോർഡ് തുടങ്ങിയവയിൽ ലഭ്യമാണ് അല്ലെങ്കിൽ പൊതു ഉപയോഗത്തിനായി നൽകിയവയാണ്. ഉദാ. ഓർഗനൈസേഷൻ വെബ്സൈറ്റുകളിൽ പ്രസിദ്ധീകരിച്ച ഇൻഫർമേഷനുകൾ.

4.2. ഐടി റിസോഴ്സുകൾ (വിവര സാങ്കേതിക ഉറവിടങ്ങൾ)

ഇൻഫർമേഷൻ ടെക്നോളജി റിസോഴ്സുകളിൽ സപ്ലൈകോയുടെ ഉടമസ്ഥതയിലുള്ളതോ കരാർ അടിസ്ഥാനത്തിൽ ഉപയോഗത്തിലുള്ളതോ ആയ ഉപകരണങ്ങൾ ഉൾപ്പെടുന്നു. കമ്പ്യൂട്ടറുകൾ, സെർവറുകൾ, ഓർഗനൈസേഷൻ നൽകിയ ലാപ്ടോപ്പുകൾ, ടാബ്ലെറ്റുകൾ, മൊബൈലുകൾ, ഡോംഗിൾസ്, ഓർഗനൈസേഷണൽ റിസോഴ്സുകളുമായി ബന്ധിപ്പിച്ചിരിക്കുന്ന വ്യക്തിഗത ഉടമസ്ഥതയിലുള്ള ഉപകരണങ്ങൾ, പ്രിന്ററുകൾ, സ്കാനറുകൾ, സുരക്ഷാ ഉപകരണങ്ങൾ, നെറ്റ്വർക്ക് ഉപകരണങ്ങൾ, മോഡം, ഫാക്സ് മെഷീനുകൾ ഓൺലൈൻ, ഓഫ്ലൈൻ സംഭരണം, മീഡിയ, അനുബന്ധ ഉപകരണങ്ങൾ, സപ്ലൈകോയുടെ വെബ്സൈറ്റ് / പോർട്ടൽ, സോഫ്റ്റ്വെയർ, വിവിധ സ്റ്റോറേജുകൾ, ഡാറ്റ ഫയലുകൾ, വീഡിയോ കോൺഫറൻസിംഗ് റൂമുകൾ, വീഡിയോ കോൺഫറൻസിംഗ് വിവരങ്ങൾ, ഇൻറർനെറ്റ്, നെറ്റ്വർക്ക്

മാനേജ്മെന്റ്/ മോണിറ്ററിംഗ് ഉപകരണങ്ങൾ, ഡാറ്റാബേസ് എന്നിവ ഉൾപ്പെടുന്നു.

4.3. ഉപയോക്താവ്

ജീവനക്കാർ, താൽക്കാലിക ജീവനക്കാർ, പ്രൊബേഷണർമാർ, കരാറുകാർ, വെണ്ടർമാർ, വിതരണക്കാർ, എന്നിവരുൾപ്പെടെ ഏത് സ്ഥലത്ത് നിന്നും സപ്ലൈകോയുടെ ഇൻഫർമേഷൻ ടെക്നൊളജി റിസോഴ്സുകൾ (ഹാർഡ്വെയർ, സോഫ്റ്റ്വെയർ, നെറ്റ്വർക്കിംഗ്, ഡാറ്റ ഫയലുകൾ മുതലായവ) ഉപയോഗിക്കുന്നവർ.

4.4. സിസ്റ്റംസ് അതോറിറ്റി

സപ്ലൈകോയിലെ എംഐഎസ് ഡിവിഷനാണ് എല്ലാ ഐടി റിസോഴ്സുകളുടെയും നിയമപരമായ ഉടമ / ഓപ്പറേറ്റർ.

4.5. ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ (ISO)

എംഐഎസ് മാനേജരെയാണ് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസറായി ചുമതലപ്പെടുത്തിയിരിക്കുന്നത്. ഓർഗനൈസേഷനുള്ള ഐടി ഉപയോഗ നയങ്ങളും മാർഗ്ഗനിർദ്ദേശങ്ങളും രൂപകല്പന ചെയ്യൽ, നടപ്പിലാക്കൽ, മെച്ചപ്പെടുത്തൽ, നിരീക്ഷിക്കൽ എന്നിവയുടെ നേതൃത്വവും നൽകേണ്ടത് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസറുടെ ഉത്തരവാദിത്തമാണ്.

4.6. നെറ്റ്വർക്ക് / സിസ്റ്റം അഡ്മിനിസ്ട്രേറ്റർ

സിസ്റ്റം അഡ്മിനിസ്ട്രേറ്റർമാർ സിസ്റ്റത്തിന്റെ ദൈനംദിന പ്രവർത്തനത്തിന് മേൽനോട്ടം വഹിക്കുന്നു. ഐടി റിസോഴ്സുകളിലേക്ക് ആർക്കെല്ലാം പ്രവേശനം അനുവദിച്ചിരിക്കുന്നതെന്ന് നിർണ്ണയിക്കാൻ ഇവർക്ക് സാധിക്കും.

എല്ലാ ഉപയോക്തൃ ഐഡികളുടെയും പാസ്വേഡുകളുടെയും അഡ്മിനിസ്ട്രേഷൻ, ഉപയോഗ അവകാശങ്ങൾ നൽകൽ, സുരക്ഷാ ഉപകരണങ്ങൾ, സുരക്ഷാ രീതികൾ എന്നിവ അവലോകനം ചെയ്യൽ, സുരക്ഷാ ലംഘനങ്ങളോട് ഉചിതമായ രീതിയിൽ പ്രതികരിക്കൽ എന്നിവയാണ് നെറ്റ്വർക്ക് / സിസ്റ്റം അഡ്മിനിസ്ട്രേറ്ററുടെ പ്രധാന ഉത്തരവാദിത്തങ്ങൾ.

4.7. സിസ്റ്റം സപ്പോർട്ട് ഓഫീസർമാർ (SSO)

മാനേജർ (എംഐഎസ്) നിയുക്തമാക്കിയ സപ്ലൈകോയുടെ സാങ്കേതിക കഴിവുള്ള വ്യക്തികളാണിവർ. ഡിപ്പോ / ഔട്ട്ലെറ്റ്, പ്രാദേശിക ഓഫീസ് തലത്തിൽ എന്തെങ്കിലും സാങ്കേതിക പ്രശ്നങ്ങൾ ഉണ്ടായാൽ ഇവർ സാങ്കേതിക പിന്തുണ നൽകുന്നു.

4.8. നെറ്റ്വർക്ക് ഓപ്പറേഷൻസ് സെന്റർ (NOC)

കേന്ദ്രീകൃത നെറ്റ്വർക്ക് ഓപ്പറേഷൻ കൺട്രോൾ സെന്റർ എല്ലാ പ്രവർത്തന സമയത്തും നെറ്റ്വർക്ക് ലഭ്യമാണെന്ന് ഉറപ്പാക്കുന്നു.

4.9. ഹെൽപ്പ് ഡെസ്ക്

സിസ്റ്റം അല്ലെങ്കിൽ നെറ്റ്വർക്കുമായി ബന്ധപ്പെട്ട എല്ലാ പ്രശ്നങ്ങൾക്കും സഹായങ്ങളും പിന്തുണയും സിസ്റ്റം സപ്പോർട്ട് ഓഫീസർമാർ അല്ലെങ്കിൽ സിസ്റ്റം സപ്പോർട്ട് ഓഫീസർമാർ ലഭ്യമല്ലാത്ത സ്ഥലങ്ങളിൽ കേന്ദ്ര ഐടി ഹെൽപ്പ്ഡെസ്ക് (എംഐഎസ് ഡിവിഷൻ) നൽകും. ഏതെങ്കിലും ഉപയോക്താവ് ഐടി സിസ്റ്റങ്ങളിൽ എന്തെങ്കിലും പ്രശ്നം കണ്ടെത്തിയാലോ അല്ലെങ്കിൽ എന്തെങ്കിലും സഹായം ആവശ്യമുണ്ടെങ്കിലോ, അവർക്ക് അവരുടെ അഭ്യർത്ഥന ഹെഡ് ഓഫീസിലെ ഐടി അഡ്മിനിസ്ട്രേറ്റർക്ക് ഇ-മെയിൽ വഴി techsupport@supplycomail.com ലേക്ക് അയയ്ക്കാം. അടിയന്തിര സാഹചര്യങ്ങളിൽ ഐടി അഡ്മിനിസ്ട്രേറ്ററെ ടെലിഫോൺ വഴി 0484-2207935 / 0484-2206791 എന്ന നമ്പറിൽ ബന്ധപ്പെടാം അല്ലെങ്കിൽ വെബ്സൈറ്റിൽ ലഭ്യമായ നമ്പറുകളിലും ബന്ധപ്പെടാം.

5. വിവര സാങ്കേതിക വിദ്യയുടെ (ഐടി) ഉപയോഗ നയം

ഉപയോക്താക്കൾ അവരുടെ ഔദ്യോഗിക ഉത്തരവാദിത്തങ്ങൾ നിറവേറ്റുന്നതിനായി ഉപയോഗിക്കുന്ന ഇൻഫർമേഷൻ സിസ്റ്റങ്ങൾക്ക് മേൽ അവർക്ക് പൂർണ്ണ ഉത്തരവാദിത്തമുണ്ടായിരിക്കും. അവർ ഇൻഫർമേഷൻ റിസോഴ്സുകൾ ശ്രദ്ധയോടെ കൈകാര്യം ചെയ്യുകയും സപ്ലൈകോയുടെ സ്വീകാര്യമായ ഉപയോഗ നയത്തിന് അനുസൃതമായി പ്രവർത്തിക്കുകയും ചെയ്യണം.

സപ്ലൈകോയുടെ ഐടി റിസോഴ്സുകളുടെ ഉപയോക്താക്കൾ ഇനിപ്പറയുന്ന നിയമങ്ങൾ പാലിക്കേണ്ടതുണ്ട്.

- സപ്ലൈകോയിലെ ജീവനക്കാർ ഇൻഫർമേഷൻ റിസോഴ്സുകളുടെ ന്യായവും ഉചിതവുമായ ഉപയോഗം പ്രാപ്തമാക്കുന്നതിനും ഇന്ത്യൻ ഗവൺമെന്റിന്റെ ബാധകമായ എല്ലാ നിയമങ്ങൾ, ചട്ടങ്ങൾ, നയങ്ങൾ, ഐടി ആക്റ്റ്, അവയുടെ ഭേദഗതി എന്നിവയ്ക്ക് അനുസൃതമായി അവരുടെ ജോലികൾ നിർവഹിക്കുന്നതിനും ഐടി മാർഗ്ഗനിർദ്ദേശങ്ങളും നയങ്ങളും പാലിക്കണം.
- ഓർഗനൈസേഷന്റെ രഹസ്യ ഇൻഫർമേഷനുകളിലേക്ക് അനുവാദമില്ലാതെ ജീവനക്കാർ അനധികൃതമായി പ്രവേശിക്കരുത്.
- കമ്പ്യൂട്ടറിൽ ജോലി ചെയ്യുമ്പോൾ ഉപയോക്താക്കൾ ഭക്ഷ്യവസ്തുക്കൾ കഴിക്കാതിരിക്കുക, വെള്ളം / പാനീയങ്ങൾ കുടിക്കാതിരിക്കുക. ഇവ അശ്രദ്ധമായി കൈകാര്യം ചെയ്താൽ കമ്പ്യൂട്ടർ അല്ലെങ്കിൽ അവയുടെ അനുബന്ധ ഉപകരണങ്ങൾക്ക് കേടുപാടുകൾ ഉണ്ടാകാൻ സാധ്യതയുണ്ട്. വൃത്തിയുള്ള കൈകളാൽ മാത്രം കമ്പ്യൂട്ടർ പ്രവർത്തിപ്പിക്കുക. സിസ്റ്റവും അനുബന്ധ ഉപകരണങ്ങളും പതിവായി വൃത്തിയാക്കുക. നിങ്ങളുടെ സിസ്റ്റവും യുപിഎസും ഉപയോഗത്തിലില്ലാത്ത സമയത്തോ ഉപയോക്താവ് ഓഫീസ് വിട്ടുപോകുമ്പോഴോ പവർ ഓഫ് ചെയ്യുക.
- ഐടി റിസോഴ്സുകൾ ഉപയോഗിച്ച് ഗെയിമുകൾ കളിക്കുന്നത് കർശനമായി നിരോധിച്ചിരിക്കുന്നു. ഇന്റർനെറ്റ് ചാറ്റും നിരോധിച്ചിരിക്കുന്നു.
- കുറ്റകരമായ വസ്തുക്കളുടെ പ്രദർശനം (കമ്പ്യൂട്ടർ സ്ക്രീനുകളിലോ പോസ്റ്ററുകളിലൂടെയോ) കർശനമായി നിരോധിച്ചിരിക്കുന്നു.
- സോഷ്യൽ നെറ്റ്വർക്കിംഗ് വെബ്സൈറ്റുകൾ, വ്യക്തിഗത മെയിലിംഗ് ലിസ്റ്റുകൾ, ചാറ്റ് റൂമുകൾ, ബ്ലോഗുകൾ എന്നിവയ്ക്ക് സപ്ലൈകോ സിസ്റ്റങ്ങൾ ഉപയോഗിക്കുന്നത് നിരോധിച്ചിരിക്കുന്നു.
- സപ്ലൈകോ പോളിസി പ്രകാരം അനുവദനീയമല്ലാതെ പരസ്യങ്ങൾ, അഭ്യർത്ഥനകൾ, പ്രമോഷനുകൾ അല്ലെങ്കിൽ മറ്റ് വാണിജ്യ സന്ദേശങ്ങൾ എന്നിവ ഉൾപ്പെടെയുള്ള വാണിജ്യ ആവശ്യങ്ങൾക്കായി സപ്ലൈകോ ഇൻഫർമേഷൻ റിസോഴ്സ്സ് ഉപയോഗിക്കരുത്.

5.1. ഇൻഫർമേഷൻ ടെക്നൊളജിയുടെ പൊതുവായ ഉപയോഗ നയം

5.1.1. പാസ്വേഡ് നയം

- പാസ്വേഡ് സുരക്ഷ ഓരോ ഉപയോക്താവിന്റെയും ഉത്തരവാദിത്തമാണ്.

- സപ്ലൈകോയുടെ കമ്പ്യൂട്ടർ, ലാപ്ടോപ്പ്, നെറ്റ്വർക്ക് എന്നീ സുരക്ഷാ സംവിധാനങ്ങളുടെ ഒരു പ്രധാന ഘടകമാണ് പാസ്വേഡുകൾ. ഈ സിസ്റ്റങ്ങൾ ഫലപ്രദമായി പ്രവർത്തിക്കുന്നുവെന്ന് ഉറപ്പുവരുത്തുവാൻ ഉപയോക്താക്കൾ മറ്റുള്ളവർക്ക് എളുപ്പത്തിൽ കണ്ടുപിടിക്കുവാൻ കഴിയാത്ത രഹസ്യസൂചകപദം(password) തിരഞ്ഞെടുക്കുവാൻ ശ്രദ്ധിക്കണം. പാസ്വേഡുകൾ നിങ്ങളുടെ ജോലിയുമായോ വ്യക്തിഗത ജീവിതവുമായോ ബന്ധപ്പെട്ടിരിക്കരുത് എന്നാണ് ഇതിനർത്ഥം.
- പാസ്വേഡ് ഉണ്ടാക്കുമ്പോൾ ഇനിപ്പറയുന്ന കാര്യങ്ങൾ പരിഗണിക്കാം.
  - ✓ പാസ്വേഡ് മറ്റുള്ളവർക്ക് പെട്ടന്ന് കണ്ടുപിടിക്കുവാൻ സാധിക്കാത്തതായിരിക്കണം.
  - ✓ കുറഞ്ഞത് 8-12 അക്ഷരങ്ങൾ ദൈർഘ്യമുള്ളതായിരിക്കണം.
  - ✓ ! $% & * ,. ? + - = പോലുള്ള ചിഹ്നങ്ങൾ ഉൾപ്പെടുത്തണം.
  - ✓ അക്ഷരങ്ങളിൽ ആരംഭിച്ച് അവസാനിപ്പിക്കണം.
  - ✓ നിങ്ങളുടെ സ്വന്തം പേര്, അല്ലെങ്കിൽ നിങ്ങളുടെ ഭാര്യയുടെയോ കുട്ടികളുടെയോ പേരുകൾ, അല്ലെങ്കിൽ നിങ്ങളുടെ ഓർഗനൈസേഷന്റെ പേര്, അല്ലെങ്കിൽ റൂം നമ്പർ അല്ലെങ്കിൽ വീട് നമ്പർ മുതലായവ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.
  - ✓ പാസ്വേഡുകൾ ഇടയ്ക്കിടെ മാറ്റണം.
  - ✓ 'പാസ്വേഡ്' എന്ന വാക്ക് ഒരിക്കലും നിങ്ങളുടെ പാസ്വേഡായി ഉപയോഗിക്കരുത്
  - ✓ പാസ്വേഡ് ശൂന്യമായി ഇടരുത്.
  - ✓ ഇൻസ്റ്റാളേഷൻ സമയത്ത് സോഫ്റ്റ്വെയർ നൽകിയ പാസ്വേഡുകൾ മാറ്റുക.
- വായിക്കാൻ കഴിയുന്ന രൂപത്തിൽ കംപ്യൂട്ടറുകളിൽ പാസ്വേഡ്സുകൾ സൂക്ഷിക്കാൻ പാടില്ല.
- പാസ്വേഡുകൾ എഴുതി അനധികൃത വ്യക്തികൾ കാണുന്ന സ്ഥലത്ത് ഉപേക്ഷിക്കരുത്.

5.1.2. സുരക്ഷ / ഉപയോഗ നിയന്ത്രണം

- ഇൻഫർമേഷൻ സിസ്റ്റങ്ങൾ ദുരുപയോഗം ചെയ്യാതിരിക്കാൻ എല്ലാ ഉപയോക്താക്കളും വേണ്ടത്ര സുരക്ഷാ നടപടികൾ പാലിക്കേണ്ടതാണ്.
- ഇൻഫർമേഷൻ സിസ്റ്റങ്ങൾ ഉപയോഗിക്കുന്നതിന് മുമ്പ്, ജീവനക്കാർ പേരും പാസ്വേഡും നൽകണം. ഉപയോഗത്തിന് ശേഷം സിസ്റ്റം

ലോഗ് ഓഫ് ചെയ്യണം. അനധികൃത പ്രവേശനവും ഉപയോഗവും തടയുന്നതിന് സിസ്റ്റം ലോക്ക് ചെയ്യണം.

- ഇൻഫർമേഷൻ സിസ്റ്റം പാസ്വേഡുകൾ രഹസ്യമായി സൂക്ഷിക്കണം, 90 ദിവസത്തിലൊരിക്കലെങ്കിലും അവ മാറ്റണം.
- ജീവനക്കാർ നെറ്റ്വർക്കിന്റെ സമഗ്രതയെയോ ലഭ്യതയെയോ ബാധിക്കുന്ന പ്രവർത്തനങ്ങളിൽ ഏർപ്പെടാൻ പാടില്ല. ഇതിൽ ഐപി വിലാസങ്ങളുടെ സ്കാൻ, നെറ്റ്വർക്ക് രഹസ്യാന്വേഷണം, സ്നിഫിംഗ്, ഹാക്കിംഗ് തുടങ്ങിയവ ഉൾപ്പെടുന്നു.
- ബാഹ്യ റിസോഴ്സുകളിൽ നിന്ന് (സിഡി, യുഎസ്ബി, മെമ്മറി ഉപകരണങ്ങൾ, ബാഹ്യ ഹാർഡ് ഡിസ്ക് മുതലായവ വഴി) അപ്ലോഡ് ചെയ്തതോ ഇൻറർനെറ്റിൽ നിന്ന് ഇൻഫർമേഷൻ സിസ്റ്റങ്ങളിലേക്ക് ഡൗൺലോഡ് ചെയ്തതോ ആയ എല്ലാ ഫയലുകളും ഉപയോഗത്തിന് മുമ്പ് ആന്റി വൈറസ് സോഫ്റ്റ്വെയർ ഉപയോഗിച്ച് സ്കാൻ ചെയ്യണം.

5.1.3. നെറ്റ്വർക്ക് /സിസ്റ്റങ്ങളിൽ വരുത്തുന്ന മാറ്റങ്ങൾ

ഉപയോക്താക്കൾ കമ്പ്യൂട്ടർ, പ്രിൻറർ തുടങ്ങിയ ഉപകരണങ്ങളിൽ ഏതെങ്കിലും സപ്ലൈകോ നെറ്റ്വർക്കിലേക്ക് മുൻകൂർ അനുവാദമില്ലാതെ ബന്ധിപ്പിക്കുകയോ വിച്ഛേദിക്കുകയോ ചെയ്യരുത്. ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ അധികാരപ്പെടുത്തിയ വ്യക്തികൾക്ക് മാത്രമേ ഏതെങ്കിലും സപ്ലൈകോ കമ്പ്യൂട്ടർ സിസ്റ്റത്തിലോ നെറ്റ്വർക്കിലോ മാറ്റങ്ങൾ വരുത്താൻ കഴിയൂ. സപ്ലൈകോ ഇൻഫർമേഷൻ സിസ്റ്റങ്ങളിലെയും നെറ്റ്വർക്കുകളിലെയും എല്ലാ മാറ്റങ്ങളും രേഖപ്പെടുത്തുകയും ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ/നെറ്റ്വർക്ക് അഡ്മിനിസ്ട്രേറ്റർ മുൻകൂട്ടി അംഗീകരിക്കുകയും വേണം.

5.2. സോഫ്റ്റ്വെയർ ലൈസൻസിംഗ് പോളിസി

സപ്ലൈകോ സ്വയം വികസിപ്പിച്ചെടുത്തതോ, വാങ്ങിയതോ അല്ലെങ്കിൽ ലൈസൻസ് ലഭിച്ചിട്ടുള്ളതോ ആയ ബിസിനസ് സോഫ്റ്റ്വെയർ ആപ്പ്ളിക്കേഷനുകളോ സപ്ലൈകോയുടെ ഉടമസ്ഥതയിലുള്ള ഉപകരണങ്ങളിലുള്ള ഫേംവെയർ, മറ്റേതെങ്കിലും സോഫ്റ്റ്വെയർ ഉൾപ്പെടെയുള്ള എല്ലാ സോഫ്റ്റ് വെയറുകളും ഹെഡ് ഓഫീസിലെ ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ/നെറ്റ്വർക്ക് അഡ്മിനിസ്ട്രേറ്ററുടെ

മുൻകൂർ അനുമതിയില്ലാതെ അവരുടെ വ്യക്തിഗത ഉപയോഗത്തിനായോ ബിസിനസ്സ് ആവശ്യത്തിനായോ ഉപയോഗിക്കരുത്. അനുവദിച്ചിട്ടില്ലാത്ത ഏതെങ്കിലും സോഫ്റ്റ്വെയർ സപ്ലൈകോ സിസ്റ്റത്തിൽ കണ്ടെത്തിയാൽ, അത് എംഐഎസ് ഡിവിഷനെ അറിയിക്കേണ്ടതാണ്. അത്തരം ഉപയോക്താവിനെതിരെ സപ്ലൈകോ ഉചിതമായ അച്ചടക്ക നടപടികൾ എടുക്കും.

ദൈനംദിന ഓഫീസ് ആവശ്യങ്ങൾക്കുള്ള എല്ലാ സോഫ്റ്റ്വെയറുകളും സപ്ലൈകോയുടെ സിസ്റ്റങ്ങളിൽ മുൻകൂട്ടി ഇൻസ്റ്റാൾ ചെയ്തിട്ടുണ്ട്. ഏതെങ്കിലും മറ്റ് ആവശ്യങ്ങൾക്കായുള്ള സോഫ്റ്റ്വെയർ ഇൻസ്റ്റാൾ ചെയ്യുന്നതിന് മുൻപ് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ / നെറ്റ്വർക്ക് അഡ്മിനിസ്ട്രേറ്ററുടെ അംഗീകാരം വേണം.

5.3. ഇൻറർനെറ്റ്, ഇൻട്രാനെറ്റ് ഉപയോഗ നയം

ഇൻറർനെറ്റ് ഉപയോഗിക്കുമ്പോൾ ഉപയോക്താക്കൾ ജാഗ്രത പാലിക്കണം സപ്ലൈകോയുടെ തത്വങ്ങളും മാർഗ്ഗനിർദ്ദേശങ്ങളും കർശനമായി പാലിക്കണം. ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ /നെറ്റ്വർക്ക് അഡ്മിനിസ്ട്രേറ്ററുടെ അംഗീകാരത്തോടെ മാത്രമേ ഇൻറർനെറ്റ് ഉപയോഗം അനുവദിക്കൂ.

സപ്ലൈകോയ്ക്ക് വേണ്ടി ബിസിനസ് നടത്തുന്നതിനായി ഇൻറർനെറ്റിലേക്കും അതിന്റെ റിസോഴ്സുകളിലേക്കും പ്രവേശനം നൽകുന്നു. ഫയർവാൾ വ്യക്തമാക്കിയ പരിമിതികളും വ്യവസ്ഥകളും അനുസരിച്ച് ഇൻറർനെറ്റിന്റെ ന്യായമായ വ്യക്തിഗത ഉപയോഗം അനുവദനീയമാണ്. മുൻകൂട്ടി അറിയിക്കാതെ തന്നെ ഏതെങ്കിലും ഇൻറർനെറ്റ് റിസോഴ്സിലേക്ക് പ്രവേശനം തടയാനുള്ള അവകാശം എംഐഎസ് ഡിവിഷന് ഉണ്ട്.

ജീവനക്കാർ അവരുടെ ഇലക്ട്രോണിക് പോസ്റ്റിംഗുകളിലോ പ്രസിദ്ധീകരണത്തിലോ സപ്ലൈകോയെയോ ജീവനക്കാരെയോ സംബന്ധിച്ച് വിവേചനപരമോ അപകീർത്തിപ്പെടുത്തുന്നതോ ആയ അഭിപ്രായങ്ങൾ നൽകരുത്.

സപ്ലൈകോയുടെ ഐടി സിസ്റ്റങ്ങളെ സംരക്ഷിക്കുന്നതിന് വേണ്ടി ഗെയിമുകൾ, വിനോദ സോഫ്റ്റ് വെയർ അല്ലെങ്കിൽ മറ്റ് അനുചിതമായ ഫയലുകൾ എന്നിവ ഡൗൺലോഡ് ചെയ്യുകയോ, കൈ മാറ്റം ചെയ്യുകയോ എതിരാളികൾക്കെതിരെ

ഗെയിമുകൾ കളിക്കുകയോ, ഇന്റെർനെറ്റിൽ ചൂതാട്ടം നടത്തുകയോ ചെയ്യുന്നത് അനുവദനീയമല്ല.

ഉപയോക്താക്കൾ ഏതെങ്കിലും തരത്തിലുള്ള ഹാക്കിംഗ് നടത്തുകയോ മറ്റ് കമ്പ്യൂട്ടറുകളിലേക്ക് നുഴഞ്ഞുകയറുകയോ ചെയ്യരുത്. സപ്ലൈകോ നെറ്റ് വർക്കിലോ ഇൻറർനെറ്റിലോ വൈറസുകളെയും ദോഷകരമായ പ്രോഗ്രാമുകളെയും ഇൻസ്റ്റാൾ ചെയ്യുകയോ പ്രവേശിപ്പിക്കുകയോ ചെയ്യരുത്. നെറ്റ്വർക്ക് /സിസ്റ്റം അഡ്മിനിസ്ട്രേറ്റർ പതിവായി സിസ്റ്റം ലോഗുകൾ അവലോകനം ചെയ്യേണ്ടതുണ്ട്.

കൂടാതെ, താഴെ വിവരിക്കുന്ന ആവശ്യങ്ങൾക്ക് ഇൻറർനെറ്റ് കണക്ഷൻ ഉപയോഗിക്കാൻ പാടില്ല.

- വിനോദ ആവശ്യങ്ങൾക്ക് വേണ്ടിയുള്ള ഡൗൺലോഡുകളും സെർവർ കമ്പ്യൂട്ടർ ഉപയോഗിക്കാതെ രണ്ടോ അതിൽ കൂടുതലോ കമ്പ്യൂട്ടറുകൾ പരസ്പരം ബന്ധപ്പെടുത്തിയുള്ള വിവര സംഭരണം (പിയർ ടു പിയർ കണക്ഷൻ) നിരോധിച്ചിരിക്കുന്നു.
- പകർപ്പവകാശമുള്ള പ്രോഗ്രാമുകൾ ഉടമയുടെ വ്യക്തമായ അനുമതിയില്ലാതെ സിസ്റ്റങ്ങളിലേക്ക് അല്ലെങ്കിൽ അതിൽ നിന്ന് കൈ മാറുന്നത് നിയമ ലംഘനമാണ്. കൂടാതെ വാണിജ്യപരമായ നേട്ടത്തിനോ ലാഭത്തിനോ വേണ്ടി ഇൻറർനെറ്റ് ഉപയോഗിക്കുന്നത് അനുവദനീയമല്ല.
- സപ്ലൈകോ ഐടി സാമഗ്രികളിൽ അല്ലെങ്കിൽ നെറ്റ് വർക്കിലേക്ക് ബന്ധിപ്പിച്ചിരിക്കുന്ന വ്യക്തിഗത മെഷീനുകളിൽ ലൈസൻസില്ലാത്ത സോഫ്റ്റ്വെയർ ഇൻസ്റ്റാൾ ചെയ്യുന്നത് കർശനമായി നിരോധിച്ചിരിക്കുന്നു.
- സപ്ലൈകോ നെറ്റ്വർക്കിലെ കമ്പ്യൂട്ടർ സിസ്റ്റത്തിലേക്ക് അനധികൃതമായി പ്രവേശിക്കുന്നതും, ഇലക്ട്രോണിക് ഫയലുകൾ അനധികൃതമായി മോഷ്ടിക്കുന്നത്, അംഗീകാരമില്ലാതെ സപ്ലൈകോയുടെ തന്ത്രപ്രധാനമായ വിവരങ്ങൾ കൈമാറുന്നത്, സപ്ലൈകോയുടെ പ്രതിച്ഛായയെ നശിപ്പിക്കുവാൻ സാധ്യതയുള്ള എല്ലാ വിധ ഉള്ളടക്കങ്ങളും പ്രചരിപ്പിക്കുന്നത് നിരോധിച്ചിരിക്കുന്നു.
- സപ്ലൈകോ നെറ്റ്വർക്കിലേക്കോ സെർവറുകളിലേക്കോ വൈറസുകൾ, ട്രോജൻ, ഇമെയിൽ ബോംബുകൾ, റാൻസം വെയർ തുടങ്ങിയ ആപത്കരമായ പ്രോഗ്രാമുകൾ കടത്തി വിടുന്നത് അനുവദനീയമല്ല.

- പകർപ്പവകാശ നിയമം, വ്യാപാര രഹസ്യം, പേറ്റൻറ് മറ്റ് ബൗദ്ധിക സ്വത്തവകാശങ്ങൾ എന്നിവയാൽ പരിരക്ഷിക്കപ്പെട്ടിട്ടുള്ള ഏതെങ്കിലും സപ്ലൈകോ നയം ലംഘിക്കുന്നത് കുറ്റകരമാണ്.
- സോഫ്റ്റ്വെയർ, സാങ്കേതിക വിവരങ്ങൾ, രഹസ്യാത്മക ബിസിനസ് ഡാറ്റ, സാങ്കേതിക പ്രമാണം, സോഫ്റ്റ്വെയർ കോഡുകൾ, ഡാറ്റ, രഹസ്യ കോഡ് രൂപത്തിൽ എഴുതുവാനുള്ള സോഫ്റ്റ്വെയർ അല്ലെങ്കിൽ സംരംഭ സാങ്കേതിക വിദ്യ എന്നിവ വെളിപ്പെടുത്തുന്നത് കുറ്റകരമാണ്.
- ഉപയോക്തൃ നാമം (user name), രഹസ്യ സൂചക പദം (password) വെളിപ്പെടുത്തുന്നത്, മറ്റുള്ളവർക്ക് അക്കൗണ്ട് ഉപയോഗിക്കാൻ അനുവദിക്കുന്നത് കുറ്റകരമാണ്.
- അശ്ലീല സ്വഭാവമുള്ള വീഡിയോകൾ കാണുന്നതും കൈമാറുന്നതും നിരോധിച്ചിരിക്കുന്നു.
- സപ്ലൈകോ സിസ്റ്റങ്ങളോ വ്യക്തിഗത സിസ്റ്റങ്ങളോ ഉപയോഗിച്ച് ഉദ്യോഗസ്ഥരും ജീവനക്കാരും ബ്ലോഗിംഗ് (ഓൺലൈൻ രചനകൾ) ചെയ്യുന്നത് നിബന്ധനകൾക്കും നിയന്ത്രണങ്ങൾക്കും വിധേയമാണ്. സപ്ലൈകോ സിസ്റ്റങ്ങളിൽ നിന്നുള്ള ബ്ലോഗിങ്ങ് സ്ഥാപനത്തിന്റെ (ഓർഗനൈസേഷന്റെ) നിരീക്ഷണത്തിന് വിധേയമാണ്. ഓർഗനൈസേഷന്റെ പ്രതിച്ഛായയെ ദോഷകരമായി ബാധിക്കുന്ന അല്ലെങ്കിൽ കളങ്കപ്പെടുത്തുന്ന ഒരു ബ്ലോഗിംഗിലും ജീവനക്കാർ ഏർപ്പെടരുത്. ബ്ലോഗിങ്ങ് സമയത്ത് ജീവനക്കാർ സ്വയം പ്രതിനിധീകരിക്കുകയും ഓർഗനൈസേഷന്റെ പ്രതിനിധിയായി സ്വയം പ്രതിനിധീകരിക്കുകയും ചെയ്യരുത്.
- വിവര സാങ്കേതിക നിയമം-2000 ലംഘിക്കുന്ന പ്രവർത്തികൾ പാടുള്ളതല്ല.

5.4. ഇ-മെയിൽ ഉപയോഗ നയം

ഐടി ഉപയോഗ നയമനുസരിച്ച് ജീവനക്കാർ ഇ-മെയിലുകൾ ശ്രദ്ധയോടെ ഉപയോഗിക്കുകയും വൈറസുകൾ, ട്രോജനുകൾ, സ്പാം മെയിലുകൾ എന്നിങ്ങനെയുള്ള ഭീഷണികളിൽ നിന്ന് ഇ-മെയിൽ സംരക്ഷിക്കപ്പെടുന്നുവെന്ന് ഉറപ്പ് വരുത്തുകയും വേണം.

ജീവനക്കാർ അജ്ഞാതരിൽ നിന്നും ലഭിച്ച ഇമെയിൽ അറ്റാച്ചുമെൻറുകൾ തുറക്കരുത്, കാരണം അവയിൽ വൈറസുകൾ, ഇമെയിൽ ബോംബ് (ഒരു ഇമെയിൽ അഡ്രസ്സിൽ കുറഞ്ഞ സമയത്തിനുള്ളിൽ പരമാവധി സന്ദേശങ്ങൾ അയച്ച് മെയിൽ ബോക്സ് നിറയ്ക്കുകയും മെയിൻ സെർവറിന്റെ പ്രതികരണ

ശേഷി നശിപ്പിക്കുകയും ചെയ്യുന്ന ക്ഷുദ്ര പ്രോഗ്രാമുകൾ), റാൻസോംവെയറുകൾ (ഇത്തരം സോഫ്റ്റ്വെയർ പ്രോഗ്രാമുകൾ സിസ്റ്റം വീണ്ടും പ്രവർത്തിക്കണമെങ്കിൽ ഫീസ് ആവശ്യപ്പെട്ടുകൊണ്ട് മെസ്സേജുകൾ അയക്കുന്ന ക്ഷുദ്ര പ്രോഗ്രാമുകൾ ആണ്), ബോട്ട് പ്രോഗ്രാമുകൾ (ഉപയോക്താവിന്റെയോ പ്രോഗ്രാമ്മുകളുടെയോ ഏജൻറ് ആയി പ്രവർത്തിക്കുന്ന സോഫ്റ്റ്വെയർ പ്രോഗ്രാമുകൾ), മലിഷ്യസ് സോഫ്റ്റ്വെയർ (ക്ഷുദ്ര സോഫ്ട്വെയറുകൾ) എന്നിവ അടങ്ങിയിരിക്കാം.

സപ്ലൈകോയിലെ നിർദിഷ്ട ഉപയോഗത്തിന് അല്ലെങ്കിൽ പൊതുവായ ഉപയോഗത്തിന് ഉദ്യോഗസ്ഥർക്ക് ഇ-മെയിൽ അക്കൗണ്ട് നല്കിയിടുണ്ട്. ആയത് പാസ്സ്വേർഡ് ഉപയോഗിച്ച് പരിരക്ഷിച്ചിരിക്കുന്നു.

സപ്ലൈകോ ഇമെയിൽ സന്ദേശങ്ങൾ ഔദ്യോഗിക രേഖകളാണ്, ബിസിനസ്സ് പ്രവർത്തനങ്ങളുടെ തെളിവായി അവ നിലനിർത്തുകയും സപ്ലൈകോ ബിസിനസ് ആവശ്യകതകൾ നിറവേറ്റുകയും ചെയ്യും.

ബാഹ്യ സൈറ്റുകളുമായുള്ള ഇൻഫർമേഷൻ കൈമാറ്റം സുരക്ഷിതമല്ലെന്ന് ഇമെയിൽ ഉപയോക്താക്കൾ അറിഞ്ഞിരിക്കണം. അതിനാൽ ഇൻഫർമേഷൻ കൈമാറ്റം വിശ്വസനീയമായ സൈറ്റുകളിൽ മാത്രമായി പരിമിതപ്പെടുത്തണം.

അശ്ലീലമോ, അപകീർത്തിപ്പെടുത്തുന്നതോ, നിരോധിച്ചിരിക്കുന്നതോ, ഓർഗനൈസേഷനെ അപകീർത്തിപ്പെടുത്തുന്ന നിയമവിരുദ്ധമായ ഉള്ളടക്കം, വാചകം, ചിത്രങ്ങൾ എന്നിവ ആന്തരികമോ ബാഹ്യമോ ആയി മറ്റുള്ളവർക്ക് കൈമാറരുത്.

5.5. ലാപ്ടോപ്പ് പോളിസി

ചില ഉദ്യോഗസ്ഥർക്ക് അവരുടെ ഓഫീസ് ജോലികൾ സുഗമമാക്കുന്നതിനായി ലാപ്ടോപ്പ് കമ്പ്യൂട്ടറുകൾ സപ്ലൈകോ വിതരണം ചെയ്യുന്നു, എല്ലാ ലാപ്ടോപ്പുകളും അനുബന്ധ ഉപകരണങ്ങളും സപ്ലൈകോയുടേതാണ്, അവ ഒരു നിശ്ചിത സമയത്തേക്ക് സപ്ലൈകോ ജീവനക്കാർക്ക് നൽകുന്നു.

സപ്ലൈകോയുടെ ലാപ്ടോപ്പ് കമ്പ്യൂട്ടറുകളുടെ ഉപയോഗത്തിന്റെ ഒരു വ്യവസ്ഥ എന്ന നിലയിൽ ഉപഭോക്താക്കൾ ഇനി പറയുന്നവയെല്ലാം പാലിക്കുകയും അംഗീകരിക്കുകയും വേണം.

- സപ്ലൈകോയുടെ ലാപ്ടോപ്പുകളിലൊന്ന് നൽകുന്നതിനുമുമ്പ്, ഉപയോക്താവ് എല്ലാ നയങ്ങളും അംഗീകരിക്കുകയും സ്വീകാര്യത ഫോമിൽ ഒപ്പിടുകയും വേണം.
- ഉപയോക്താവ് സോഫ്റ്റ്വെയറോ ഹാർഡ്വെയറോ ഇൻസ്റ്റാൾ ചെയ്യാനോ നെറ്റ്വർക്ക് ക്രമീകരണങ്ങൾ ഉൾപ്പെടെ സിസ്റ്റം കോൺഫിഗറേഷൻ മാറ്റുന്നതിനോ ശ്രമിക്കരുത്.
- ഉപയോക്താക്കൾ ലാപ്ടോപ്പുകൾ, ഉപകരണങ്ങൾ എന്നിവ കേടുപാടുകളിൽ നിന്നും മോഷണങ്ങളിൽ നിന്നും സംരക്ഷിക്കണം.
- ഓരോ ഹാർഡ്വെയർ തകരാറിനും (കേടുപാടു തീർക്കൽ, ചെലവുകൾ ഉൾപ്പെടെ) ഓരോ ഉപയോക്താവിനും പൂർണ ഉത്തരവാദിത്തമുണ്ട്.
- ജോലി സംബന്ധമായ ഉപയോഗത്തിന്റെ ഫലമായുണ്ടാകുന്ന കമ്പ്യൂട്ടർ തകരാറുകൾക്ക് ഉപയോക്താവ് ഉത്തരവാദിയായിരിക്കില്ല; എന്നിരുന്നാലും, അശ്രദ്ധമൂലം ഉണ്ടാകുന്ന ഏത് പ്രശ്നങ്ങൾക്കും ഉപയോക്താവ് ഉത്തരവാദികളാകും.

5.5.1. ലാപ്ടോപ്പ് ഉപയോഗ പൊതുനിയമങ്ങൾ

- ലാപ്ടോപ്പ് ഉപയോഗത്തിലില്ലാത്തപ്പോഴെല്ലാം അത് ഓഫ് ചെയ്യുക. ലാപ്ടോപ്പ് താത്കാലികമായി നിർത്തിവെയ്ക്കുകയോ നിഷ്ക്രിയ അവസ്ഥയിലോ കൊണ്ട് നടക്കരുത്.
- ലാപ്ടോപ്പുകൾ, മറ്റ് അനുബന്ധ ഉപകരണങ്ങൾ എന്നിവ വ്യക്തിഗത ആവശ്യത്തിന് ഉപയോഗിക്കുന്നത് നിരോധിച്ചിരിക്കുന്നു.
- ലാപ്ടോപ്പ് നിങ്ങളുടെ അടുത്തും അല്ലെങ്കിൽ കാണാവുന്ന വിധത്തിലും സൂക്ഷിക്കുക. അല്ലെങ്കിൽ, സുരക്ഷിതമായി സൂക്ഷിക്കുക.
- അംഗീകൃത ജീവനക്കാരുടെ ഔദ്യോഗിക ഉപയോഗത്തിനായി ലാപ്ടോപ്പുകൾ നൽകുന്നു. സപ്ലൈകോ ലാപ്ടോപ്പുകൾ വായ്പക്കെടുക്കാനോ അല്ലെങ്കിൽ മറ്റുള്ളവർക്ക് ഉപയോഗിക്കാനോ നൽകരുത്.
- ലാപ്ടോപ്പുകളിൽ ഇൻസ്റ്റാൾ ചെയ്തിരിക്കുന്ന ആന്റി വൈറസ് സോഫ്റ്റ്വെയർ കൃത്യമായ ഇടവേളകളിൽ അപ്ഡേറ്റ് ചെയ്തില്ലെങ്കിൽ ലാപ്ടോപ്പ് ദുർബലമാകും.
- അനുയോജ്യമായ ഫയർവാൾ പാക്കേജ്(സെക്യൂരിറ്റിസിസ്റ്റം) ഇൻസ്റ്റാൾ ചെയ്തിട്ടില്ലെങ്കിൽ ലാപ്ടോപ്പുകൾ ഇൻറർനെറ്റുമായി ബന്ധിപ്പിക്കാൻ പാടില്ല.

- ഇ-മെയിൽ അറ്റാച്ചുമെന്റുകൾ വൈറസിന്റെ പ്രധാന ഉറവിടങ്ങളിലൊന്നാണ്. അറിയാത്ത ഇ-മെയിൽ അറ്റാച്ചുമെന്റുകൾ തുറക്കുന്നത് ഒഴിവാക്കുക.
- അനധികൃത സോഫ്റ്റ്വെയർ പ്രോഗ്രാമുകൾ ഡൗൺലോഡ് ചെയ്തോ, ഇൻസ്റ്റാൾ ചെയ്തോ ഉപയോഗിക്കരുത്. വ്യക്തിഗത പ്രോഗ്രാമുകളൊന്നും ഉപയോഗിക്കരുത്.
- അപകടസാധ്യത കുറയ്ക്കുന്നതിന് വേണ്ടി ഏതെങ്കിലും സുരക്ഷാ സംഭവങ്ങൾ (വൈറസ് ആക്രമണം പോലുള്ളവ) കണ്ടാൽ ഉടൻ തന്നെ എംഐഎസ് ഡിവിഷനിൽ റിപ്പോർട്ട് ചെയ്യുക.
- നിങ്ങളുടെ ലാപ്ടോപ്പിൽ പാസ്വേഡുകൾ (രഹസ്യസൂചകപദം) ഒരിക്കലും സൂക്ഷിക്കരുത്.
- ലാപ്ടോപ്പിന്റെ കീബോർഡും ടച്ച്പാഡും സിസ്റ്റത്തിന്റെ ബാക്കി ഭാഗങ്ങളുമായി ശാശ്വതമായി ഘടിപ്പിച്ചിരിക്കുന്നതിനാൽ, അവ ഉപയോഗിക്കുന്നതിന് മുമ്പ് നിങ്ങളുടെ കൈകൾ ശുദ്ധമാണെന്ന് ഉറപ്പാക്കുക.
- ലാപ്ടോപ്പിന് സമീപത്തായി പാനീയങ്ങളോ ഭക്ഷണമോ വെയ്ക്കരുത്.
- ലാപ്ടോപ്പ് ബാറ്ററിയിൽ നിന്ന് കൂടുതൽ ആയുസ്സ് കിട്ടാൻ ലാപ്ടോപ്പ് 100 ശതമാനം ചാർജ്ജയാൽ അത് അൺപ്ലഗ് ചെയ്യുക.
- ലാപ്ടോപ്പ് ചാർജ് ചെയ്തതിനുശേഷം അത് പൂർണ്ണമായും ഡിസ്ചാർജ് ചെയ്യുന്നത് ഒഴിവാക്കുക. ബാറ്ററി ചാർജ് നില 20 ശതമാനം മുതൽ 80 ശതമാനം വരെ നിലനിർത്താൻ ശ്രദ്ധിക്കേണ്ടതാണ്
- അശ്ലീല, വംശീയ, അപകീർത്തിപ്പെടുത്തുന്ന ഫയലുകൾ, ഫോട്ടോഗ്രാഫുകൾ, വീഡിയോകൾ അല്ലെങ്കിൽ ഇ-മെയിൽ സന്ദേശങ്ങൾ എന്നിവ പോലുള്ളവ ഒരിക്കലും ലാപ്ടോപ്പുകളിൽ സംഭരിക്കരുത്, ഉപയോഗിക്കരുത്, പകർത്തരുത്, പ്രചരിപ്പിക്കരുത്.
- ലാപ്ടോപ്പിന്റെ ഉപയോക്താവ് ലാപ്ടോപ്പുകളുടെയും വിവരങ്ങളുടെയും ഉപയോഗത്തിന് ബാധകമായ പ്രസക്തമായ നിയമങ്ങളും ചട്ടങ്ങളും നയങ്ങളും പാലിക്കണം, ഉദാ. സപ്ലൈകോ നയം, ലൈസൻസ്, പകർപ്പവകാശം, സ്വകാര്യതാ നിയമങ്ങൾ.

6. ഡാറ്റാ ബാക്കപ്പ് പോളിസി

ഇൻഫർമേഷനുകൾ നഷ്ടപ്പെടുന്നത് തടയുന്നതിന് ഒരു ബാക്കപ്പ് നടപടിക്രമം ആവശ്യമാണ്. .

ഹെഡ് ഓഫീസിലെ സെർവർ ഡാറ്റ ബാക്കപ്പ് ചെയ്യുന്നതിനുള്ള ഉത്തരവാദിത്തം നെറ്റ്വർക്ക്/ഡാറ്റാബേസ് അഡ്മിനിസ്ട്രേറ്റർമാർക്കാണ്.

- വൈറസ് ആക്രമണം പലപ്പോഴും കമ്പ്യൂട്ടറിലെ ഡാറ്റയെ നശിപ്പിക്കും. ശരിയായ ബാക്കപ്പുകൾ ഇല്ലാതെ, നശിപ്പിച്ച ഫയലുകൾ വീണ്ടെടുക്കൽ അസാധ്യമായിരിക്കും.
- പൊതുവായ നിയമം: എല്ലാ നിർണായക ബിസിനസ്സ് അപ്ലിക്കേഷനുകൾക്കും ദിവസേന (അതായത് തിങ്കൾ മുതൽ ഞായർ വരെ) പൂർണ്ണ ബാക്കപ്പ് നടത്തുന്നു.
- ഡാറ്റാബേസ് സെർവറുകളിലെ ഡാറ്റ ബാക്കപ്പ്: മുൻനിശ്ചയിച്ച സമയത്ത് ഒരു സ്വയം പ്രവർത്തിക്കുന്ന നടപടിക്രമത്തിലൂടെ ഡാറ്റാബേസിലെ എല്ലാ ഇൻഫർമേഷനുകളും ബാക്കപ്പ് ചെയ്യുന്നുണ്ടെന്ന് ഉറപ്പ് വരുത്തേണ്ടതാണ്. കൂടാതെ അതിന്റെ ഡാറ്റ സമഗ്രതയും ഉറപ്പ് വരുത്തേണ്ടതാണ്.
- ഔട്ട്ലെറ്റ് / ഡിപ്പോയിലെ ഡെസ്ക്ടോപ്പ് പിസിയിലെ ഡാറ്റ ബാക്കപ്പ്: ഔട്ട്ലെറ്റ് / ഡിപ്പോയുടെ ചുമതല ഏൽപ്പിച്ച ഉദ്യോഗസ്ഥന്റെ ഉത്തരവാദിത്തമാണിത്. ഉത്തരവാദിത്തപ്പെട്ട ഉദ്യോഗസ്ഥർ അവരുടെ സുപ്രധാന ഡാറ്റയുടെ പതിവ് ബാക്കപ്പുകൾ പരിശോധിക്കണം. വൈറസ് ആക്രമണം പലപ്പോഴും കമ്പ്യൂട്ടറിലെ ഡാറ്റ നശിപ്പിക്കും. ശരിയായ ബാക്കപ്പുകൾ ഇല്ലാതെ, നശിപ്പിച്ച ഫയലുകൾ വീണ്ടെടുക്കൽ അസാധ്യമായിരിക്കും.
- കമ്പ്യൂട്ടറിന്റെ ഹാർഡ് ഡിസ്ക് സാധാരണ സി, ഡി എന്നിങ്ങനെ വിഭജിക്കാം. മറ്റ് സോഫ്റ്റ്വെയറുകൾ സി ഡ്രൈവിലും, ഉപയോക്താക്കളുടെ ഡാറ്റ ഡി ഡ്രൈവിലും ആയിരിക്കണം. ഏതെങ്കിലും വൈറസ് പ്രശ്നമുണ്ടായാൽ, സാധാരണയായി സി ഡ്രൈവ് മാത്രമേ തകരാറിലാകുകയുള്ളു. അത്തരമൊരു സാഹചര്യത്തിൽ സി ഡ്രൈവ് മാത്രം ഫോർമാറ്റുചെയ്യുന്നത് ഡാറ്റ നഷ്ടത്തെ പരിരക്ഷിക്കും.
- ഇതുകൂടാതെ, ഉപയോക്താക്കൾ അവരുടെ വിലയേറിയ ഡാറ്റ സിഡിയിലോ പെൻ ഡ്രൈവുകൾ പോലുള്ള മറ്റ് സംഭരണ ഉപകരണങ്ങളിലോ നെറ്റ്വർക്കിൽ കണക്റ്റുചെയ്തിരിക്കുന്ന മറ്റ് കമ്പ്യൂട്ടറിലോ സൂക്ഷിക്കണം.
- ഏതെങ്കിലും ഔട്ട്ലെറ്റ് / ഓഫീസിൽ ഒന്നിൽ കൂടുതൽ കമ്പ്യൂട്ടർ ഉണ്ടെങ്കിൽ, ബാക്കപ്പ് ഡാറ്റ മറ്റൊരു കമ്പ്യൂട്ടറിലും സംഭരിക്കേണ്ടതാണ്. സിസ്റ്റം സപ്പോർട്ട് ഓഫീസർമാർ അവരുടെ പരിധിയിൽ വരുന്ന എല്ലാ ഔട്ട്ലെറ്റുകളും ഡിപ്പോകളും അവരുടെ ഡാറ്റ പതിവായി ബാക്കപ്പ് ചെയ്യുന്നുണ്ടെന്ന് പരിശോധിക്കുകയും ഉറപ്പാക്കുകയും വേണം.

7. ലംഘനങ്ങൾ

ഇനിപ്പറയുന്ന പ്രവർത്തനങ്ങൾ പൊതുവേ നിരോധിച്ചിരിക്കുന്നു:

- സപ്ലൈകോയുടെ ഇൻഫർമേഷൻ സിസ്റ്റങ്ങൾ ഉപയോഗിച്ച് നിയമവിരുദ്ധമായ ഒരു പ്രവർത്തനത്തിലും ജീവനക്കാർ ഏർപ്പെടാൻ പാടില്ല.
- അശ്ലീലമെന്ന് കരുതപ്പെടുന്നവ സംഭരിക്കുന്നതിനോ കൈമാറുന്നതിനോ സിസ്റ്റങ്ങൾ ഉപയോഗിക്കാൻ പാടില്ല.
- ഓർഗനൈസേഷന്റെ പുറത്തുള്ള കക്ഷികൾക്ക് വ്യക്തിഗത നേട്ടത്തിനായി സപ്ലൈകോയുടെ രഹസ്യ ഇൻഫർമേഷനുകൾ, വ്യക്തിഗത വിവരങ്ങൾ, അതിന്റെ സാമ്പത്തിക വിവരങ്ങൾ, ഡാറ്റ, തന്ത്രപരമായ പദ്ധതികൾ എന്നിവ നൽകരുത്.
- സിസ്റ്റങ്ങളിൽ അറിയപ്പെടാത്ത അല്ലെങ്കിൽ വ്യാജ ഐഡന്റിറ്റികളുടെ ഉപയോഗം നിരോധിച്ചിരിക്കുന്നു.
- വിവര സാങ്കേതിക നിയമം-2000 ലംഘിക്കുന്ന പ്രവർത്തികൾ പാടുള്ളതല്ല.

'സംഭവം' എന്ന പദത്തിന്റെ നിർവചനം :

കമ്പ്യൂട്ടർ സുരക്ഷാ നയങ്ങൾ, സ്വീകാര്യമായ ഉപയോഗ നയങ്ങൾ, സുരക്ഷാ രീതികൾ എന്നിവയുടെ ലംഘനം അല്ലെങ്കിൽ ഭീഷണി എന്നാണ് ഒരു സംഭവത്തെ നിർവചിച്ചിരിക്കുന്നത്.

ലംഘനങ്ങൾ റിപ്പോർട്ടുചെയ്യുക:

ഈ നയത്തിന്റെ ലംഘനങ്ങൾ ശ്രദ്ധയിൽപ്പെട്ടാൽ ആയത് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ / നെറ്റ്വർക്ക് അഡ്മിന് റിപ്പോർട്ട്ചെയ്യണം, കൂടാതെ സിസ്റ്റം തകരാറുകൾ, സിസ്റ്റം സുരക്ഷയുമായി ബന്ധപ്പെട്ട സംശയങ്ങൾ അല്ലെങ്കിൽ നിയമ വിരുദ്ധമോ ഉചിതമല്ലാത്തതോ ആയ സിസ്റ്റം പ്രവർത്തനങ്ങൾ എന്നിവ റിപ്പോർട്ടുചെയ്യണം. എല്ലാ ജീവനക്കാരും നിരീക്ഷിച്ച ഏതെങ്കിലും സംഭവം ശ്രദ്ധയിൽ പെട്ടാൽ ആയത് എംഐഎസ് ഡിവിഷൻ ഹെൽപ്പ്ഡെസ്കിലേക്ക് അല്ലെങ്കിൽ ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർക്ക് റിപ്പോർട്ട് ചെയ്യണം. സംഭവങ്ങൾ ഫോൺ വഴിയോ ("0484-2207935 / 0484-2206791") അല്ലെങ്കിൽ ഇമെയിൽ വഴിയോ ("techsupport@supplycomail.com") റിപ്പോർട്ട് ചെയ്യാം.

കമ്പ്യൂട്ടിംഗ് പ്രിവിലേജുകളുടെ ദുരുപയോഗം:

സപ്ലൈകോ ഇൻഫർമേഷൻ റിസോഴ്സുകളായ കമ്പ്യൂട്ടറുകൾ, സോഫ്റ്റ്വെയർ, ഡാറ്റ, നെറ്റ്വർക്കുകൾ എന്നിവ ശരിയായ അംഗീകാരമില്ലാതെ ഉപയോക്താക്കൾ ഉപയോഗിക്കരുത്. ഉദാഹരണത്തിന്, സപ്ലൈകോ ഉൾപ്പെടുന്ന നെറ്റ്വർക്കുകളുടെ ദുരുപയോഗം അല്ലെങ്കിൽ ആ നെറ്റ്വർക്കുകളുമായി ബന്ധിപ്പിച്ചിട്ടുള്ള മറ്റ് സൈറ്റുകളിലെ കമ്പ്യൂട്ടറുകൾ തുടങ്ങിയവ സപ്ലൈകോ കമ്പ്യൂട്ടിംഗ് പ്രത്യേകാവകാശങ്ങളുടെ ദുരുപയോഗമായി കണക്കാക്കും.

പ്രിവിലേജുകളുടെ സസ്പെൻഷൻ (പ്രത്യേകാവകാശങ്ങൾ താത്കാലികമായി നിർത്തി വെക്കൽ):

സിസ്റ്റം / നെറ്റ്വർക്ക് അഡ്മിനിസ്ട്രേറ്റർമാർ അവരുടെ മേൽനോട്ടത്തിലുള്ള ഇൻഫർമേഷൻ റിസോഴ്സുകളുടെ സമഗ്രത നിലനിർത്തേണ്ടത് ആവശ്യമായി വന്നാൽ ഇൻഫർമേഷൻ റിസോഴ്സുകൾ ഉപയോഗിക്കാനുള്ള അനുമതി താൽക്കാലികമായി നിർത്തിവച്ചേക്കാം.

സഹകരണ അഭ്യർത്ഥന:

നയ ദുരുപയോഗത്തെക്കുറിച്ചുള്ള ഏത് അന്വേഷണവുമായും ഉപയോക്താക്കൾ സഹകരിക്കേണ്ടതാണ്. സഹകരിക്കാത്ത പക്ഷം പ്രത്യേകാവകാശങ്ങൾ റദ്ദാക്കുകയോ അല്ലെങ്കിൽ മറ്റ് അച്ചടക്ക നടപടികളോ ഉണ്ടാകാം.

ഇൻഫർമേഷനും സിസ്റ്റങ്ങളും ആക്സസ് ചെയ്യുന്നു :

ഒരു വ്യക്തിയുടെയോ സപ്ലൈകോ കമ്മ്യൂണിറ്റിയുടെയോ സുരക്ഷ ഉറപ്പുവരുത്തുക, നിയമം പാലിക്കുക വിവര ഉപായങ്ങളുടെ ശരിയായ പ്രവർത്തനം ഉറപ്പാക്കുക എന്നിവയ്ക്കായി വിവരങ്ങളും വിവര ഉപാധികളും പരിശോധിക്കുകയും നിരീക്ഷിക്കുകയും ചെയ്യേണ്ടതുണ്ട്. ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർക്ക് മാത്രമേ ഈ പരിശോധനയ്ക്കും നിരീക്ഷണത്തിനും അംഗീകാരം ഉള്ളൂ.

നിയമ, ഓർഗനൈസേഷൻ പ്രക്രിയകൾക്കായുള്ള ആക്സസ്:

ചില സാഹചര്യങ്ങളിൽ ഓർഗനൈസേഷൻ, മൂന്നാം കക്ഷികൾക്ക് ഇലക്ട്രോണിക് അല്ലെങ്കിൽ മറ്റ് രേഖകൾ, അല്ലെങ്കിൽ ആ രേഖകളുമായി ബന്ധപ്പെട്ട വിവരങ്ങൾ അല്ലെങ്കിൽ വിവര ഉപാധികളുടെ ഉപയോഗവുമായി ബന്ധപ്പെട്ട വിവരങ്ങൾ നൽകേണ്ടി വരും. കൂടാതെ, സംരംഭകൻ അതിന്റെ വിവര രേഖകൾ അവലോകനം ചെയ്യാം, ഉദാ. അന്വേഷണങ്ങളുമായി ബന്ധപ്പെട്ട് സംരംഭകന്റെ ശരിയായ പ്രവർത്തനത്തിനായി അല്ലെങ്കിൽ വ്യക്തികളുടെയോ സംരംഭകന്റെയോ സുരക്ഷ പരിരക്ഷിക്കുന്നതിന്.

ഓർഗനൈസേഷന് സേവനങ്ങൾ നൽകുന്നതിനും പരിപാലിക്കുന്നതിനും മെച്ചപ്പെടുത്തുന്നതിനും മൂന്നാം കക്ഷി സേവന ദാതാക്കൾക്ക് ഡാറ്റയിലേക്ക് ന്യായമായ പ്രവേശനം സംരംഭകൻ അനുവദിച്ചേക്കാം.

നെറ്റ്വർക്കുകളുടെ കേടുപാടുകളും അധിക ഉപയോഗവും ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർക്ക് റിപ്പോർട്ട് ചെയ്യേണ്ടതാണ്. നെറ്റ്വർക്ക് അഡ്മിനിസ്ട്രേറ്റർ പതിവായി നെറ്റ്വർക്ക് ട്രാഫിക്കിനെ നിരീക്ഷിച്ചുകൊണ്ടിരിക്കും. സിസ്റ്റം അല്ലെങ്കിൽ നെറ്റ്വർക്ക് സുരക്ഷാ ഏകീകരണം അപഹരിക്കപ്പെട്ടുവെന്ന് നെറ്റ്വർക്ക് അഡ്മിനിസ്ട്രേറ്റർക്ക് ബോധ്യപ്പെട്ടാൽ അവസ്ഥ ശരിയാക്കുന്നതുവരെ അല്ലെങ്കിൽ പ്രശ്നം പരിഹരിക്കുന്നതുവരെ നിയന്ത്രണങ്ങൾ ഏർപ്പെടുത്തുകയും, കുറ്റകൃത്യങ്ങൾ വളരെ ഗുരുതരമായ സ്വഭാവമുള്ളതാണെങ്കിൽ, ഒരു റിപ്പോർട്ട് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർക്ക് അയയ്ക്കുകയും ചെയ്യും.

ഇമെയിൽ, അച്ചടിച്ച അറിയിപ്പുകൾ അല്ലെങ്കിൽ വാർത്തകൾ മുഖേനയുള്ള ഒരു ഹ്രസ്വ അറിയിപ്പിന് ശേഷം പുതിയ നയങ്ങൾ അല്ലെങ്കിൽ നയത്തിലെ മാറ്റങ്ങൾ പ്രാബല്യത്തിൽ വരും.

---------- അവസാനത്തെ പേജ്----------