

# BUSINESS POLICIES OF THE COMPANY

In adherence to the

1. The Master directions and guidelines issued by Reserve Bank of India (RBI) applicable for Non-Banking Finance Companies and
2. The Companies Act, 2013 and Rules made thereunder

## INDEX

S No	Policy Name	Page No
1	Fair Practice Code (Malayalam)	1
2	Fair Practice Code (English)	4
3	Interest Rate Policy	10
4	KYC and Prevention of Money Laundering Policy	17
5	Gold Lending Policy	34
6	Gold Auction Policy	38
7	The Grievance Redressal Policy	43
8	Prudential Norms on Income Recognition, Asset Classification and Provisioning pertaining to advances – RBI circular dated 12/11/2021	48
9	Fraud Reporting	50
10	IT Policy	51
11	Policy on Loans and Advances to Directors and Senior Officers	73
12	Risk Management Policy 2023-24	80
13	POSH	89
14	Ombudsman Scheme	101
15	Customer Security Tips	106
16	Be Aware - RBI	109
17	Red Flag Indicators	148

**A)**

Applicable Regulation : RBI/2011-12/470 DNBS.CC. PD. No.266 /03.10.01/2011-12 dated 26<sup>th</sup> March 2012  
 Company Name : JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED  
 CIN : U65921KL1996PTC009845  
 Applicability : Registered Office & Branch offices of the company in Kerala

**B ) ലക്ഷ്യങ്ങൾ**

FPC യുടെ ലക്ഷ്യങ്ങൾ താഴെ പറയും പ്രകാരമാണ്.

- i) ഉപഭോക്താക്കളുമായി ഇടപെടുമ്പോൾ മികച്ച നടപടി സ്വീകരിക്കുക.
- ii) വെല്ലുവിളിയുയർത്തുന്ന ലക്ഷ്യങ്ങൾ വയ്ക്കുകയും ഉയർന്ന പ്രവർത്തന നിലവാരം കൈവരിക്കുകയും ചെയ്ത് ഉപഭോക്തൃ സംതൃപ്തി ഉറപ്പാക്കുക.
- iii) വ്യാപാരത്തിൽ ഏർപ്പെടുമ്പോൾ സുതാര്യവും ന്യായവും നീതിശാസ്ത്രാനുസാരിയായതും സമർത്ഥിക്കാവുന്നതുമായ നടപടി പിന്തുടരുക.
- iv) ഉപഭോക്താവിന് /ഭാവി ഉപഭോക്താക്കൾക്ക് ആവശ്യമായ എല്ലാ വിവരങ്ങളും വിവരണങ്ങളും നൽകുകയും പരസ്യ സഹായക പൂർണ്ണമായ ദീർഘകാല ബന്ധം വളർത്തിയെടുക്കുകയും ചെയ്യുക.
- v) നിരന്തരമായി വളർന്നുകൊണ്ടിരിക്കുന്ന സംതൃപ്തരായ ഉപഭോക്താക്കളുടെ അടിസ്ഥാന കെട്ടിപ്പടുക്കുക അതേസമയം സംശയകരമായ സാക്ഷ്യപത്രങ്ങളോ ക്രിമിനൽ പശ്ചാത്തലമോ ഉള്ള ഉപഭോക്താക്കളെ എടുക്കുന്നത് ഒഴിവാക്കുകയും ചെയ്യുക.

**C ) സത്യവാങ്മൂലവും പ്രതിജ്ഞാബദ്ധതയും**

- i) ആർ ബി ഐ, എസ് ഇ ബി ഐ, ഐ ആർ ഡി എ, സർക്കാർ, പ്രാദേശിക ഭരണകൂടങ്ങൾ മുതലായ സ്ഥാപനങ്ങൾ പുറപ്പെടുവിക്കുന്ന നിയമങ്ങൾ, ചട്ടങ്ങൾ, മാർഗ്ഗനിർദ്ദേശങ്ങൾ എന്നിവ പാലിക്കുന്നതാണെന്ന് ഉറപ്പ് തരണം.
- ii) കഴിവുറ്റതും മികച്ചതും കൃതാർത്ഥവുമായ സേവനങ്ങൾ വഴി ഉപഭോക്താക്കൾക്ക് സംതൃപ്തമായ സേവനം കമ്പനിയുടെ എല്ലാ ഓഫീസുകളിലും കമ്പനി ഉറപ്പ് വരുത്തുന്നതാണ്.
- iii) കമ്പനിക്കുള്ളിൽ തന്നെ ലക്ഷ്യങ്ങൾ ഉന്നമിടുകയും അവ നടപ്പിലാക്കാനും മെച്ചപ്പെടുത്താനും നിരന്തരമായി ശ്രമിക്കുകയും ചെയ്യും. ഇപ്രകാരം, വ്യവസായത്തിൽ നിലനിൽക്കുന്ന നിലവാരത്തിനപ്പുറം പോകാൻ സാധിക്കും.
- iv) മതം, ജാതി, ലിംഗം, ഭാഷ എന്നീ കാര്യങ്ങളിന്മേൽ ഉപഭോക്താക്കളോട് വേർതിരിവ് കാണിക്കുകയില്ലെന്ന് കമ്പനി ഉറപ്പുനൽകുന്നു.
- v) ഉപഭോക്താവിനും/ഭാവി ഉപഭോക്താക്കൾക്കും കമ്പനിയുടെ ഉൽപ്പന്നങ്ങളെയും സേവനങ്ങളെയും സംബന്ധിച്ച് കമ്പനി പൂർണ്ണവും വ്യക്തവുമായ എല്ലാ വിവരങ്ങളും നൽകുന്നതായിരിക്കും. അതോടൊപ്പം തന്നെ ഭാവിയിൽ തെറ്റിദ്ധാരണ പരത്തുന്നതോ തെറ്റിധരിപ്പിക്കുന്നതോ ആയ പരസ്യങ്ങളോ മാധ്യമ പ്രസിദ്ധീകരണങ്ങളോ യാതൊന്നും തന്നെ കമ്പനി അവലംബിക്കുന്നതല്ല.
- vi) ഒളിഞ്ഞിരിക്കുന്ന ചാർജ്ജുകൾ അഥവാ സുതാര്യതയില്ലായ്മയുടെ ഘടകങ്ങൾ ഉള്ള ഉല്പന്നങ്ങൾ/സേവനങ്ങൾ അവതരിപ്പിക്കുന്നത് ഒഴിവാക്കുമെന്ന് കമ്പനി ഉറപ്പുനൽകുന്നു.
- vii) എല്ലാ ഉപഭോക്താക്കളോടും കമ്പനി പ്രാദേശിക ഭാഷയിൽ ആശയവിനിമയം നടത്തുകയും ഉപഭോക്താവ് ആവശ്യപ്പെട്ടാൽ മാത്രം ഇംഗ്ലീഷിലും ആശയവിനിമയം നടത്തുന്നതുമാണ്.
- viii) ഉപഭോക്താവ് പണയം വെച്ചിരിക്കുന്ന ഉരുപ്പടി സുരക്ഷിതവും ഭദ്രവുമാക്കി വയ്ക്കാൻ കമ്പനി സാധ്യമായതും യുക്തിപൂർവ്വവുമായ നടപടികൾ എടുക്കുന്നതാണ്. കമ്പനിയുടെ കസ്റ്റഡിയിൽ ഇരിക്കുമ്പോൾ ഉരുപ്പടിക്ക് സംഭവിക്കാവുന്ന സാഹചര്യപരമോ സൂക്ഷ്മതാക്കുറവുമുലമോ വഞ്ചനമുലമോ ആയ നഷ്ടങ്ങൾക്കു നഷ്ടപരിഹാരം നൽകുന്നതാണെന്ന് ഉറപ്പുനൽകുന്നു.
- ix) ഇടപാട് നടത്തുന്ന ഉപഭോക്താവ് ശ്രദ്ധയില്ലായ്മ മൂലമോ എഴുതുമ്പോൾ വരുന്ന തെറ്റ് മൂലമോ വരുത്തുന്ന കാര്യങ്ങൾ മുതലെടുപ്പിനായി ഉപയോഗിക്കില്ലെന്ന് കമ്പനി ഉറപ്പുനൽകുന്നു.
- x) ഉപഭോക്താക്കളുടെ പരാതികളും നിർദ്ദേശങ്ങളും എത്രയും വേഗം പരിഹരിക്കുന്നതിനായി പടിപടിയായി ഉയർന്ന നിലയിൽ പരിഹാരം തേടാനുള്ള സാധ്യതയോട് കൂടിയ സുസ്ഥാപിതമായ പരാതി പരിഹാര പ്രക്രിയ സ്ഥാപിക്കുന്നതിന് കമ്പനി പ്രതിജ്ഞാബദ്ധമാണ്.
- xi) കമ്പനി FPC (Fair Practice Code) സ്വന്തം വെബ്സൈറ്റിൽ പ്രദർശിപ്പിക്കും. ഉപഭോക്താവ് ആവശ്യപ്പെടുകയാണെങ്കിൽ FPC യുടെ ഒരു പകർപ്പ് നൽകും.

**D ) നല്ല പ്രവർത്തന ചട്ടങ്ങൾ**

**I ) വായ്പകൾ, വായ്പാ വ്യവസ്ഥകൾ, പലിശ നിരക്ക് മറ്റു നിരക്കുകൾ എന്നിവ**

- i) വായ്പ എടുക്കുവാൻ വരുന്ന ഇടപാടുകൾക്ക് അതതു ബ്രാഞ്ചുകളിൽനിന്നും തുക ഈടാക്കാതെ തന്നെ വായ്പാ അപേക്ഷയോടൊപ്പം ബോധിപ്പിക്കേണ്ടതായ രേഖകൾ ഏതെന്ന് സൂചിപ്പിക്കുക കൂടി ചെയ്യുന്ന പൂർണ്ണതയോട് കൂടി ലഭിച്ചിട്ടുള്ള വായ്പാ അപേക്ഷയുടെ രസീതുകൾ ഉടൻ തന്നെ ഉപഭോക്താക്കൾക്ക് നൽകുന്നതാണ്. കമ്പനിയുടെ സേവന വ്യവസ്ഥകളെ അടിസ്ഥാനപ്പെടുത്തി വായ്പാ അപേക്ഷകൾ ഉടൻ തന്നെ അനുവദിക്കുകയോ തള്ളുകയോ ചെയ്യുന്നതാണ്. വായ്പാ തുക ലഭ്യമാക്കുന്നതും അതിനുവേണ്ട സെക്യൂരിറ്റി സ്വീകരിക്കുന്നതും ഏകദേശം ഒരേ സമയത്തായിരിക്കും.
- ii) എല്ലാ വിവരങ്ങളും അറിഞ്ഞുകൊണ്ട് തന്നെ തീരുമാനം എടുക്കുന്നതിന് സഹായകമാകത്തക്കവിധം വായ്പയുമായി ബന്ധപ്പെട്ട ലഭ്യമാകുന്ന തുക, പലിശനിരക്ക്, മറ്റു ചിലവുകൾ, പിഴ പലിശ, പലിശ കണക്കാക്കുന്ന രീതി, പലിശയിലുള്ള കിഴിവ് എന്നിവ വായ്പ അനുവദിക്കുന്നതിന് മുമ്പായി ഉപഭോക്താവിനോട്/ഭാവി ഉപഭോക്താവിനോട് വെളിപ്പെടുത്തുന്നതാണ്. ഉപഭോക്താവ്/ഭാവി ഉപഭോക്താവ് ആവശ്യപ്പെടുന്ന പക്ഷം വായ്പ അനുവദിക്കുന്നതിന് മുമ്പ് തന്നെ വായ്പാ വ്യവസ്ഥകൾ ലഭ്യമാക്കുന്നതാണ്.
- iii) പ്രാദേശിക ഭാഷയിലോ ഉപഭോക്താവിന് മനസ്സിലാകുന്ന മറ്റേതെങ്കിലും ഭാഷയിലോ ലോൺ സൗകര്യത്തെ സംബന്ധിക്കുന്ന നിബന്ധനകളും വ്യവസ്ഥകളും അടങ്ങിയ വായ്പാ അനുമതി പത്രം (പണയ ടിക്കറ്റ്) ഉപഭോക്താവിന് നൽകുന്നുവെന്ന് കമ്പനി ഉറപ്പുവരുത്തണം. വായ്പാ തുക, വായ്പാ അക്കൗണ്ട് നമ്പർ, പലിശ നിരക്ക്, ചാർജ്ജുകൾ, വായ്പാ നടപടി പ്രക്രിയ ഫീസ് തുടങ്ങിയ വിവരങ്ങൾ വായ്പാ അനുമതി

പത്രത്തിൽ (പണയ ടിക്കറ്റ്) ഉണ്ടായിരിക്കണം. കമ്പനിയുടെ അംഗീകൃത ഉദ്യോഗസ്ഥന്റെ ഒപ്പോടു കൂടിയ വായ്പ അനുമതി പത്രം (പണയ ടിക്കറ്റ്) ഉപഭോക്താക്കൾക്ക് സൗകര്യപ്പെടുത്തുന്ന പണയ ഉരുപ്പടി (സ്വർണ്ണം) ക്ഷേമ രസീതി കൂടിയാണ്.

iv) പലിശനിരക്ക് ഉൾപ്പെടെയുള്ള വ്യവസ്ഥകളുടെയും നിബന്ധനകളുടെയും കാര്യത്തിൽ സാധാരണയായി കമ്പനി യാതൊരു തരത്തിലുള്ള മാറ്റങ്ങളും/ഭേദഗതികളും വരുത്താറില്ല. ഉപഭോക്താക്കളെ സാമ്പത്തികമായോ അല്ലാതെയോ ദോഷകരമായി ബാധിക്കും എന്നതിനാലാണിത്. അസാധാരണ സാഹചര്യങ്ങളിൽ അത്തരം മാറ്റങ്ങൾ/ഭേദഗതികൾ അനിവാര്യമായി വരികയാണെങ്കിൽ പുതിയ സാഹചര്യങ്ങൾ കണക്കിലെടുത്തുകൊണ്ട് അത്തരം മാറ്റങ്ങളെക്കുറിച്ച്/ഭേദഗതികളെക്കുറിച്ച് ഉപഭോക്താവിന് മതിയായതും ശരിയായ രീതിയിലുള്ളതുമായ നോട്ടീസ് നൽകുന്നതാണ്.

**II) വിപണനവും പ്രചാരണോപാധികളും**

i) ഉപഭോക്താവ് വെളിപ്പെടുത്തിയ ആവശ്യങ്ങൾക്കും പ്രതീക്ഷകൾക്കും എതിരായി മനഃപൂർവ്വമോ ഏതെങ്കിലും ഗുരൂ ഉദ്ദേശത്തോടെ സ്വാർഥ താല്പര്യത്തോടെയോ കമ്പനി മനഃപൂർവ്വമായി യാതൊരു ഉൽപ്പന്നത്തെയും പരിപോഷിപ്പിക്കുന്നതല്ല. വിപണനവും നടത്തിപ്പുമായി ബന്ധപ്പെട്ട ഉദ്യോഗസ്ഥന്മാർക്ക് ഇക്കാര്യത്തിൽ ഉചിതമായ പരിശീലനങ്ങളും നിർദ്ദേശങ്ങളും കമ്പനി നൽകുന്നതും അതുവഴി ഉപഭോക്താക്കൾക്ക് തെറ്റിദ്ധാരണ ഉണ്ടാക്കി വിപണനം നടത്തില്ലെന്ന് കമ്പനി ഉറപ്പാക്കുകയും ചെയ്യും.

ii) ലോണിൻമേലുള്ള പലിശയ്ക്ക് കമ്പനി, കൊള്ളപ്പലിശ ഈടാക്കി ലാഭം കൊയ്യുകയോ മാർക്കറ്റിലെ വിപരീത സാഹചര്യങ്ങൾ മുതലെടുക്കുകയോ ചെയ്യുന്നതല്ല. വായ്പയ്ക്ക് ഈടാക്കുന്ന പലിശനിരക്ക് ഫണ്ടിന്റെ ചിലവ്, റിസ്ക് പ്രീമിയം, വായ്പ, സ്കീം ഗ്രാമിന്റെ മുക്തിയിൽ നൽകുന്ന വായ്പ, ലാഭത്തിന്റെ മാർജിൻ മുതലായ മാറാവുന്ന കാര്യങ്ങളിൽ അധിഷ്ഠിതമായിരിക്കും. പലിശനിരക്ക് കാലാകാലങ്ങളിൽ നിലനിൽക്കുന്ന റെഗുലേറ്ററി മാർഗ്ഗ നിർദ്ദേശങ്ങൾ, കമ്പനിയുടെ പലിശനിരക്കിലുള്ള പോളിസി എന്നിവയ്ക്ക് അനുസൃതമായിരിക്കണം. ഇൻഡസ്ട്രിയലിലെ രീതികൾ, ലക്ഷ്യങ്ങൾ, എന്നിവയ്ക്ക് അനുസരിച്ചും ആയിരിക്കണം ഇത്.

iii) വായ്പ സ്കീമുകൾ, പലിശ നിരക്കുകൾ, ഓരോ ഗ്രാമിനും ലഭിക്കുന്ന വായ്പ, ചാർജ്ജുകൾ തുടങ്ങിയവയെ സംബന്ധിച്ച് പൂർണ്ണവും പുതുക്കിയതുമായ വിവരങ്ങൾ കമ്പനിയുടെ വെബ്സൈറ്റിൽ പ്രസിദ്ധീകരിക്കുന്നതാണ്. ഇവ ബ്രാഞ്ചുകളിലും പ്രദർശിപ്പിക്കും. കാലാകാലങ്ങളിൽ കമ്പനിയുടെ മാനേജ്മെന്റ് എടുക്കുന്ന തീരുമാനങ്ങളെ അടിസ്ഥാനമാക്കി വിവിധ മിഡിയ ചാനലുകൾ, പോസ്റ്ററുകൾ, ബ്രോഷറുകൾ, നോട്ടീസുകൾ, ഡിസ്പ്ലേ എന്നിവയിലൂടെയും പൂർണ്ണമായതോ തിരഞ്ഞെടുത്തതോ ആയ വിവരങ്ങൾ ലഭ്യമാക്കുന്നതാണ്.

**III) ക്വട്ടിംഗ് ഈടാക്കൽ, സെക്യൂരിറ്റി വസ്തുക്കൾ തിരികെ കൊടുക്കലും മറ്റു ബാധ്യതകൾക്കായി തടഞ്ഞു വയ്ക്കലും**

i) നല്ല പ്രവർത്തന ചട്ടം എന്ന നിലയിൽ അപ്രതീക്ഷിതമോ, അസാധാരണ സാഹചര്യങ്ങളിലോ, കമ്പനി താല്പര്യങ്ങളെ പ്രതികൂലമായി ബാധിക്കുന്ന സമയത്തോ, അല്ലാതെ യാതൊരു കാരണവശാലും കമ്പനി നൽകിയ വായ്പ തുക മുൻധാരണ പ്രകാരം നിശ്ചയിച്ചിട്ടുള്ള കാലാവധിക്ക് മുമ്പ് തിരികെ ആവശ്യപ്പെടുന്നതല്ല. ഉദാഹരണമായി, സെക്യൂരിറ്റി മൂലം കാര്യമായി കുറഞ്ഞു പോകുന്നതോ, സ്വർണ്ണത്തിന്റെ പരിശുദ്ധി അസ്വീകാര്യമാണെന്നു കാണുകയോ, സർക്കാരിന്റെയോ, മറ്റു നിയന്ത്രണ സംവിധാനങ്ങളുടെയോ നിർദ്ദേശം മൂലമോ മറ്റുമാണ് ഇത്തരം സന്ദർഭങ്ങൾ ഉണ്ടാകുന്നത്. സ്വാഭാവിക കാലാവധിക്ക് മുമ്പ് വായ്പ തുക ആവശ്യപ്പെടുന്ന സന്ദർഭങ്ങളിൽ മതിയായതും യുക്തിസഹജമായതുമായ നോട്ടീസ് ഉപഭോക്താവിന് നൽകിയിരിക്കും.

ii) പണയ ഉരുപ്പടി വിറ്റഴിക്കാതെ തന്നെ ഉപഭോക്താവിനെ ക്വട്ടിംഗ് തിരിച്ചടയ്ക്കാൻ പ്രേരിപ്പിക്കുന്ന തരത്തിൽ മുദ്രവായതോ പ്രേരണാപൂർവ്വമുള്ളതോ ആയ ശ്രമങ്ങൾ കമ്പനി നടത്തും. ക്വട്ടിംഗ് പിരിച്ചടയ്ക്കാനായി കഠിനമായതോ നിർബന്ധപൂർവ്വമായതോ ആയ നടപടികൾ കമ്പനി സ്വീകരിക്കുന്നതല്ല.

iii) ലോൺ അനുവദിച്ച സമയത്ത് ഉണ്ടായിരുന്ന അതേ അവസ്ഥയിൽ തന്നെ ലോൺ തിരിച്ചടയ്ക്കുമ്പോൾ കമ്പനി ഉപഭോക്താവിന് പണയ ഉരുപ്പടി (സ്വർണ്ണം) തിരിച്ചു നൽകും. ജീവനക്കാർ കൈകാര്യം ചെയ്യുമ്പോഴുണ്ടാകുന്ന തകരാറുമൂലം പണയ ഉരുപ്പടി (സ്വർണ്ണം) ക്ക് എന്തെങ്കിലും കേടുപാടുകൾ സംഭവിച്ചാൽ ഓരോ കേസിലെയും അടിസ്ഥാനമാക്കി കമ്പനി സ്വന്തം ചിലവിൽ കേടുപാടുകൾ തീർത്തുകൊടുക്കുകയോ അല്ലെങ്കിൽ ഉപഭോക്താവിന് ന്യായമായ നഷ്ടപരിഹാരം നൽകുകയോ ചെയ്യും. കമ്പനിയുടെ കസ്റ്റഡിയിൽ വരുന്നതിനു മുമ്പ് വായ്പ അനുവദിക്കുന്ന സമയത്ത് പണയ ഉരുപ്പടിക്ക് (സ്വർണ്ണം) തകരാർ ഉണ്ടാകാതെ ഇക്കാര്യം അനുമതി പത്രത്തിൽ (പണയ ടിക്കറ്റ്) കാണിച്ചിരിക്കും.

iv) വായ്പ ഇടപാട് അവസാനിപ്പിക്കുന്ന സന്ദർഭത്തിൽ ഏതു സമയത്തും, അധിക പണത്തിന്മേലോ ഈടാക്കലോ നിയമപരമായ അവകാശം കമ്പനിക്ക് ഉണ്ടായിരിക്കുന്നതാണ് അങ്ങനെ കമ്പനിക്കുള്ള അവകാശം, ഉപഭോക്താവ് എന്ന നിലയിലോ ജാമ്യക്കാരൻ എന്ന നിലയിലോ ക്വട്ടിംഗ് ഉണ്ടാകുന്ന സന്ദർഭത്തിൽ മാത്രം കമ്പനിക്ക് ഉണ്ടായിരിക്കുന്നതും ഉപഭോക്താവിനെ രേഖാമൂലം വ്യക്തമായ രീതിയിൽ അറിയിച്ച ശേഷം മാത്രം അവകാശം സ്ഥാപിക്കുന്നതാണ്.

v) ഏത് തുക അടയ്ക്കുമ്പോഴും ഉടൻ തന്നെ ഒപ്പിട്ട രസീതി നൽകുന്നതും അത് സാധാരണ നിലയിൽ കമ്പ്യൂട്ടർ തയ്യാറാക്കിയ രസീത് ആയിരിക്കുന്നതാണ്. ചെക്കോ, ഡ്രാഫ്റ്റ്, ഇലക്ട്രോണിക് ട്രാൻസ്ഫെറോ ആയി കമ്പനി തുക സ്വീകരിക്കുന്നതായിരിക്കും. എന്നാൽ അത്തരം സന്ദർഭങ്ങളിൽ തുക കമ്പനിയിൽ എത്തി എന്ന് ഉറപ്പാക്കിയ ശേഷം മാത്രം ജാമ്യവസ്തു (സ്വർണ്ണം) തിരികെ കൊടുക്കുന്നതാണ്.

vi) വായ്പ അനുമതി പത്രത്തിൽ (പണയ ടിക്കറ്റ്) വായ്പയുടെ ബാധകമായ ഏല്ലാ നിബന്ധനകളും അടങ്ങിയിരിക്കുന്നുവെങ്കിലും പലിശ, മുതൽ എന്നിവ തിരിച്ചടക്കേണ്ട തീയതിയെക്കുറിച്ച് അറിയിക്കാനായി കമ്പനി ഉപദേശങ്ങൾ, റിമൈൻഡറുകൾ എന്നിവ അയയ്ക്കാനായി ശ്രമം ചെലുത്തുന്നതാണ്. കത്തുകൾ, കൊറിയർ സർവ്വീസ്, ടെലിഫോൺ, എസ്.എം.എസ് എന്നിവ വഴിയാണ് ഇത് അയയ്ക്കുക.

vii) ലോൺ നിലവിലിരിക്കുന്ന സമയത്തോ അത് ക്ലോസ് ചെയ്യുമ്പോഴോ, ഉപഭോക്താവോ അദ്ദേഹം അധികാരപ്പെടുത്തിയ പ്രതിനിധിയോ ആവശ്യപ്പെടുകയാണെങ്കിൽ ലോണിന്റെ സ്റ്റേറ്റ്മെന്റ് നൽകുന്നതാണ്. അക്കൗണ്ട് ക്ലോസ് ചെയ്ത് 30 കലണ്ടർ ദിവസങ്ങൾക്കുശേഷമാണ് അത്തരം ആവശ്യങ്ങൾ ഉന്നയിക്കുന്നതെങ്കിൽ കമ്പനിയുടെ വിവേചനാധികാരം ഉപയോഗപ്പെടുത്തി ന്യായമായ പ്രോസസിംഗ് ചാർജ്ജുകൾ ഈടാക്കാവുന്നതാണ്.

viii) ഏറ്റവും അവസാന മാർഗ്ഗം എന്ന നിലയിൽ മാത്രമേ കമ്പനി പണയ ഉരുപ്പടി (സ്വർണ്ണം) വിൽക്കുകയുള്ളൂ. അതും, ക്വട്ടിംഗ് തുക തിരിച്ചടയ്ക്കാനായി ആവശ്യത്തിന് മുന്നറിയിപ്പ് നൽകിയതിനു ശേഷം മാത്രം. അത്തരം മുന്നറിയിപ്പ് അനുമതി പത്രത്തിൽ (പണയ ടിക്കറ്റ്) പറഞ്ഞിരിക്കുന്ന നിബന്ധനകളും വ്യവസ്ഥകളും പ്രകാരമായിരിക്കും. കൂടാതെ ബാധകമായ നിയമങ്ങളും റെഗുലേറ്ററി മാർഗ്ഗനിർദ്ദേശങ്ങളും അനുസരിച്ചായിരിക്കും. പണയ ഉരുപ്പടി (സ്വർണ്ണം) വിൽക്കുന്നത് പൊതു ലേലത്തിലൂടെയായിരിക്കും. പലിശയും മറ്റു ചാർജ്ജുകളുമടക്കം ലോൺ അക്കൗണ്ട് ക്ലോസ് ചെയ്യുവാനായി കമ്പനി അറിയിപ്പ് നൽകിയിട്ടും ഉപഭോക്താവ് വേണ്ടരീതിയിൽ പ്രതികരിക്കാതിരുന്നാലാണ് ഇപ്രകാരം ചെയ്യുക.

ix) വായ്പ അപേക്ഷയിലും വായ്പ അനുമതി പത്രത്തിലും (പണയ ടിക്കറ്റ്) കമ്പനിയുടെ മേൽ ചുമത്തപ്പെട്ട അധികാരങ്ങൾ ഉപയോഗിച്ച് സാധാരണ കാലയളവിനും മുമ്പ് സെക്യൂരിറ്റി വിറ്റഴിക്കാനോ തീരുമാനിക്കപ്പെടുന്ന പക്ഷം, ക്വട്ടിംഗ് ഈടാക്കാൻ ആരംഭിക്കുന്നതിനു മുമ്പുതന്നെ മതിയായ മുന്നറിയിപ്പ് ഉപഭോക്താവിന് നൽകുന്നതാണ്.

x) ഏല്ലാ ക്വട്ടിംഗ് കമ്പ്യൂട്ടറും പൂർണ്ണമായും തീർത്തു കഴിഞ്ഞാലുടനെ ഉപഭോക്താവ് സെക്യൂരിറ്റി തിരിച്ചടയ്ക്കണമെന്നാണ് കമ്പനി ആഗ്രഹിക്കുന്നതും അതാണ് പ്രോത്സാഹിപ്പിക്കുന്നതും. എന്നിരുന്നാലും ചില അത്യപൂർവ്വ സാഹചര്യങ്ങളിൽ വായ്പ അടച്ചു തീർന്നാലും കമ്പനിയുടെ തകരാറുമൂലമല്ലാതെ തന്നെ പണയ ഉരുപ്പടി (സ്വർണ്ണം) തിരിച്ചടയ്ക്കാൻ ഉപഭോക്താവിന് കഴിയാതെ വരാം. അത്തരം സാഹചര്യങ്ങളിൽ ന്യായമായ സുരക്ഷിത കസ്റ്റഡി ചാർജ്ജ് ഈടാക്കുന്നതാണ്. ഇത് ഉപഭോക്താക്കളെ യഥാസമയം അറിയിക്കുകയും ബ്രാഞ്ച് പരിസരത്തും

കമ്പനിയുടെ വെബ്സൈറ്റിലും പ്രദർശിപ്പിക്കുകയും ചെയ്യുന്നതാണ്.

xi) വായ്പയെ സംബന്ധിച്ച വ്യവസ്ഥകളെയും നിബന്ധനകളെയും സംബന്ധിച്ച കാര്യങ്ങൾക്കല്ലാതെ ഉപഭോക്താവിന്റെ കാര്യങ്ങളിൽ കമ്പനി ഇടപെടുന്നതല്ലെന്നും, എന്നാൽ ഇടപാട് സമയത്ത് ഉപഭോക്താവ് നൽകിയ വിവരങ്ങളും വെളിപ്പെടുത്തലുകളും മതിയായതല്ലാത്തതും കളവാ യതമാണ് എങ്കിൽ ആയതിന് നിർബന്ധിതനായേക്കാവുന്നതുമാണ്.

**IV ) ഉപഭോക്താക്കൾക്കുള്ള സേവനവും പരാതി പരിഹാരവും**

i) ഉപഭോക്താക്കളുടെ പരാതികളും ആവലാതികളും പരമാവധി കുറഞ്ഞതിനും ഒഴിവാക്കുന്നതിനും ആവശ്യമായ നടപടികൾ കമ്പനി നടപ്പാ ക്കുന്നതാണ്.

ii) ഈടായി വെച്ചിട്ടുള്ള ഉരുപ്പികൾ വായ്പ അനുവദിച്ച ബ്രാഞ്ചിൽ നിന്ന് മാത്രമേ തിരിച്ചെടുക്കാൻ കഴിയുകയുള്ളൂ എന്ന നിബന്ധനയോടെ വായ്പാ തുക മുഴുവനായോ ഭാഗികമായോ കമ്പനിയുടെ ഏത് ശാഖകളിലും അടയ്ക്കുന്നതിന് ഉപഭോക്താവിന് സൗകര്യം ഉണ്ടായിരിക്കുന്നതാ ണ്.

iii) ഫലപ്രദമായ ഉപഭോക്താവ് പരാതി പരിഹാര സംവിധാനം കമ്പനി നടപ്പിലാക്കുന്നതാണ്. ഇതിന്റെ വിശദവിവരങ്ങൾ വെബ്സൈറ്റിലും എല്ലാ ശാഖകളിലും പ്രദർശിപ്പിക്കുന്നതാണ്. ഈ സംവിധാനത്തിൽ പരാതി രജിസ്റ്റർ ചെയ്യാവുന്ന ഉദ്യോഗസ്ഥരുടെ പേരുകൾ, തപാൽ മേ ൽവിലാസം, ടെലിഫോൺ നമ്പറുകൾ, ഇ-മെയിൽ വിലാസം, എസ്കലേഷൻ മാട്രിക്സ്, പരാതി ലഭിച്ചതായി അറിയിപ്പ് നൽകേണ്ട സമ യപരിധി, പരാതി കൈകാര്യം ചെയ്യുവാനുള്ള സമയപരിധി തുടങ്ങിയവ വിശദമായി പ്രദർശിപ്പിക്കുന്നതാണ്. ബിസിനസ്സ് ഇടപാടുകൾ നടക്കു ന്ന എല്ലാ ഓഫീസുകളിലും RBI, തിരുവനന്തപുരത്തിന്റെ പൂർണ്ണമായ സമ്പർക്ക വിവരങ്ങൾ നൽകിയിരിക്കും. RBI, തിരുവനന്തപുരത്തിന്റെ അധികാരപരിധിയിലാണ് കമ്പനിയുടെ ഓഫീസ് സ്ഥിതി ചെയ്യുന്നത് എന്നതിനാലാണിത്. കമ്പനിക്ക് പരാതി ലഭിച്ച ഒരു മാസത്തിനുള്ളി ൽ അവിടുന്ന് പരിഹാരമാകുന്നില്ലെങ്കിൽ ഉപഭോക്താവിന് നേരിട്ട് RBI യെ സമീപിക്കാവുന്നതാണ്.

iv) ഉപഭോക്താക്കളോട് കമ്പനി ഉദ്യോഗസ്ഥർ സൗഹൃദത്തോടെ പെരുമാറുന്നുവെന്നും മോശമായി പെരുമാറാതിരിക്കാനും മര്യാദയില്ലാത്ത തും നീതിരഹിതവുമായ പെരുമാറ്റങ്ങൾ കമ്പനി ഉദ്യോഗസ്ഥരിൽ നിന്നും ഉണ്ടാകരുത് എന്ന് ഉറപ്പു വരുത്തുന്നതിനുമായി കാര്യക്ഷമമായ പരിശീലന പരിപാടി കമ്പനി നടപ്പിലാക്കുന്നതാണ്.

v) വിവിധ ഇടപാടുകൾ നടത്താനും പൂർത്തിയാക്കാനും ആവശ്യമായ സമയത്തെക്കുറിച്ചുള്ള നിയമങ്ങൾ കമ്പനി ഉണ്ടാക്കുന്നതും പ്രദർശിപ്പിക്കുന്നതുമാണ്.

vi) ഉപഭോക്താക്കളോട് കമ്പനി സഹതാപപൂർണ്ണമായ സമീപനമായിരിക്കും പുലർത്തുക. പ്രത്യേകിച്ചും പാവപ്പെട്ടവരോടും, സവിശേഷാധി കാരങ്ങൾ ഒന്നും തന്നെയില്ലാത്തവരോടും.

**V ) സെക്യൂരിറ്റി വീണ്ടും കൈവശത്തിലാക്കൽ (ക്രമേഴ്സുൽ വാഹനങ്ങൾ)**

i) തിരിച്ചടവിൽ വീഴ്ച വരുത്തുകയോ, മറ്റേതെങ്കിലും തരത്തിലുള്ള വീഴ്ച ഉണ്ടാകുകയോ ചെയ്താൽ ലോൺ എഗ്രിമെന്റിൽ നിഷ്കർഷിച്ചിട്ടുള്ള നിയമങ്ങളും വ്യവസ്ഥകളും പ്രകാരം കടശ്ശിക തിരിച്ചു പിടിക്കുന്നതിന് വേണ്ടി ജാമ്യം നടപ്പിലാക്കുവാനുള്ള അവകാശം കമ്പനിക്ക് ഉണ്ടായി രിക്കും. ലോണുകൾ തിരിച്ചു പിടിക്കുന്ന സന്ദർഭത്തിൽ കടം വാങ്ങിയവരെ അസമയങ്ങളിൽ ബുദ്ധിമുട്ടിക്കുകയോ ലോൺ തിരിച്ചു പിടിക്കുവാ ൽ ബലപ്രയോഗം നടത്തുകയോ പോലുള്ള അനാചിതമായ ശല്യപ്പെടുത്തലുകൾക്ക് കമ്പനി മുതിരുകയില്ല.

ii) വായ്പ കരാറിൽ പറഞ്ഞിട്ടുള്ള നിയമങ്ങളിലും നിബന്ധനകളിലും വ്യവസ്ഥ ചെയ്തിട്ടുള്ളത് പ്രകാരം അല്ലാതെ, കടം വാങ്ങിയ ആൾ വെളി പ്പെടുത്തിയിട്ടില്ലാത്ത പുതിയ വിവരങ്ങൾ കമ്പനിയുടെ ശ്രദ്ധയിൽ വരുന്നില്ല എങ്കിൽ, കടം വാങ്ങിയ ആളുടെ കാര്യങ്ങളിൽ ഇടപെടുന്നതിൽ നിന്നും കമ്പനി വിട്ടു നിൽക്കുന്നതായിരിക്കും.

iii) വായ്പ കൊടുക്കുന്നതിന്റെ കാര്യത്തിൽ കമ്പനി ലിംഗം, ജാതി, മതം, എന്നിവയുടെ അടിസ്ഥാനത്തിൽ യാതൊരു വിവേചനവും കാണിക്കു കയില്ല.

iv) കടം വാങ്ങുന്ന ആളുടെ അക്കൗണ്ട് ട്രാൻസ്ഫർ ചെയ്യുന്നതിനെപ്പറ്റി, കടം വാങ്ങുന്ന ആളിൽ നിന്നോ, അക്കൗണ്ട് ടേക്ക് ഓവർ ചെയ്യുവാൻ ഉദ്ദേശിക്കുന്ന ബാങ്കിൽ നിന്നോ/ബാങ്കിങ് ഇതര ഫൈനാൻസ് കമ്പനിയിൽ നിന്നോ അപേക്ഷ ലഭിച്ചാൽ സമ്മതമോ മറ്റു തരത്തിലുള്ള പ്ര തികരണമോ അതായത് കമ്പനിയുടെ എതിർപ്പ് ഉണ്ടെങ്കിൽ അതോ അപേക്ഷ കൈപ്പറ്റി 21 ദിവസത്തിനകം അറിയിക്കുന്നതാണ്.

v) സെക്യൂരിറ്റി വീണ്ടും കൈവശത്തിലാക്കൽ കടശ്ശിക തിരിച്ചു പിടിക്കുവാൻ ഉദ്ദേശിച്ചുള്ളതാണ്. കടം വാങ്ങിയ ആൾക്ക് സെക്യൂരിറ്റി നഷ്ട മാക്കുക എന്ന ഉദ്ദേശ്യത്തോടെ അല്ല. സെക്യൂരിറ്റി കൈവശം വീണ്ടെടുക്കൽ പ്രക്രിയകളിൽ സമുചിത നടപടികളിലൂടെ സെക്യൂരിറ്റി കൈവശം എടുക്കൽ, സെക്യൂരിറ്റിക്ക് വിലയിടൽ, സെക്യൂരിറ്റി വസൂലാക്കൽ എന്നിവ ഉൾപ്പെടുന്നു. ഇവയെല്ലാം ന്യായയുക്തവും സുതാര്യവുമായ രീതിയിൽ നടത്തുന്നതാണ്. ശരിയായ നോട്ടീസുകൾ നൽകി മാത്രമേ വീണ്ടും കൈവശത്തിലാക്കൽ നടത്തുകയുള്ളൂ. സെക്യൂരിറ്റി വീണ്ടും കൈവശത്തി ലെടുക്കുമ്പോൾ യഥാവിധി നിയമ പ്രകൃതി വഴി മാത്രമേ ചെയ്യുകയുള്ളൂ. കൈവശം ഏറ്റെടുത്ത ശേഷം കൊലാറ്ററിന്റെ സുരക്ഷിതത്വം ഉറപ്പു വരുത്തുന്നതിന്, ബിസിനസ്സിന്റെ സാധാരണ നടത്തിപ്പിന്റെ ഭാഗമായി കമ്പനി യുക്തിസഹജമായ എല്ലാ ശ്രമവും നൽകുന്നതാണ്.

vi) സമുചിതമായ ഒരു പരാതി പരിഹാര സംവിധാനം നടപ്പിലാക്കും. അതുവഴി കമ്പനിയുടെ ഉദ്യോഗസ്ഥരുടെ തീരുമാനങ്ങളിൽ നിന്നും ഉത്ഭവിക്കുന്ന തർക്കങ്ങൾ കേൾക്കുകയും തീർപ്പു കൽപ്പിക്കുകയും ചെയ്യുന്നതാണ്.

**VI ) മറ്റു കാര്യങ്ങൾ**

i) സാധാരണ ബിസിനസ്സ് സമയം, അവധി ദിവസങ്ങളുടെ ലിസ്റ്റ് എന്നിവ കമ്പനിയിൽ പ്രദർശിപ്പിച്ചിരിക്കും. എന്തെങ്കിലും മാറ്റങ്ങൾ ഉണ്ടെ ക്കിൽ അവ ശാഖാ പരിസരത്ത് പ്രദർശിപ്പിച്ചിരിക്കുന്ന നോട്ടീസിലൂടെയോ പത്രക്കുറിപ്പിലൂടെയോ അറിയിക്കും.

ii) ഉപഭോക്താക്കളുടെ വ്യക്തിപരമായ വിവരങ്ങൾ യാതൊരു കാരണവശാലും അനർഹരായ ആൾക്കാരെക്കോ, സ്ഥാപനങ്ങൾക്കോ മുന്നാമത് കക്ഷികൾക്കോ കമ്പനി നൽകുന്നതല്ല. എന്നാൽ ഏതെങ്കിലും നിയമപരമായ കാര്യങ്ങൾക്കുവേണ്ടി നിയമ വിധേയമായി ആവശ്യപ്പെടുന്ന പക്ഷം ഉപഭോക്താവിന് നോട്ടീസ് നൽകാതെ തന്നെ ആയതു നൽകുന്നതിന് കമ്പനി ബാധ്യസ്ഥനായിരിക്കുന്നതാണ്.

iii) കമ്പനി അതിന്റെ ശാഖകൾ വഴി ലോക്കർ സൗകര്യം നൽകിയിട്ടുള്ള സ്ഥലങ്ങളിലെല്ലാം പ്രസ്തുത പ്രവർത്തനം റിസർവ്വ് ബാങ്കിന്റെ നിയ ത്രണത്തിൽ കീഴിലുള്ളതല്ലെന്ന് ഉപഭോക്താവിനെ/ഉപഭോക്താക്കളെ അറിയിക്കുവാൻ സമുചിതമായ വെളിപ്പെടുത്തൽ നടത്തിയിട്ടുണ്ടെന്ന് ഉറപ്പു വരുത്തും.

**ഭേദഗതികൾ :**

ലോക്കർ സൗകര്യത്തെപ്പറ്റി പോയിന്റ് D(V) ചേർക്കൽ - റിപൊസഷൻ ഓഫ് സെക്യൂരിറ്റി ആൻഡ് D(VI) (iii) 12 ഫെബ്രുവരി 2016 ലെ ബോർഡ് മീറ്റിങ്ങിൽ അംഗീകരിച്ചതു പ്രകാരം.



**JEWEL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies the FPC guidelines to be followed branches/all offices.

**FAIR PRACTICE CODE**

**1. Name:**

These guidelines may be called “Fair Practice Code -2023-24”

**2. Effective Date**

They shall come into force on 01<sup>st</sup> April, 2023.

**3. Applicability:**

This code shall be applicable all over the company business activities.

\*\*\*\*\*

**A. PREAMBLE /INTRODUCTION**

The Fair Practice Code (FPC) has been formulated by JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED in response to guidelines issued by Reserve Bank of India vide circular DNBS.CC.PD. No.266 / 03.10.01 / 2011-12 dated 26 March, 2012 titled “Guidelines on Fair Practices Code for NBFCs” replacing the existing code posted on the Company’s website.

The FPC will be applicable to all the offices of the Company including the Head Office, Thrissur, Kerala, the Regional Offices located in various Centers and the Branches located across Kerala. The FPC shall be binding on all the employees and officers of the Company.

**B OBJECTIVES**

The objectives of the FPC are as under:

- (i) Adopt the best practices in dealings with customers.
- (ii) Set challenging benchmarks and strive to achieve high operating standards for ensuring customer satisfaction.
- (iii) Follow transparent, fair, ethical and legally tenable practices while conducting business.
- (iv) Provide all necessary information and inputs to customers / prospective customers and promote a mutually beneficial long-term relationship.

- (v) Facilitate a continuously growing base of satisfied customers while scrupulously avoiding acquisition of customers having doubtful credentials or criminal background.

## **C DECLARATIONS & COMMITMENTS**

- (i) The Company undertakes to abide by all applicable laws, regulations and guidelines passed / issued by the Regulators (Reserve Bank of India, SEBI, IRDA etc.) and other competent authorities such as Government, Local Authority etc.
- (ii) The Company commits itself to full customer satisfaction through efficient, professional and courteous services across all its offices.
- (iii) The Company shall consistently strive to meet with and improve upon the internally set benchmarks and practices and be ahead of the standards prevalent in the industry.
- (iv) The Company undertakes not discriminate customers on grounds of religion, caste, gender or language.
- (v) The Company will provide clear and full information about its products and services to its customers / prospective customers and will not resort to any misleading or potentially misguiding advertisement or publicity.
- (vi) The Company undertakes to desist from introducing any products / services having elements of 'hidden charges or lack of transparency.
- (vii) The Company will communicate in the local language with the customer and in English at the request of the customer
- (viii) The Company undertakes to take all possible and reasonable measures to secure the safe custody of the security pledged by the customer and to compensate the customer for any accidental, inadvertent or fraudulent loss of the security whilst in the custody of the Company.
- (ix) The Company undertakes not to take advantage of any unintentional or clerical error made by the customer while transacting business.
- (x) The Company is committed to put in place a system for promptly addressing complaints and suggestions of the customers supplemented with a structured Grievance Redressal Mechanism having an escalation matrix.
- (xi) The Company shall display the FPC on its website and also make available to the Customer, on request, a copy of the FPC on demand.

## **D) FAIR PRACTICES**

- (i) LOANS, TERMS & CONDITIONS, INTEREST RATE & CHARGES
- (ii) The Company shall make available loan application forms in local language to all prospective customers free of cost at the concerned branches mentioning also the supporting documents to be submitted along with. An acknowledgement for receipt of duly completed loan application forms will be given to the customer in all cases. As a matter of policy and customer service loan applications are sanctioned / rejected immediately. Disbursement of the loan and acceptance of security will be carried out nearly simultaneously.

- (iii) The Company shall disclose all relevant information relating to a loan / product such as eligible loan amount, interest rate, charges, penal/overdue interest, interest calculation methodology, rebate on interest etc. before sanction of the loan to enable the customer / prospective customer to take an informed decision. The Customer / prospective customer will also be provided, on request, the detailed terms and conditions of the loan before sanction.
- (iv) The Company shall ensure that a loan sanction letter (pawn ticket) is given to the customer containing all the terms and conditions governing the loan facility in the local language or other language understood by the customer. The loan sanction letter (pawn ticket) will also mention the loan amount, loan account number, interest rate, charges, loan processing fees etc. The loan sanction letter (pawn ticket) which will bear the signature of the authorized official of the company will also serve as a receipt for the security (gold) pledged at the branch by the customer.
- (v) The Company shall not in the normal course make any changes / modifications in the terms and conditions of the loan, including rate of interest, which could adversely affect the customer financially or otherwise. In abnormal circumstances when such changes / modifications are inevitable, keeping in view the new circumstances, adequate and proper notice shall be given to the customer about any such change/modification.

## **(II) MARKETING & PROMOTION**

- i. The Company shall not deliberately promote a product with any ulterior / selfish motives or contrary to the customer requirements or expectations as disclosed by the customer. The Company will ensure that its personnel engaged in marketing and operations are suitably trained and instructed so as to preclude selling of its products by misrepresentation to the customer / prospective customer.
- ii. The Company will not indulge in profiteering by charging usurious rates of interest on loans or take undue advantage of adverse market conditions. The rates of interest will be based on variables such as cost of funds, risk premium, loan scheme, loan per gram, profit margin etc. and shall be in conformity with the Interest Rate policy of the Company and Regulatory Guidelines from time to time. It shall also, by and large, be in tune with industry practices and benchmarks.
- iii. Full and updated information regarding loan schemes, rate of interest, loan per gram, charges etc. will be displayed on the website of the Company and also displayed in the branches. Complete or select information will also be made available through various media channels, posters, brochures, notices, displays etc. based on the decisions of the management of the Company from time to time.

## **(III) RECOVERY OF DUES, EXERCISE OF LIEN & DELIVERY OF SECURITY**

- i. The Company will not, as a matter of fair dealing, normally recall the loan before the initially agreed tenure except in unanticipated or abnormal circumstances where the Company's interests are adversely affected e.g. when the security value diminishes substantially, when the quality of gold is not found to be acceptable, due to any regulatory / government directives etc. In all such cases proper and reasonable notice shall be given to the customer recalling the loan before expiry of the normal tenure.
- ii. The Company will make all possible soft or persuasive efforts to get the customer to repay the dues without resorting to disposal of the security. The Company does



not accept nor will it encourage the use any coercive or hard measures to recover its dues from the customer.

- iii. The Company will deliver the security (gold) to the customer immediately upon settlement of the loan in the same condition as was at the time of sanction of the loan. In case of any damage caused to the security (gold) due to mishandling by its employees, the Company shall at its cost get the damage repaired or alternately pay reasonable compensation to the customer on a case to case basis. If the security (gold) has signs of damage thereon, before being taken custody of by the Company at the time of sanction of loan, the fact will be briefly incorporated in the sanction letter (pawn ticket).
- iv. The Company will exercise only legitimate right of lien over the pledged security or such cash surplus as may arise upon settlement of existing loans at any time. Such right of lien shall arise only if the customer has any other dues, either directly or as guarantor, and will be subject to proper intimation of such right of lien being given to the customer by the Company.
- v. The Company shall issue a signed and, normally, a system generated receipt for all cash payments made by the customer immediately. The Company shall also accept payments vide cheques, demand drafts, electronic transfers etc. subject to the condition that return of the security (gold) will be made only after confirmation of realization.
- vi. Even though the loan sanction letter (pawn ticket) contains all applicable terms and conditions of the loan the Company shall, nevertheless, endeavour, on a best effort basis, to send advices, reminders etc. regarding due date for payment of interest, principal etc. by letter, courier service, telephone , SMS etc.
- vii. The Company shall, on demand, provide the customer or his duly authorized representative with a statement of the loan account at any time during the currency of the loan or immediately upon closure. However, the Company may, at its discretion, require payment of reasonable processing charges by the customer for providing statement of account if such demand is made 30 calendar days after closure of the account.
- viii. The Company will resort to disposal of security (gold) only as a last resort and that too after adequate and proper notice is served on the customer to repay the dues. Such notice will be as per the terms contained in the sanction letter (pawn ticket) and also in compliance with applicable laws and regulatory guidelines. The disposal of the security (gold) will be taken up through public auction when the customer does not positively respond to the communications sent by the Company to close the loan account along with interest and other charges.
- ix. Where the Company proposes to dispose of the security even before the normal tenure of the loan based on the rights conferred on the Company vide loan application and loan sanction letter (pawn ticket) adequate and proper notice will be served on the customer before such action is initiated for recovery of dues.
- x. The Company prefers and encourages customers to take back delivery of the security immediately upon full settlement of all dues. However, should there be exceptional instance of the Customer being unable to take delivery of the security (gold), not attributable to the inability of the Company, after closure of the loan account reasonable safe custody charges may be payable which will be duly

advised to the customer or displayed in the branch premises and the Company's website.

- xi. The Company will not interfere in the affairs of the customers except for the purposes mentioned in the terms & conditions of the loan or when constrained to do so due to inadequate or false disclosures made by the borrower at the time of putting through the transactions.

**(IV) CUSTOMER SERVICE & GRIEVANCE REDRESSAL**

- i. The Company will implement all possible steps to prevent and minimize customer complaints / grievances
- ii. The Company will facilitate the customer to pay the whole or part of the dues at any of the branches of the Company subject to the condition that delivery of the pledged security shall be made only at the branch where loan was originally disbursed.
- iii. The Company will put in place an effective Customer Grievance Redressal mechanism details of which will be displayed on the website and in all the branches. The mechanism will specify inter alia the names & designations of the officials with whom complaints can be registered, their postal address / telephone numbers/ email address, escalation matrix, time limit for acknowledging receipt of complaint, time limit for dealing with the complaint etc. It will also put in place at all offices where business is transacted, the complete contact details of the Regional Office of RBI, Thiruvananthapuram, within whose jurisdiction the registered office of the company is situated, so that the customers may directly approach the RBI in case their grievances are not redressed within one month of the receipt of complaints by the company”
- iv. The Company will put in place an effective training system to ensure that employees of the Company are customer friendly and do not resort to rude, inappropriate or unethical behaviour.
- v. The Company will endeavor to work out and display the time norms for putting through and completing the various transactions.
- vi. The Company will have a sympathetic approach to the problems faced by the customer especially the poor and underprivileged sections.

**(V) REPOSSESSION OF SECURITY (COMMERCIAL VEHICLES)**

- i. The Company reserves the right to enforce security for recovery of dues on the terms and conditions stipulated in the loan agreement in case of default in payment or on the occurrence of any other event of default. During recovery of loans, the Company will not resort to undue harassment like bothering the borrowers at odd hours or use of force for recovery of loans.
- ii. The Company would refrain from intervening in the affairs of the borrowers except as provided in the terms and conditions mentioned in the loan agreement, unless new information, not disclosed by the borrower, has come to the notice of the Company.
- iii. The Company would not discriminate on grounds of sex, caste and religion in the matter of lending.

- iv. In case of receipt of request for transfer of borrower account, either from the borrower or from a bank/non-banking finance company, which proposes to take over the account, the consent or otherwise i.e. objection of the Company, if any, would be conveyed within 21 days from the date of receipt of request.
- v. Repossession of security is aimed at recovery of dues and not to deprive the borrower of the security. The recovery process through repossession of security will involve repossession, valuation of security and realization of security, through appropriate means. All these would be carried out in a fair and transparent manner. Repossession will be done only after issuing proper notices. Due process of law will be followed while taking repossession of the security. The Company will take all reasonable care for ensuring the safety and security of the collateral after taking custody, in the ordinary course of the business
- vi. An appropriate grievance redressal mechanism would be put in place whereby disputes arising out of the decisions of Company's functionaries would be heard and disposed off.

**(VI) MISCELLANEOUS**

- i. The Company shall display the normal business hours at the respective branches, the list of holidays and notify the changes, if any, by way of a notice displayed in the premises of the branch or through press notification.
- ii. Personal information of the customer will not be shared with unauthorized persons or agencies or third parties by the Company. However, the Company will be bound to honour and comply with legal or regulatory requirements, if any, in this matter obligating it to part with such information even without notice to the customer.
- iii. Wherever locker facility is extended by the Company through its branches, it shall be ensured that appropriate disclosure are in place to communicate to the customers that the activity is not regulated by the Reserve Bank.

**Amendments:**

- 1. Insertion of Point D(V)-Repossession of security and D(VI)(iii) regarding locker facility as approved in the Board meeting dated 12th February, 2016.

BY THE ORDER OF THE BOARD

For JEWEL ROCK HIRE PURCHASE  
AND LEASING PRIVATE LIMITED

Director

---

**CC:**

- 1. Legal Department
- 2. Administration Department
- 3. HR Department

Dated this the 01<sup>st</sup> Day of April, 2023



**JEWEL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies the guidelines to be while fixing the interest rates of the loan products and services of the company.

**INTEREST RATE POLICY**

**1. Name:**

These guidelines may be called in Interest Rate Policy – 2023-24

**2. Effective Date**

They shall come into force on 01<sup>st</sup> April, 2023.

**3. Applicability:**

This policy is applicable to all loans sanctioned by the company

---

**OBJECTIVE**

The Company has been following certain procedures and practices in the matter of fixing interest rates on gold loans (assets) and NCDs/Subordinated Bonds (liabilities). Interest rates are not controlled by the Reserve Bank of India. However, RBI has vided circular DNBS. CC.PD. No .266/03.10.01/2011-12 dated 26 March 2012 (Guidelines on Fair Practices Code for NBFCs) directed NBFCs to have a documented Interest Rate Policy / Model approved by the Board of Directors which would lay down internal principles and procedures in determining interest rates and other charges on the loan products offered by NBFCs. The specific points referred to in the above referred RBI circular are:

1. Charging of excessive interest rates by NBFCs.
2. The need for adoption of an interest rate model along with approach for gradations of risk & rationale for charging differential rates.
3. Disclosure of rates of interest rates, changes thereof and publicity thereto.
4. Adoption of annualized rates of interest while dealing with customers.

**The main objectives of the interest rate policy are to:**

1. Ensure that interest rates are determined in a manner as to ensure long term sustainability of business by taking into account the interests of all stakeholders,
2. Develop and adopt a suitable model for calculation of a reference rate.

3. Enable fixation of interest rates which are reasonable: both actual and perceived.
4. Ensure that computation of interest is accurate, fair and transparent in line with regulatory expectations and market practices.
5. Charge differential rates of interest linked to the risk factors as applicable.
6. Facilitate transition to income recognition norms that may be stipulated by RBI in future and adoption of best practices.

## **DETAILS OF THE POLICY**

### **Methodology for calculation of interest on loan accounts**

The main spirit underlying the methodology is to project a transparent and fair approach to the customers and also be in readiness to adopt the practices now in vogue amongst commercial banks keeping in view the peculiarities of the gold loan business.

- **On the daily balances**  
Interest amount shall be calculated on the daily outstanding balance in the loan account at the applicable rate.
- **Minimum period for which interest chargeable:**  
The minimum period for which interest is payable by the borrower shall not exceed 1 day only. Interest payable / receivable shall be calculated on the actual daily outstanding balance.
- **Basis - number of days per year:**  
Interest shall be calculated based on 360 days a year. Dates of disbursement and closure of account shall both be included for computation of interest.
- **Compounding:**  
Compounding of interest where applicable, as provided in the loan scheme, shall not be at a frequency more than 1 month / 30 days in a year
- **Fixed rate - Floating rate**  
All loans shall be granted at fixed rate only.

### **Annualised rate of interest**

- i) Interest rate quoted shall be on annualized basis only in all documents, internal instructions/ communications and publicity materials (pamphlets, brochures, hoardings, etc)
- ii) Where the rates are mentioned in non-annualized form (e.g., in product promotion) the annualized rate shall also be mentioned along with so as to comply with regulatory requirements and Fair Practices Code,

### **Risk Based Gradation of Interest Rates**

- i) Considering the nature of the loans (collateral valuation being vital) the major inherent risk is the Loan to Value (LTV) or Loan per Gram. Since a higher LTV translates to a higher risk it stands to reason that LTV and Interest rate should be correlated. Accordingly, assuming all other factors to be the same a higher LTV loan should attract a correspondingly higher interest rate as compared with a lower LTV loan.
- ii) The LTV linkage with interest rate shall be at the time of sanction of loan and cannot be changed subsequently due to movements in the overall collateral coverage arising from market movements in gold prices,
- iii) Where substantially low rates of interest are charged on certain / special schemes or in specified regions/areas / branches the maximum amount per borrower shall be appropriately restricted and checks put in place to prevent misuse of the facility. Such schemes shall be periodically reviewed and appropriately modified to meet with the overall objectives of floating such schemes.

### **Maximum/ Ceiling Interest Rate on Loans**

- i) Keeping in view the regulatory (RBI) expectations from NBFCs and also the Fair Practices Code the maximum interest rate chargeable shall be fixed at 26 %\*\* pa across all states / regions excluding compounding effect where applicable under any schemes.
- ii) The above-mentioned ceiling shall be reviewed periodically at quarterly (calendar) intervals or more frequently, as and when required, by the Board of Directors keeping in view regulatory guidelines / directives, intensity of competition in the market, net interest margin target, market rates etc.

### **Penal Interest on overdue loans**

When the loan remains outstanding beyond the 'normal' tenure (Between 3 Months and 1 year) without FULL servicing of interest due penal interest may be charged at a rate not exceeding 3% pa (i.e. at the contracted rate plus 300 basis points) on the amount due and payable. Penal interest provisions shall be calculated and will apply only after the expiry of the 'normal' tenure. Penal interest may be waived, in full or in part, in deserving cases with the reason being recorded by Managing Director on the recommendations of the Executive Director which is at present on recommendation of Deputy General Manager.

### **Rebate on interest**

Schemes offering rebate on the interest rate may also be considered on the ground that customers who regularly service interest payable on loans deserve to be incentivized. The extent of rebate may vary from scheme to scheme but may not exceed 3% pa (300 basis points on the contracted rate). Rebate may be considered at the time of full settlement in cases where interest payable has been serviced by the due dates without any default on all occasions. However, a grace period of 3 calendar days may also be considered and built into the loan scheme.

### **Due date for servicing interest**

Interest will be calculated from the date of disbursement and shall be charged for the day of closure of the account also as per current practice. The due date for payment of interest shall run from the date of disbursement,

### **Structured Products**

Products offered and features thereof shall be straight forward, transparent and simple to understand so as to comply with the letter and spirit of RBI guidelines. Structured products, when introduced, should comply with the basic features of the Interest Rate policy and the FPC. Features of such products, especially the differential features, should be clearly explained to and understood by the prospective borrower before sanction as a matter of fair practice. Operational personnel should be well equipped in this regard.

### **Base Rate and Net Interest Margin**

- i) In order to arrive at a proper basis for arriving at the cost of borrowings / funds / resources a suitably calculated 'base rate' shall be developed keeping in the weighted average cost of borrowings, interest paid on liability products (NCDs / Subordinated Bonds) and return on equity capital. Return on equity capital shall be taken at 15 %, Interest rate on loans shall be based on the 'base rate' so that scope for interest rate mismatches is minimized,
- ii) The base rate shall be calculated at the end of every month and approved by the Board.
- iii) The NIM (Net Interest Margin) shall be calculated over the 'base rate' so calculated to arrive at the lending rate.
- iv) iv) The NIM shall be capped at 14% (1400 basis points) over the 'base rate'.
- v) Lending at or below the 'base rate' shall be done only for short term promotion of business either for a specific loan scheme or specific branch(es) or for lending to poor downtrodden sections.
- vi) Lending at or below the 'base rate' shall not exceed 10% of the total loan portfolio.
- vii) Lending at below the ['base rate' plus operational expenses] shall not exceed 15% of the total loan portfolio.

### **Interest rates on loans against Commercial Vehicles**

1. The Interest rate applicable to each loan account will be assessed based on multiple parameters like tenure, borrower profile, borrowers' repayment capacity based on the cash flows, loan to value of the asset financed, type of collateral security provided by the borrower and past repayment track record of the borrower, etc.

2. The rates of interest for the same product and tenor availed during same period by different customers need not be standardized but could be different for different customers depending upon consideration of any or combination of a few or all factors listed above.
3. The Company shall intimate the borrower loan amount, annualized rate of interest and method of application at the time of sanction of the loan along with the tenure and amount of monthly installment.
4. The company also offers variable and equated monthly installments schemes. Interest would be charged and recovered on monthly basis.
5. The other charges such as processing fees, additional interest charged on delayed payments and cheque bouncing charges are mentioned in the Schedule which is part of the Loan Agreement
6. Other financial charges like pre payment/ foreclosure charges, cheque swaps, cash handling charges, RTGS/ other remittance charges, commitment fees, charges on various other services like issuing NO DUE certificates, NOC, letters ceding charge on assets/ security, security swap & exchange charges, field collection charges etc. would be levied by the company wherever considered necessary. Besides the base charges, the service tax and other cess would be collected at applicable rates from time to time. Any revision in these charges would be with prospective effect.
7. Interest rate models, base lending rate and other charges, and their periodic revisions are made available to our prospective and existing customers through our offices and branches. Prior to entering into an agreement with our customers, we provide them with our statement of charges and interest and address their queries and questions on the same, to their satisfaction. Our loan officers ensure charges and rates of interest are explained clearly and transparently to the people who may be interested in our products.
8. Claims for refund or waiver of charges/ penal interest / additional interest would normally not be entertained by the company and it is at the sole discretion of the company to deal with such requests if any.
9. The maximum interest rate chargeable shall be fixed at 28% p. a. across all states / regions / vehicle categories / borrower categories.

**Other Charges Recovery of Out-of-Pocket Expenses**

1. The Company may also levy other charges such as loan\_processing fees, insurance (of gold ornaments), processing charges for delivery of gold against lost pawn ticket, safe custody charges (due to failure to take delivery of gold ornaments immediately after closure of account), statement of account etc. In addition, the Company shall be entitled to recover costs incurred in connection with postage, legal costs etc. The above charges shall be pegged at reasonable levels and in the spirit of Fair Practice.



2. Guidance Rates are as under

Description of the charges	Extent of charges	Comments
Loan processing, Appraisal charges, Insurance etc.	Will be capped at 1% of the loan amount. A reasonable minimum and maximum in absolute terms may be prescribed.	Segments borrows (i.e. small borrowers), Special schemes may be exempted from such charges.
Delivery against lost Pawn Ticket – processing charges	Between a minimum of Rs 50 and maximum of Rs 250 per pledge	
Safe custody charges – when borrower does not immediately take delivery of the pledged gold ornaments	Between 0.10% to 0.25% per month subject a reasonable minimum and maximum in absolute terms	
Statement of account	Free of cost if demanded within 30 days of closure of account. In other cases a minimum of Rs. 25 and maximum of Rs. 100 per statement	
Postage, Courier charges	As per Existing circular	

3. The actual rates from time to time shall fixed by the board within the band / limits mentioned under each head and reviewed at atleast half yearly intervals.
4. board shall have the authority to implement any other reasonable / justifiable charge from time to time.
5. Taxation regulations as applicable shall be complied with.
6. Discretion to waive / reduce the charges shall be vested with a senior functionary on a case to case basis after suitable delegation of powers is worked out and approved.

**BY THE ORDER OF THE BOARD**

**For JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

- 1. Legal Department**
- 2. Administration Department**
- 3. HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**



**JEWEL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies the guidelines to be followed branches/offices while admitting customers

**KNOW YOUR CUSTOMER (KYC) AND PREVENTION OF MONEY  
LAUNDERING ACTIVITIES POLICY**

**4. Name:**

These guidelines may be called The Know Your Customer (KYC) And Prevention of Money Laundering Activities Policy – 2023-24

**5. Effective Date**

They shall come into force on 01<sup>st</sup> April, 2023.

**6. Applicability:**

This policy is applicable to all loans sanctioned by the company

---

**OBJECTIVE**

The KYC AML policy is framed in line with RBI Direction / Prevention of the Money Laundering Act, 2002 /Rules as amended from time to time.

The KYC policy has been framed by the Company for the following purposes:

1. To prevent criminal elements from using Company for Money Laundering and Terrorist Funding activities;
2. To put in place an effective system and procedure for Customer identification and verifying its / his / her identity and residential address.
3. To enable Company to know and understand its customers and their financial dealings better which, in turn, would help the Company to manage risks prudently;
4. To put in place appropriate controls for detection and reporting of suspicious activities as envisaged under the Anti Money Laundering Act, 2002 and in accordance with laid down procedures;
5. To comply with applicable laws and regulatory guidelines;

## **DEFINITIONS**

- 1) "Customer "means;
  - a) a person who is engaged in a financial transaction or activity with Jewel Rock Hire Purchase and Leasing Private Limited and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
  - b) any other person connected with a financial transaction which can pose significant reputation or other risks to Jewel Rock Hire Purchase and Leasing Private Limited.
  
- 2) "Senior Management"  
Senior Management for the purpose of the policy shall constitute Executive Directors, Managing Director, Deputy General Manager – Business Operations, Managing Director
  
- 3) "Obtaining certified copy of Officially Valid Document (OVD)" – Means comparing the copy of OVD with the original and recording the same on the copy by authorized officer of Jewel Rock Hire Purchase and Leasing Private Limited.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained:

- a) authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- b) branches of overseas banks with whom Indian banks have relationships,
- c) Notary Public abroad,
- d) Court Magistrate,
- e) Judge,
- f) Indian Embassy/Consulate General in the country where the non-resident customer resides.

Certified OVD shall also contain the customer id number and shall be filed carefully for future verification.

## **KEY ELEMENTS OF THE POLICY**

This policy is applicable to all business operations and services, Money Transfer Services, etc and also applicable to business verticals of Jewel Rock Hire Purchase and Leasing Private Limited and it is to be read in conjunction with related operational guidelines issued from time to time.

The policy includes the following key elements:

- 1) Customer Acceptance Policy (CAP)
- 2) Customer Identification Procedures (CIP)
- 3) Monitoring of Transactions
- 4) Risk Management

## **CUSTOMER ACCEPTANCE POLICY (CAP)**

Jewel Rock Hire Purchase and Leasing Private Limited's CAP lays down criteria for acceptance of customers. While taking decision to grant any facilities to the customers as well as during the continuation of any facilities the following norms and procedures will be followed by the company

- a) No account will be opened in anonymous or fictitious/benami name.
- b) Customers will be accepted only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks will be done before opening a new account to ensure that the identity of the Customer does not match with any person with known criminal background or with banned entities.
- c) Jewel Rock Hire Purchase and Leasing Private Limited will refrain from opening an account where the company is unable to apply appropriate Customer Due Diligence (CDD) measures either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- d) No transaction or account-based relationship shall be undertaken without the
- e) Customer Due Diligence procedure (CDD), set out in this policy.  
A Unique Customer Identification Code (UCIC) shall be allotted to new and existing customers. Jewel Rock Hire Purchase and Leasing Private Limited shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of Jewel Rock Hire Purchase and Leasing Private Limited desires to open another account with Jewel Rock Hire Purchase and Leasing Private Limited, there shall be no need for a fresh CDD exercise.

Implementation of CAP should not become too restrictive and result in denial of the JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED 's services to general public, especially those who are financially or socially disadvantaged

## **CUSTOMER IDENTIFICATION PROCEDURE (CIP)**

Customer Identification involves verification of customer's identity by using reliable, independent source documents, data or information. Jewel Rock Hire Purchase and Leasing Private Limited shall obtain enough information necessary to verify the identity of each Customer. A broad guideline for the customer identification is given below:

Jewel Rock Hire Purchase and Leasing Private Limited shall ensure that Customer identification process is undertaken, whenever;

- a) an account-based relationship is being established;
- b) carrying out any international money transfer operations for a person who is not an account holder;
- c) there is doubt about the authenticity or adequacy of customer identification data already obtained. transactions with walk in customers, where the amount involves equal or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

- d) When Jewel Rock Hire Purchase and Leasing Private Limited has reasons to believe that a customer is intentionally Structuring transactions into a series of transactions below the threshold of Rupees Fifty thousand.

### **CUSTOMER DUE DILIGENCE PROCEDURE (CDD) IN CASE OF INDIVIDUALS**

For undertaking CDD, Jewel Rock Hire Purchase and Leasing Private Limited shall obtain the following from an individual while establishing an account-based relationship or while dealing with individual who is a beneficial owner, authorised signatory or power of attorney holder related to any legal entity;

- a. A certified copy of Officially Valid Documents (OVD), as given in Annexure I, containing details of proof of their identity and address;
- b. One recent photograph (For the gold loan customers capturing of photos of the individuals and keeping in the ERP to be continued);
- c. A certified copy of the Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962;
- d. and such other documents pertaining to the nature of business or financial status specified in this policy.

Jewel Rock Hire Purchase and Leasing Private Limited may carry out Offline Verification of customers if they are desirous of undergoing Aadhaar Offline Verification for identification purposes.

Wherever Aadhaar details are collected, it shall be ensured that customers have redacted or blacked out their Aadhaar numbers through appropriate means.

The e-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification, when NBFCs or itself are authorised by RBI to do such verification for establishing account-based relationship.

### **CUSTOMER DUE DILIGENCE BY THIRD PARTY**

In compliance of the KYC regulations, Jewel Rock Hire Purchase and Leasing Private Limited may rely on the customer due diligence done by third parties, which are regulated entities, for verifying identity of customers at the time of commencement of account-based relationship, subject to the following conditions.

- a) Records or information of the customer due diligence carried out by the third party is obtained within 2 days from the third party or from Central KYC Records Registry.
- b) Jewel Rock Hire Purchase and Leasing Private Limited is satisfied those copies of the identification data and other relevant documents relating to the customer due diligence requirements will be available from the third party up on request without delay.

- c) The third party is regulated, supervised or monitored and has capabilities to comply with the customer due diligence and record keeping requirements as prescribed in the Prevention of Money Laundering Act.
- d) The third party shall not be based in a country or jurisdiction assessed as high risk. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable will be that of Jewel Rock Hire Purchase and Leasing Private Limited. (Description of Regulated entities are given in Annexure II)

**SIMPLIFIED PROCEDURES FOR SMALL VALUE GOLD LOANS:**

For customers with aggregate loans below Rs.0.50 lakh, Proof of Identity alone will be sufficient provided the customer gives full and complete address in the loan application form and his telephone number is confirmed by the branches to be correct.

If a person is unable to produce identity documents as mentioned in Annexure I (i.e., any of OVDs), interim / Temporary KYC documents such as Labour card, Civil ID card, Credit Card, Employer Company ID card, LIC card, State ID card, Bank Pass Book, etc. may be accepted subject to the following conditions:

- a. The customer shall provide a self-attested photograph of the customer.
- b. Branch Head shall certify under his/her signature that the customer has affixed his signature or thumb impression in his presence.
- c. The account shall remain operational initially for 12 months, within which the customer must furnish his identity documents for conducting CDD as mentioned in CDD guidelines. Customer shall be suitably informed at the time of starting the relationship
- d. Maximum outstanding shall not exceed Rs 0.50 Lakh in all their accounts taken together at any point of time and the total credit in all the accounts taken together shall not exceed Rs. 1.00 lakh in a year.
- e. The customer shall be made aware that no further transaction will be permitted until full KYC procedure is completed in case of condition no. d. above is breached.
- f. Regularization of Interim/Temporary KYC: In order not to inconvenience the customer, the Jewel Rock Hire Purchase and Leasing Private Limited shall notify the customer when the balance reaches rupees forty thousand (Rs. 40,000/-) or the total credit in a year reaches rupees eighty thousand (Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted and that otherwise the operations in the account will be stopped when the total balance in all the accounts taken together exceeds Rs 0.50 Lakh at any point of time or the total credit in the accounts in year exceeds Rs 1.00 Lakh.

KYC verification once done by one branch shall be valid for transfer of account to any other branch, provided full KYC verification has already been done and

the same is not due for periodic updation.

### **SELLING THIRD PARTY PRODUCTS**

While selling third party products, Jewel Rock Hire Purchase and Leasing Private Limited shall comply with the following directions:

- a. Identity and address of the walk-in customers shall be verified for transactions above Rs 0.50 lakh, whether conducted as a single transaction or several transactions that appear to be connected.
- b. Transaction details of sale of third-party products and related records shall be maintained as specified under this policy.
- c. AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be made available.
- d. Transactions involving Rs 0.50 lakh and above shall be undertaken only by:
  - a) Debit to customer's account or against cheque, transfer from banks / debit cards / credit card etc.
  - b) Obtaining and verifying PAN (regular customer as well as walk in customer).

**Note:** Direction no. d shall also apply to sale of Jewel Rock Hire Purchase and Leasing Private Limited 's own products, sale and reloading of prepaid / travel cards and any other products for Rs 0.50 lakh and above

### **ISSUANCE OF PREPAID PAYMENT INSTRUMENTS (PPI)**

With regard to the PPI, Jewel Rock Hire Purchase and Leasing Private Limited shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

### **MONITORING OF TRANSACTIONS**

- a. Jewel Rock Hire Purchase and Leasing Private Limited shall monitor transactions of a suspicious nature on an ongoing basis for the purpose of reporting it to the appropriate authorities. (An illustrative list of suspicious transactions is given in Annexure III). The extent of monitoring by the Jewel Rock Hire Purchase and Leasing Private Limited will depend on the risk sensitivity of the account and special attention will be given to all complex unusually large transactions, which have no apparent economic or lawful purpose.
- b. Jewel Rock Hire Purchase and Leasing Private Limited shall exercise caution with respect to the transactions with persons (including legal persons and other financial institutions) from the countries which have been identified by Financial Action Task Force (FATF) as high risk and non-cooperative jurisdictions with respect to compliance with the FATF Recommendations, 2012.
- c. Jewel Rock Hire Purchase and Leasing Private Limited shall file Suspicious Transaction Report (STR), Cash Transaction Report (CTR), counterfeit



currency report (CCR) and other applicable reports filling under FATCA in terms of the direction of the RBI/PMLA in respect of all products/ services.

### **Ongoing due diligence**

- a. Jewel Rock Hire Purchase and Leasing Private Limited shall undertake on going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and source of funds.
- b. Any unusual pattern in the operations of the accounts like transactions exceeding threshold limits, high turnover in the accounts compared to the average outstanding etc shall be closely monitored. The extent of monitoring shall be aligned with the risk category of the Customer and high-risk category accounts shall be subjected to more intensified monitoring.
- c. A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

### **Periodic updation**

Periodic updation shall be carried out at least once in every two years, for high-risk Customers, once in every eight years for medium risk Customers and once every ten years for low-risk Customers as per the following procedure:

- a. CDD as specified in above shall be carried out at the time of updation. In the case of low-risk customers when there is no change in status with respect to their identities and addresses, a self-declaration to that effect shall be obtained.
- b. In case of legal entities, Jewel Rock Hire Purchase and Leasing Private Limited shall review the documents sought at the time of opening of account and obtain fresh certified copies.
- c. Physical presence of the customers need not be insisted up on for the purpose of furnishing OVD or furnishing consent for Aadhaar Offline verification unless there are sufficient reasons for their physical presence to establish their bona-fides. In normal case, OVD/Consent forwarded by the customer through mail/post, etc., can be accepted.
- d. Jewel Rock Hire Purchase and Leasing Private Limited may provide an acknowledgement with date of having performed KYC updation

(Note: The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.)

**Existing customers**

In case of existing customers, Jewel Rock Hire Purchase and Leasing Private Limited shall obtain PAN or Form No.60 by such date notified by the Central Government, failing which Jewel Rock Hire Purchase and Leasing Private Limited shall temporarily cease operations in the account till the time the PAN number of Form No.60 is submitted by the customer.

Prior to ceasing operations of an account temporarily, Jewel Rock Hire Purchase and Leasing Private Limited shall give the clients an accessible notice and reasonable opportunity to be heard. Jewel Rock Hire Purchase and Leasing Private Limited may allow relaxations for continued operations of the account, if the borrower is unable to provide these documents due to injury, infirmity on account of old age or otherwise etc for a maximum period of 6 months. These relaxations shall be permitted by Senior Management.

Operations of the customers without PAN or Form No.60 shall be monitored closely and shall ensure that transaction does not exceed Rs 5 lakh.

For gold loan customers, a copy of the PAN Card of the borrower shall be collected for all transaction above 5 lakhs

**RISK MANAGEMENT**

Jewel Rock Hire Purchase and Leasing Private Limited has put in place appropriate procedures to ensure effective implementation of KYC guidelines.

- a. Risk categorization of Customers shall be undertaken based on various factors, such as nature of employment, business activity of the Customer, location of Customer and his/its clients, mode of payments, volume of turnover, social / financial status and credit history. Jewel Rock Hire Purchase and Leasing Private Limited has categorized its customers into 'High Risk / Medium Risk / Low Risk' based on the profile of the customers. Jewel Rock Hire Purchase and Leasing Private Limited shall apply higher due diligence measures keeping in view the risk level
- b. Jewel Rock Hire Purchase and Leasing Private Limited has developed robust underwriting procedures for onboarding borrowers, which include verification of ownership of the gold ornaments (in the case of gold loans), assessment of financial resources of the borrowers, collection of their market reports etc (for other loans).
- c. Jewel Rock Hire Purchase and Leasing Private Limited's internal audit periodically evaluate the level of adherence to the KYC procedures. Audit function shall provide an independent evaluation of the effectiveness of KYC policies and procedures, including legal and regulatory requirements.

## **Money Laundering and Terrorist Financing Risk Assessment**

Jewel Rock Hire Purchase and Leasing Private Limited shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, cognizance of the overall sector-specific vulnerabilities if any, that the regulator/supervisor may share from time to time shall be taken.

The risk assessment exercise shall be conducted on a quarterly basis and parameters of the assessment shall be modified, in alignment with the outcome of the risk assessment exercise. An internal document detailing the assessment process may be kept separately for the same.

The outcome of the exercise shall be put up to Risk Management Committee and should be available to competent authorities and self-regulating bodies.

## **ENHANCED DUE DILIGENCE**

**Accounts of Politically Exposed Persons (PEP):** Special care and diligence will be taken in respect of Politically Exposed Persons. Generally, the Jewel Rock Hire Purchase and Leasing Private Limited would not open accounts of PEP. Decision to deal with such persons as a Customer shall be taken up at a senior management level and shall be subjected to enhanced monitoring.

**Accounts of non-face-to-face customers:** These customers are those who opened accounts without visiting the branches / offices of Jewel Rock Hire Purchase and Leasing Private Limited or meeting its officials. Jewel Rock Hire Purchase and Leasing Private Limited shall ensure that first payment from these accounts shall be affected through the customers' KYC-Complied account with another Regulated Entity.

**Client accounts opened by professional intermediaries:** Jewel Rock Hire Purchase and Leasing Private Limited shall ensure while opening client accounts through professional intermediaries, that:

- a. Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
- b. Jewel Rock Hire Purchase and Leasing Private Limited shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- c. Jewel Rock Hire Purchase and Leasing Private Limited shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to Jewel Rock Hire Purchase and Leasing Private Limited.

- d. All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of Jewel Rock Hire Purchase and Leasing Private Limited, and there are 'subaccounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Jewel Rock Hire Purchase and Leasing Private Limited, the Jewel Rock Hire Purchase and Leasing Private Limited shall look for the beneficial owners.
- e. Jewel Rock Hire Purchase and Leasing Private Limited shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
- f. The ultimate responsibility for knowing the customer lies with Jewel Rock Hire Purchase and Leasing Private Limited.

### **CONFIDENTIALITY OF INFORMATION ABOUT CUSTOMERS**

All the information collected from the customers by Jewel Rock Hire Purchase and Leasing Private Limited shall be kept confidential and all such information shall be treated as per the agreement/terms and conditions signed by the customers. Additionally, the information sought from each Customer should be relevant to the risk perceived in respect of that Customer, should not be intrusive and should be in line with the guidelines issued by the RBI in that behalf.

Information collected from customers shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

Exception to the confidentiality of customer information shall be as under:

- a. Where disclosure is under compulsion of law.
- b. Where there is a duty to the public to disclose.
- c. The interest of the company requires disclosure.
- d. Where the disclosure is made with express or implied consent of the customer.

### **MAINTENANCE OF RECORDS OF TRANSACTIONS**

Jewel Rock Hire Purchase and Leasing Private Limited shall maintain proper records of the transactions as required under the provisions of PML Act and Rules. Jewel Rock Hire Purchase and Leasing Private Limited shall

- a. maintain all necessary records of transactions between Jewel Rock Hire Purchase and Leasing Private Limited and the customer, both domestic and international, for at least five years from the date of transaction or any other higher periods specified in any other law
- b. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended.

- c. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005)
- d. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
  - 1. the nature of the transactions;
  - 2. the amount of the transaction and the currency in which it was denominated;
  - 3. the date on which the transaction was conducted; and
  - 4. the parties to the transaction.
- e. Jewel Rock Hire Purchase and Leasing Private Limited have a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

## **GENERAL**

### **1. Adherence to KYC guidelines by agents**

- a. Agents shall be appointed only after detailed due diligence and ensuring that they are fully compliant with KYC guidelines applicable to NBFCs.
  - b. Jewel Rock Hire Purchase and Leasing Private Limited shall make available all information to RBI to verify the compliance with KYC guidelines. Jewel Rock Hire Purchase and Leasing Private Limited shall be responsible for non-compliance of KYC guidelines by agents.
2. **Principal Officer** Jewel Rock Hire Purchase and Leasing Private Limited has designated Managing Director as Principal Officer (PO) responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law/regulations.
  3. **Designated Director** Jewel Rock Hire Purchase and Leasing Private Limited has nominated Executive Director, as Designated Director, to ensure overall compliance with the obligations under Prevention of Money laundering Act, 2002 and Rules framed thereunder, from time to time.
  4. **CDD Procedure and sharing KYC information with central KYC records Registry (CKYCR)** Jewel Rock Hire Purchase and Leasing Private Limited shall capture the KYC information for uploading the data pertaining to all new individual accounts opened on or after 1/4/2017 with the CKYCR in the manner mentioned in the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and

Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR.

5. **Training Programme** Jewel Rock Hire Purchase and Leasing Private Limited shall have adequate screening mechanism as an integral part of personnel recruitment / hiring process and also should have an ongoing employee training programs so that members of the staff are adequately trained in KYC/AML/CFT procedures. Training requirements shall have different focuses for front line staff and officer/staff dealing with new customers so that all concerned fully understand the rationale behind the KYC policies and implement them consistently.

#### **COMPLIANCE OF KYC POLICY**

- a. Jewel Rock Hire Purchase and Leasing Private Limited 's internal audit and compliance functions periodically evaluate the level of adherence to the KYC policies and procedures. The compliance function and audit function together shall provide an independent evaluation of the effectiveness of KYC policies and procedures, including legal and regulatory requirements. The Audit Committee of the Board shall review adherence to the KYC guidelines at quarterly intervals.
- b. Internal Audit shall on a yearly basis conduct an evaluation of compliance functions of policies and procedures including legal and regulatory requirements.

#### **OTHER OPERATING INSTRUCTIONS**

- a. In case of customers whose accounts have not been operated (or who have not been transacting) for more than 12 months, fresh KYC documents will need to be taken before undertaking any new transactions. System based control will be put in place.
- b. As a policy, Gold loan will be granted to individuals only and not to companies, firms, trusts etc.
- c. In the case of 'pardanashin' (veil) women, capturing of the customer's photograph (in Customer ID file on the system) may waived provided an acceptable Proof of Identity document is furnished and KYC verification has been carried down by any of female staffs.

**ANNEXURE I  
OFFICIALLY VALID DOCUMENTS (OVD)**

**1. Individuals**

Officially Valid Documents (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the voters identity card issued by the election commission of India, job card issued by NREGA duly signed by an Officer of the state government and letter issued by the National Population Register containing details of name and address.

Provided that,

- a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- b. where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the LIMITED purpose of proof of address: -
  - a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
  - b) property or Municipal tax receipt;
  - c) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
  - d) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;
- c. the customer shall submit OVD with current address within a period of three months of submitting deemed OVDs
- d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

**Non-Individuals (Companies, Firms, Trusts etc.)**

KYC norms are applicable to non-individuals also. The requirements are as under

Companies	<p>Certified copies of each of the following documents shall be obtained:</p> <ul style="list-style-type: none"> <li>a) Certificate of incorporation with Memorandum &amp; Articles of Association</li> <li>b) Resolution of Board of Directors for opening the account and Power of Attorney / authorization of persons to operate the account on its behalf</li> <li>c) PAN allotment letter/ PAN of the Company</li> </ul> <p>Documents as specified in para 1 above of the individuals holding attorney /authorisation to transact on company's</p>
-----------	---

	behalf.
Partnership Firms	<p>Certified copies of each of the following documents shall be obtained:</p> <p>a) Registration certificate.  b) Partnership deed.  c) PAN of the partnership firm</p> <p>Documents as specified in para 1 above of the individuals holding attorney /authorisation to transact on its behalf.</p>
Proprietorship Firms	<p>For opening an account, CDD of the individual (proprietor) as mentioned in para 3.2.1 shall be carried out PLUS any two of the below mentioned documents,</p> <p>a) Registration certificate, if registered  b) Certificate/License issued under Shops &amp; Establishment Act  c) GST and Income Tax returns  d) GST registration certificate (provisional/ final)  e) Utility bills such as electricity, water, telephone bills etc.  f) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.  g) IEC (Import Export Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.</p>
Trusts	<p>For opening an account, certified copies of each of the following documents shall be obtained:</p> <p>a) Certificate of registration  b) Trust Deed  c) Power of attorney authorizing a person to carry out transactions on behalf of the trust  d) PAN or Form No.60 of the trust  e) Resolution of the managing body of the trust / association.</p> <p>Valid documents identifying the trustees, power of attorney holder etc. (same as applicable for individuals as mentioned in para 1 above).</p>
An unincorporated association or a body of individuals	<p>For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents shall be obtained:</p> <p>(a) Resolution of the managing body of such association or body of individuals  (b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals  (c) Power of attorney granted to transact on its behalf  (d) Documents, as specified in Para 1, of the person holding an attorney to transact on its behalf and</p>



	(e) Such information as may be required by JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED to collectively establish the legal existence of such an association or body of individuals.
Juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats	For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents shall be obtained: (a) Document showing name of the person authorised to act on behalf of the entity; (b) Documents, as specified in Para 1, of the individual holding an attorney to transact on its behalf and (c) Such documents as may be required by Jewel Rock Hire Purchase and Leasing Private Limited to establish the legal existence of such an entity/juridical person.

## ANNEXURE II

### Regulated Entities:

- a. All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949.
- b. All India Financial Institutions (AIFIs).
- c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).
- d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
- e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

### **ANNEXURE III**

#### **ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS**

Broad categories of reasons for suspicion and examples of suspicious transactions generally observed in Non- Banking Financial Companies are indicated as under:

- 1. Identity of client:**
  - False identification documents
  - Identification documents which could not be verified within reasonable time
  - Accounts opened with names very close to other established business entities.
- 2. Background of Client:**
  - Suspicious background or links with known criminals.
- 3. Multiple Accounts:**
  - Large number of accounts having a common account holder, introducer or authorized personnel.
- 4. Signatory with no rationale:**
  - Unexplained transfers between multiple accounts with no rationale.
- 5. Activity in accounts:**
  - a. Unusual activity compared with past transactions- Sudden activity in dormant accounts;
  - b. Activity inconsistent with what would be expected from declared business.
- 6. Nature of transactions:**
  - a. Unusual or unjustified complexity;
  - b. No economic rationale or bonafide purpose;
  - c. Frequent cash transactions;
  - d. Nature of transactions inconsistent with what would be expected from declared business.
- 7. Value of Transactions:**
  - a. Value just under the reporting threshold amount in an apparent attempt to avoid reporting.
  - b. Value inconsistent with the client's apparent financial standing.
- 8. Indicators of Suspicious Transactions:**
  - a. Reluctant to part with information, data and documents;
  - b. Submission of false documents, purpose of loan and detail of accounts;
  - c. Reluctance to furnish details of source of funds;
  - d. Reluctance to meet in person, representing through power of attorney;
  - e. Approaching a distant branch away from own address;
  - f. Maintaining multiple accounts without explanation;
  - g. Payment of initial contribution through unrelated third-party account;
  - h. Suggesting dubious means for sanction of loan;
  - i. Where transactions do not make economic sense;
  - j. Where doubt about beneficial ownership;
  - k. Encashment of loan through a fictitious bank account;
  - l. Sale consideration quoted higher or lower than prevailing prices;
  - m. Request for payment in favor of third party with no relation to transaction;
  - n. Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent;
  - o. Frequent request for change of address;
  - p. Over-payment of instalments with a request to refund the overpaid amount.

BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED

Director

---

**CC:**

4. Legal Department
  5. Administration Department
  6. HR Department
- 

Dated this the 01<sup>st</sup> Day of April, 2023



## **JEWEL/LEGAL/NOTIFICATION**

**Thrissur, April 01, 2023**

In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies the guidelines to be followed branches/offices while sanctioning loans against the security of single product-Gold Jewellery.

### **GOLD LENDING POLICY**

**1.**

1. These guidelines may be gold The Gold Lending Policy- 2023-24
2. They shall come into force on 01<sup>st</sup> April, 2023.

**2. Applicability:**

This policy is applicable to loans sanctioned against security of single product- Gold Jewellery.

**3. Loan to Value (LTV):**

The company shall maintain a Loan to Value (LTV) Ratio not exceeding 75 per cent for loans granted against the collateral security of gold jewellery. The management reserves the right to determine the LTV based on the existing marketing conditions of the state. The head office shall provide the LTV ratio on day to day basis to branches.

**4. Determination of Value of Gold**

The intrinsic value of the gold is only considered for determining loan amount. The following are the guidelines of Reserve Bank of India, adopted by the company for the purpose of determination of value of gold:

- 1) The gold jewellery accepted as collateral by the Company shall be valued by taking into account the preceding 30 days' average of the closing price of 22 carat gold as per the rate as quoted by the Bombay Bullion Association Ltd. (BBA) or the historical spot gold price data publicly disseminated by a commodity exchange regulated by the Forward Markets Commission.
- 2) If the purity of the gold is less than 22 carats, the company shall translate the collateral into 22 carat and state the exact grams of the collateral. In other words, jewellery of lower purity of gold shall be valued proportionately.
- 3) Company, while accepting gold as collateral, shall give a certificate to the borrower on their letterhead, of having assayed the gold and state the purity (in terms of carats) and the weight of the gold pledged.

## **5. Prohibited forms of Gold as Collateral Security**

The lending on the following forms of gold prohibited:

- 1) bullion / primary gold and
- 2) gold coins & offerings to a temple.

The company shall not grant any advance for purchase of gold in any form including primary gold, gold bullion, gold jewellery, gold coins, units of Exchange Traded Funds (ETF) and units of gold mutual fund.

## **6. Verification of Ownership of Collateral Security**

Where the gold jewellery pledged by a borrower at any one time or cumulatively on loan outstanding is more than 20 grams, company shall keep a record of the verification of the ownership of the jewellery. The ownership verification need not necessarily be through original receipts for the jewellery pledged but a suitable document shall be prepared to explain how the ownership of the jewellery has been determined, particularly in each and every case where the gold jewellery pledged by a borrower at any one time or cumulatively on loan outstanding is more than 20 grams.

## **7. Safety and security measures to be followed by company lending against collateral of gold jewellery**

- 1) Company shall ensure that necessary infrastructure and facilities are put in place, including safe deposit vault and appropriate security measures for operating the vault, in each of its branches where gold jewellery is accepted as collateral. This is required to safeguard the gold jewellery accepted as collateral and to ensure convenience of borrowers.

## **8. The duties and responsibilities of Branch Managers in lending against collateral of gold jewellery.**

1. Compliance of KYC (Know Your Customer) guidelines issued by the Reserve Bank of India. i.e., the applicant shall submit the following documents along with loan application
  1. Color Photo
  2. Self-Attested Copy of Permanent Account Number (PAN) Card
  3. Self-Attested Copy of Aadhar/Passport/Voters ID
  4. Verified Mobile Number 2(Nos)
  5. Verified E-mail Id
2. Compliance of assaying procedures issued by the company for determining value/quality of the jewellery received.
  1. Verification of KYC of the Customer

2. The branch shall sanction loan only to those customers who are belonging to the permitted areas of operation of branch by the head office.
3. The Branch shall take the photo of the customer with date & time through our software.
4. No loan shall be renewed without the presence of customer in Branch
  
5. Verification (weight, purity etc.) of gold jewellery by the Branch Manager and in his absence Assistant Branch Manager/Executive, who have relevant experience in verification of gold jewellery with the prior approval of management.
6. Determining the value of the gold by using the electronic weighing machine by the branch executive/assistant branch manager.
7. Finalization of scheme of loan with customer.
8. Recommending & forwarding the of loan application of customer for the approval of branch manager.
9. Verification of documents and sanctioning of loan to the customer by the Branch Manager.
10. Disbursement of loan amount to the customer along with the acknowledgment.
11. If the loan amount exceeds Rs. 3 Lacs (Rupees Three Lakhs) the prior approval of the Head office shall be taken.
12. If the loan amount exceeds Rs. 3 Lacs (Rupees Three Lakhs), the collective photos of gold jewellery and photo of weight information's shall be shared with Head office- Accounts Department
  
3. Declaration from the customers to satisfy ownership of the gold jewellery
  
4. Ensure that, there is always Adequate systems for storing the jewellery in safe custody, reviewing the systems on an on-going basis, training the concerned staff. Obtain the periodic report from internal auditors that, procedures are strictly adhered to.
  
5. Periodically audit by a qualified/experienced gold appraiser (Purity, weight, amount disbursed etc.)
  
6. Ensure that, the jewellery accepted as collateral shall be appropriately insured.

## **9. Fraudulent Transactions**

Any fraudulent transactions noticed/found by the branch employees;

1. They shall inform the Internal Auditor & Administration Manager via e-mail within 24hrs of event.

2. The administration manager shall initiate the procedure for verification of details of transaction. The report should be submitted to the Legal Department for further process within 48hrs of mail.
3. The legal Department should make necessary arrangements for safeguarding the interest of the company within 48hrs receipt of report from Administration Manager and report should be submitted to the Managing Director within Next 48hrs.
4. Allow appropriate time limit to settle the Fraud.
5. If the fraud is not settled, the legal department shall take appropriate legal action against staffs who were involved in the fraud.
6. Proceed with legal action, whether Civil or Criminal, up to the settlement of Fraud or up to the final Judgement of legal action.

**BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE  
AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

7. **Legal Department**
8. **Administration Department**
9. **HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**



**JEWEL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies the guidelines to be followed branches/offices while sanctioning loans against the security of single product-Gold Jewellery & Auction thereon if any

**GOLD AUCTION POLICY**

These guidelines may be called The Gold Auction Policy- 2023-24

**1. Effective Date**

They shall come into force on 01<sup>st</sup> April, 2023.

**2. Applicability:**

This policy is applicable to loans sanctioned against security of single product- Gold Jewellery.

**3. Loan Agreement**

The company shall ensure that, the loan agreement shall also disclose details regarding auction procedure.

**4. Place of Auction**

The auction shall be conducted in the same town or taluka in which the branch that has extended the loan is located.

However, In reference to the “DOR.NBFC (PD). CC.No.108/03.10.001/2019-20” of Reserve Bank of India, the company can however pool gold jewellery from different branches in a district and auction it at any location within the district, subject to meeting the following conditions:

- i. The first auction has failed.
- ii. The company shall ensure that all other requirements of the extant directions regarding auction (prior notice, reserve price, arms-length relationship, disclosures, etc.) are met.

**5. Reserve Price**

While auctioning the gold the company must declare a reserve price for the pledged ornaments. The reserve price for the pledged ornaments shall not be less than 85 per cent of the previous 30 days average closing price of 22 carat gold as declared by the Bombay Bullion Association Ltd. (BBA) or the historical spot gold price data publicly disseminated by a commodity exchange regulated by the Forward Markets Commission and value of the jewellery of lower purity in terms of carats shall be proportionately reduced. The IRR (Internal Rate of Return) fixed by the Management shall be considered while fixing Reserve Price.



**6. Auctioneers**

Gold pledged shall be auctioned only through auctioneers approved by the Board. The company or its employees shall not participate in the auctions held.

**7. Advertisement**

The auction shall be announced to the public by issue of advertisements in at least two newspapers, one in vernacular and another in national daily newspaper.

**8. Proceedings of Auction**

The company shall provide the full details of the value fetched in the auction and the outstanding dues adjusted and any amount over and above the loan outstanding shall be payable to the borrower.

**9. Transparency & Arms-length relationship during the auction**

The company shall ensure that, Transparent auction procedure in case of non-repayment with adequate prior notice to the borrower. There shall be no conflict of interest and the auction process must ensure that there is arm's length relationship in all transactions during the auction including with group companies and related entities.

**10. Annual Reports**

The company shall disclose in their annual reports the details of the auctions conducted during the financial year including the number of loan accounts, outstanding amounts, value fetched and whether any of its sister concerns participated in the auction.

**BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE  
AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

- 10. Legal Department**
- 11. Administration Department**
- 12. HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**



**JEWL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

**THE GOLD AUCTION POLICY RULES, 2023-24**  
JEWRL/LEGAL/NOTIFICATION APRIL-2023  
Thrissur, Dated 01<sup>st</sup> April, 2023

**GOLD AUCTION POLICY**

1. **These rules may be called The Gold Auction Policy Rules, 2023**
2. **They shall come into force on 01<sup>st</sup> April, 2023.**
3. **The Gold Collection and Auction Rules to be followed:**
  - 3.1.1. **Contacting of Customer**

The branch manager shall ensure that, there is regular communication of reminder with the customer about the due date of payment of interest of the loan amount availed and also inform the customer that if the account is not settled before the maturity, the jewellery will be sold in auction. Preferably, 15 days before due date. The mode of communication can be Tele calling, messages, e-mail, direct meeting subject to the approval of deputy general manager.
  - 3.1.2. **Failure in settlement of interest and principal before the maturity period of the scheme availed.**

The branch manager shall ensure that, if any loan account holder failed to settle the loan account along with principle and interest amount before the maturity period of the scheme availed, the file shall be transferred to legal department within 24hrs with the approval of DGM, for sending legal notice (Registered) demanding the closure of account and intimating the auction procedures.
  - 3.1.3. **Auction List**

If the loan account holder fails to settle the matter within 15 days from the date of sending the registered legal notice or customer has not responded to the intimation letter of the company, then the branch manager shall include the name of loan account holder to the Upcoming Auction List within 2 days.
  - 3.1.4. **Submission of Auction List and Gold Jewellery to Head Office**

The branch shall handover the Auction List along with the gold jewellery to head office directly or through internal auditor or the person authorized by the Company to do so. Sufficient acknowledgment shall be collected

from the Head Office.

**3.1.5. Gold Appraiser Report**

The administration manager shall ensure that, the Head Office appraising of the purity, weight, value of the gold under auction by a qualified appraiser is completed and his report shall be submitted to Auction Officer

**3.1.6. Determination of Reserve Price**

The administration department shall ensure that, the finance department has provided the reserve price to be fixed the gold under the auction list.

**3.1.7. List of Auctioneers**

The administration department shall ensure that, the list of auctioneers & auction list is approved by the board of directors or board committee formed for the purpose. The approval reference number should be mentioned in the lists.

**3.1.8. Public Notice of Auction**

The administration department shall ensure that, the auction shall be announced to the public by issue of advertisements in at least two newspapers, one in vernacular and another in national daily newspaper indicating the place, date and time and other relevant information.

**3.1.9. Auction**

The administration department shall ensure that,

- a) Auction has been held on at the right place at right time.
- b) All participants marked their attendance in the register
- c) The reserve price shall be announced by the Auction Officer.
- d) The final bid amount of all auctioneers shall be noted by the Auction Officer.
- e) The highest bid amount shall be noted by the Auction Officer.
- f) After deciding the successful bidder, two witness signatures (from the participants) shall be obtained by the Auction Officer on the bid record.
- g) The bid record shall include the details of highest bid amount and successful bidder and final bid amount of all auctioneers.

**Auction Participants**

**Internal Parties**

- 1. Auction Officer
- 2. Administration Manager
- 3. Finance Manager
- 4. Branch Manager or Assistant Branch Manager
- 5. Special invitees, with prior approval of board of directors

**External Parties**

1. Borrowers
2. Approved auctioneers
3. Special invitees, with prior approval of board of directors

**3.1.10. Settlement and Closure of Loan Account**

After completion of successful auction, the loan account of the defaulter shall be closed and any excess amount, if any, found shall be refunded to the defaulter after deducting dues if any with the company.

Similarly, in the settlement of account after completion of auction, the company has incurred any loss and which also fails to meet the IRR fixed by the Board of Directors, then that files should be transferred to legal department for initiating legal actions.

**BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE  
AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

- 13. Legal Department**
- 14. Administration Department**
- 15. HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**



**JEWEL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies the guidelines to be followed branches/offices while dealing with customer grievances.

**The Grievance Redressal Policy**

**1. Name:**

These guidelines may be called The Grievance Redressal Policy 2023

**2. Effective Date**

They shall come into force on 01<sup>st</sup> April, 2023.

**3. Applicability:**

This policy is applicable to all over the offices of the company including branch office, liaison office, head office, corporate office and registered office of the company.

**4. Types of Grievances:**

The expected grievances are classified in the following manner

**Branch Office Level**

1. Customer Grievances
2. Employees Grievances
3. Statutory Regulators Grievances

**Head Office Level**

1. Employees Grievances
2. Statutory Regulators Grievances

**5. Officers in Charge:**

The officers in charge is for dealing grievances in designated in the following manner.

Operational Level Officer	:	Internal Auditors
Middle Management Level Officer	:	Administration Manager
Management Level Officer	:	Managing Director

**BY THE ORDER OF THE BOARD**  
**For JEWEL ROCK HIRE PURCHASE**

**AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

- 16. Legal Department**
- 17. Administration Department**
- 18. HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**



**JEWL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

**THE GRIEVANCES REDRESSAL POLICY RULES, 2023**  
 JEWRL/LEGAL/NOTIFICATION APRIL-2023  
 Thrissur, Dated 01<sup>st</sup> April, 2023

**THE GRIEVANCES REDRESSAL POLICY**

1. These rules may be called The Grievances Redressal Policy Rules, 2023
2. They shall come into force on 01<sup>st</sup> April, 2023.
3. The Grievances Redressal Policy Rules, 2023 to be followed:

**BRANCH OFFICE LEVEL**

**Customer Grievances**

S No	Matter of issue	Level of Compliant	Level of Officer	Turnaround Time (TAT) Required
1	Product	Branch Office Level	Internal Auditor	1-3 Days
2	Service	Head Office Level	Administration Manager	1-2 Days
3	Legal Matters		Legal Head	1-3 Days
4	RBI Related Matters		Managing Director	1-3 Days

**Employee Grievances**

S No	Matter of issue	Level of Compliant	Level of Officer	Turnaround Time (TAT) Required
1	Infrastructure Facilities & Others	Branch Office Level	HR Department	1-3 Days
2	Service	Head Office Level	Administration Manager	1-2 Days
3	Legal Matters		Legal Head	1-3 Days
4	RBI Related Matters		Managing Director	1-3 Days

**Statutory Regulators Grievances**

S No	Matter of issue	Level of Compliant	Level of Officer	Turnaround Time (TAT) Required
1	Compliance of Local Laws	Branch Office Level	Administration Manager	1-3 Days
2	Other Legal Matter	Head office Level	Legal Head	1-3 Days
3	RBI Compliance		Managing Director	1-3 Days

### HEAD OFFICE LEVEL

#### Employee Grievances

S No	Matter of issue	Level of Compliant	Level of Officer	Turnaround Time (TAT) Required
1	Infrastructure Facilities & Others	Branch Office Level	HR Department	1-3 Days
2	Service	Head Office Level	Administration Manager	1-2 Days
3	Legal Matters		Legal Head	1-3 Days
4	RBI Related Matters		Managing Director	1-3 Days

#### Head Office Levels

#### Statutory Regulators Grievances

S No	Matter of issue	Level of Compliant	Level of Officer	Turnaround Time (TAT) Required
1	Compliance of Local Laws	Branch Office Level	Administration Manager	1-3 Days
2	Other Legal Matter	Head office Level	Legal Head	1-3 Days
3	RBI Compliance/Other Compliances of Laws		Managing Director	1-3 Days

**Provided that,**

The time for the compliance of law can be changed as per the provision of the concerned law.



**BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE  
AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

- 1. Legal Department**
- 2. Administration Department**
- 3. HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**



**JEWEL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

**Prudential Norms on Income Recognition, Asset Classification and Provisioning pertaining to advances – RBI circular dated 12/11/2021**

**RBI instructions on 'Prudential norms on Income Recognition, Asset Classification and Provisioning, pertaining to Advances dated 12th November 2021.**

With reference to the RBI circular no. RBI/2021-2022/125 DOR.STR.REC.68/21.04 .048/2021-22 on 'Prudential norms on Income Recognition, Asset Classification and Provisioning, pertaining to Advances — Clarifications' dated 12th November 2021, the following clarifications may kindly be noted.

1. **Clarification on 'Overdue'**  
**An amount is to be treated as 'Overdue' if it is not paid on the due date fixed by the Company.**
  
2. **Classification as Special Mention Account (SMA) and Non-Performing Asset (NPA)** The RBI circular DBR.No.BP.BC.45/21.04.048/2018-19 dated 7th June, 2019 on 'Prudential Framework for Resolution of Stressed Assets' requires the lenders to recognize incipient stress in borrower accounts, immediately on default, by classifying them as special mention accounts (SMA). It is clarified that the intervals are intended to be continuous and accordingly, the basis for classification of SMA categories shall be as follows:

Loans other than revolving facilities	
<b>SMA Sub-categories</b>	<b>Basis for classification — Principal or interest payment or any other amount wholly or partly overdue</b>
SMA-0	Up to 30 days
SMA-1	More than 30 days and up to 60 days SMA-2
SMA-2	More than 60 days and up to 90 days Accordingly,

Accordingly, the date of SMA/NPA shall reflect the asset classification status of the loan account, at the day-end of that calendar date. An illustration of such classification is as follows:

<b>SMA Categories</b>	<b>Basis for classification — Principal or interest payment or any other amount wholly or partly overdue</b>	<b>If a customer takes a loan on 1st Jan 2021 and repayment is made without default till 1st Dec 2021 and subsequent repayments are not made. Then the loan will fall in</b>
SMA-0	Upto 30 days	SMA 0 on 1st Jan 2022
SMA-1	More than 30 days and upto 60 day	SMA 1 on 31st Jan 2022
SMA-2	More than 60 days and upto 90 days	SMA 2 on 2nd Mar 2022
NPA	More than 90 days	The loan will be treated as NPA upon running day-end process on 1st April 2022

Case (B) Gold Loan

SMA Categories	Basis for classification — Principal or interest payment or any other amount wholly or partly overdue	A customer takes a loan on 1st Jan 2021 with maturity date as on 29th Jun 2021 (6-month scheme) and If the Principal or interest payment or any other amount wholly or partly overdue in such loan on 29th Jun 2021, then the loan will fall in
SMA-0	Up to 30 days	SMA 0 on 29th Jun 2021
SMA-1	More than 30 days and up to 60 days	SMA 1 on 29th Jul 2021
SMA-2	More than 60 days and upto 90 days	SMA 2 on 28th Aug 2021
NPA	More than 90 days	The loan will be treated as NPA upon running day-end process on 27th Sept 2021

In the above context, it is further clarified that borrower accounts shall be flagged as overdue by the lending institutions as part of their day-end processes for the due date, irrespective of the time of running such process.

**3. NPA Classification in case of interest payments.**

In case of interest payments in respect of term loans, an account will be classified as NPA, if the interest applied at a specified date remains overdue for more than 90 days.

These instructions shall be effective from 31st March, 2022. Accordingly, in respect of any borrower account which becomes overdue on or after 31st March, 2022, its classification as NPA shall be based on the account being overdue for more than 90 days.

**4. Upgradation of accounts classified as NPAs**

In this regard, it is clarified that loan accounts classified as NPAs may be upgraded as 'Standard' asset only if entire arrears of interest and principal are paid by the borrower (applicable from October 1, 2022). Regarding upgradation of accounts classified as NPA due to restructuring, non-achievement of date of commencement of commercial operations (DCCO), etc., the instructions as specified for such cases shall continue to be applicable.

**BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE  
AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

- 19. Legal Department**
- 20. Administration Department**
- 21. HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**



**JEWEL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

**FRAUD REPORTING TO RBI:**  
**TIMELY INTIMATION OF FRAUD INCIDENTS DETECTED & FILING OF POLICE COMPLAINT**

With reference to the captioned subject, the following directions are notified for strict compliance.

**1. Intimation on fraud incidents**

It may be noted that in the instance of a fraud being detected, intimation (details in brief) shall be provided to the Compliance Department ([accounts@jewelrockfinance.com](mailto:accounts@jewelrockfinance.com)) within 2 days of such detection or conclusion of the incident as fraud, by the concerned RMs where the fraud has occurred at the regional/branch level and in the case of fraud detected at HO or in other business verticals (SME/VEF) by the concerned departments at HO/Vertical Heads. Further, a detailed report in the prescribed format shall be submitted within 10 days of such detection.

**2. Filing of Police Complaint in all incidents where the commitment of fraud has been detected/ confirmed, police complaint should compulsorily be filed against those involved in the following instances.**

- The amount involved in fraud is above Rs. 10,000, committed by the staff.
- The amount involved in fraud is Rs. 1 lakh & above, committed by customers/external parties.

The above instructions are in line with the RBI's Directions/Circular (Master Direction: "Monitoring of Frauds in NBFCs (Reserve Bank) Directions, 2016" DNBS. PPD.01/66.15.001/2016-17, dated September 29, 2016 and Master Circular: "Future approach towards monitoring of frauds in NBFCs", DNBR (PD) CC.No.058/03.10.119/2015-16) on reporting requirement concerning fraud.

**BY THE ORDER OF THE BOARD**  
**For JEWEL ROCK HIRE PURCHASE**  
**AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

- 22. Legal Department**
- 23. Administration Department**
- 24. HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**



In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies the guidelines to be followed in Information Technology (IT) operations/activities in the company

## INFORMATION TECHNOLOGY POLICY (IT POLICY)

JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED come under Section-B category of asset size below 500 crores. The Information Technology Policy is designed considering the basic standards mentioned in RBI Master Direction-Information Technology Framework for NBFC sector. It also includes the main policies and sub policies given below.

Using this policy

One of the challenges facing organizations today is enabling employees to work productively while also ensuring the security of the IT network and crucial part is the data on it. Given that technology is continually changing, employees play a significant role in IT security. This policy provides a framework for users to follow when accessing IT systems and the data on them. It is intended to act as a guideline for organization looking to implement or update their own Acceptable Use Policy.

SI No.	Policies	Policy No.
1	Physical/ Logical Access Control Policy	ITP-001
2	Password Policy	ITP-002
3	A Well-Defined User Role	ITP-003
4	Maker Checker Concept	ITP-004
5	Information Security Policy	ITP-005
6	Cyber security Policy	ITP-006
7	Electronic channel security Policy for Mobile Financial Services, Social Media & Digital Signature Certificates	ITP-007
8	System Generated MIS Reports	ITP-008
9	System Generated COSMOS Returns	ITP-009
10	Business Continuity Planning Policy	ITP-010
11	Data Backups and Retention Policy	ITP-011
12	E-mail Usage and Retention Policy	ITP-012

Sl .No.	Policy Name	Policy No	Effective Date
1	Physical/ Logical Access Control Policy	ITP-001	1 <sup>st</sup> April 2021

### **Purpose**

The objective of this Access Control Policy is to provide access to information processing facilities and information assets of organization only for authorized purposes and to establish individual accountability.

### **Scope**

This policy applies to any entity (person) and the access credentials (such as user accounts) with access to the information processing facilities and information assets.

### **Policy**

The access control policy has been segregated into two parts namely Physical Access Control and Logical Access Control.

#### **Physical Access Control**

1. Physical access to all information processing facilities shall be protected by access control systems such as biometric systems, access card etc.
2. Where locks with keys are used, procedures for secure management of the keys must be in place.
3. Records from access control systems must be kept secure and archived.
4. Access to the specific areas (such as data centre, backup storage locations etc.) requires approval from the IT Department. Additional physical access control measures shall be implemented to restrict the access to the selected personnel.
5. All users who have physical access to the information processing facilities shall wear visible identity cards.
6. Access cards, passes, keys or other tokens must be retrieved from staff or contract staff when their employment or contract ceases.
7. Access passes shall be provided to visitors & vendors while entering the premises and should be retrieved on leaving the premises.
8. All physical access must be logged and made available for review when required.

#### **Logical Access Control**

Access to the IT components and data is generally known as logical access. In other terms, any access to the Information processing systems should be considered as logical access. Logical access should be based on the principles of Authentication, Authorization and Accountability

### **Logical access**

1. Access to the IT infrastructure which includes, but not limited to, network devices, network VPN services, operating systems, applications, databases, data files should be granted on the basis of business needs.
2. Access should be allowed on the basis of positive identification and positive authorization.
3. Any access to information systems should be denied by default and access permissions are built, step by step, on a need-to-know basis or on the concept of least privileges.
4. Adequate segregation of duties or separation of privileges within systems should be incorporated. This will ensure that authority is not focused on a single individual.

### **User Authorization**

1. All access requests to data and systems must be formally authorized. Access must be given only on a need-to-know basis.
2. Any access requested by a contractor, temporary staff, or third parties must be authorized by IT Sr. Manager and must be for a limited period, with a defined end date and time. Such access must be promptly disabled

### **User Access Modifications**

1. Access must be modified as required when employees move internally within organization or on vacation for more than 15 days
2. The IT Systems Manager shall have the authority to disable accounts without reference if necessary and notify IT Department.
3. Transfer of user accounts or using other employee user credentials to login is also not permitted.

### **User Access Review**

1. All user access privileges must be recorded and reviewed annually. IT Systems Manager shall coordinate with other departments to perform this review
2. The access rights of all user accounts must be on a need-to-know basis.
3. All user activities should be logged and should be made available for review when required

## **Administrator Access Modifications**

Whenever a System, Application and/or Network Administrator leave the team/department, steps must be taken to change all the administrative passwords of organization information systems which are under the custody of the staff. This should include, but not limited to, the passwords of routers, switches, firewalls, servers, databases and service accounts.

## **Local Administrator Access**

Local Administrator access to workstations shall be granted only when there is a requirement. This elevated privilege shall be granted based on the approval from the IT Department and will only be valid for a limited period of time.

## **Temporary Accounts**

1. Third parties, Temporary staff or staff filling a temporary role shall not use an existing user's identification.
2. The temporary account that is released for use must be for a limited period with a predefined end date and time.

## **Third party access**

1. Access granted to third parties, which includes but not limited to vendors, contractors, external auditors, etc should have the supporting business documents which clearly justify the business needs.
2. Third party access must be for a limited period with a predefined end date and time.

## **Termination of Access**

1. The Employees' Manager ensures that all such user accounts to access ended.
2. Any client user accounts used by the employee should be disabled or the account password should be changed.
3. Codes or passwords for systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate.
4. IT System Managers should be informed by the Human Resources department when employee resignation / termination processed.

## **Enforcement**

Any employee who is found to have violated this policy may be subject to disciplinary action, up to termination of employment.



Sl. No.	Policy Name	Policy No	Effective Date
2	Password Policy	ITP-002	1 <sup>st</sup> April 2021

### **Purpose**

The purpose of this policy is to provide the guidelines necessary for all of the employees of the JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED users to create appropriate passwords and to use them and protect them in an appropriate manner.

### **Scope**

The policy applies to all JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED computers and devices that store company information. It applies to all users of the organization's network, using any device that has access to the network.

### **Policy**

All company-owned workstations and servers must be protected using a user ID and strong password combination. Passwords are used for user accounts, servers, data base, e-mail accounts, network devices, Web & Mobile applications, Firewall devices, Wi-Fi devices, etc. Users of any company-owned systems that require a password must follow the guidelines below for creating passwords:

1. Passwords for typical user accounts should be at least eight characters in length; administrative passwords should be at least 15 characters in length.
2. A password cannot be a word or phrase that can be found in any dictionary or a word spelled backwards.
3. It should contain at least one upper case letter, one non-alpha character and at least one special character (e.g. @\$%^&).
4. Must not be a common pattern found on a standard keyboard or any other common pattern of letters or numbers.
5. It should not be based on personal information such as birthdays, addresses, names, etc.

It is important to protect the secrecy of passwords. The following guidelines must be followed when handling passwords:

1. Passwords can never be written down anywhere that is not under lock and key (no sticky notes!).
2. All user account passwords must be changed every 180 days and cannot be reused. All administrative passwords must be changed every three months.
3. Password can never be included in e-mails or other form of electronic communications.
4. Users must have different passwords for each system that does not use some method of single sign on.

5. Never reveal your password to anyone over the phone, including help desk personnel.
6. Do not share your passwords with assistants, co-workers, family members, or friends. All passwords must be treated as company confidential.
7. Do not use the "Remember Password" feature of any application.
8. Do not store your passwords in any portable electronic device such as tablets or cell phones.

Any exceptions to this policy must be approved in advance by the company IT department.

**Enforcement**

Any employee who is found to have violated this policy may be subject to disciplinary action, up to termination of employment.

Sl. No.	Policy Name	Policy No	Effective Date
3	A Well Defined User Role	ITP-003	1 <sup>st</sup> April 2021

**Purpose**

The objective of this User Role Policy is to define individual user role of organization.

**Scope**

This policy applies to all individuals under organization with access to the information processing facilities and information assets.

**Policy**

**A Well-Defined User Role**

Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users. Users will get access to data only through the authorization and access control process. Access only that data which s/he has a need to know to carry out job responsibilities. Disseminate data to others only when authorized by the concerned departments under the organization.

**User Registration and Deregistration**

1. Every staff, customer and third party, requiring access to the IT infrastructure, standalone systems and applications must have a unique user ID and a personal secret password. This user ID and password will be required to establish positive identification and authentication.
2. Human Resources department is required to inform the IT Department with up-to-date and relevant personnel details to ensure that the appropriate security controls are implemented in light of this information
3. Unique user IDs assigned so that access and modifications can be traced.
4. The user who gains access to the system / application should read and understand the Information Security policy and related policies before the logical access are granted. Non- compliance with the policies will result in disciplinary action, which is dependent on the nature and severity of the transgression.
5. The user registration should be approved by the IT Sr. Manager after reviewing the business need for the access of the requesting user.
6. The user should be deregistered or disabled when the access is no more needed.

**User identification and Authentication**

1. Users are accountable for all activities performed with their personal user IDs. User IDs shall not be utilized by anyone other than the individuals to whom they have been issued except for super administrator accounts.
2. All systems that connect to the IT infrastructure must make use of proper access controls that prohibit access to resources without proper authentication procedures
3. Every authentication process for computers connected to the IT infrastructure must (wherever possible) include a notice warning against unauthorized use and consequences thereof.

**Enforcement**

Any employee who is found to have violated this policy may be subject to disciplinary action, up to termination of employment.

Sl. No.	Policy Name	Policy No	Effective Date
4	Maker Checker Concept	ITP-004	1 <sup>st</sup> April 2021

**Maker-checker** is one of the central principles of authorization in the information systems of JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED. The principle of Maker and Checker means that for each transaction, there must be at least two individuals necessary for its completion. While one individual may create a transaction, the other individual should be involved in confirmation/authorization of the same.

There is every possibility of a mistake creeping in a transaction, if a single person handles the entire process of the transaction in the system. The Maker& Checker is a procedure followed in all major financial institutions to do away with such accidental / procedural mistakes created. This ensures that the transaction is done with four eyes principle and the person in charge who is answerable to the functions of the branch/HO as the approving authority, is part of the sanction process of the loans and other transactions in the system.

The important points of the Maker-Checker are mentioned below for deeper understanding and effective functioning.

1. The Maker is the person who enters the transaction in the computer system. He / She enters all the relevant details in the Software Module. Once entered, it is submitted for approval of the Checker.
2. The Checker is the person in charge who has to verify the details of the transaction entered by the maker logging in his / her login ID. He/ She should go through the details of the transactions entered by the maker and verify the same. Once satisfied, Checker can approve the transaction. If the Checker feel that the transaction cannot be approved for any reasons then, the Checker can reject the transaction.
3. Once approved by the Checker, the maker can go for the printing of the documents and complete the transaction.
4. Approval matrix is created based on the amount of the transaction in the application software. Branch level and HO level approvals are required to complete the transaction categorized in different hierarchy levels.
5. In case the Maker/Checker is on leave for the day or absent for short periods then he/she have to approach their reporting authority who will allot the powers of the Checker to another person, who is the in charge in the absence of the Maker/Checker. The reporting authority should take care to re allot the role of the Maker/Checker to the person of the branch/HO once the staff resumes for duty.
6. If the branch level authority cannot do this process due to leave or absent for short periods meeting etc., this can be done by the authorized HO official. This needs a prior intimation to HO official to do the change/ allotment of the Maker/Checker.

Sl. No.	Policy Name	Policy No	Effective Date
5	Information Security Policy	ITP-005	1 <sup>st</sup> April 2021

#### **Purpose**

This policy establishes the integral foundation for security standards, processes and procedures of Information Security that will be followed by the organization

#### **Scope**

The policy applies to all users of information technology within the company. Policy also applies to all dataassets of the organization which includes,

1. Intellectual property owned by company or provided by a third party.
2. Personally Identifiable Information for employees, clients or other third parties.
3. Financial and business information of the company, its employees, clients or other third parties.
4. All Public or Private data or information assets of the company.

#### **Policy**

The IT Department must establish and provide governance for information technology policies, procedures, and best practices for the company's technology infrastructure in order to secure all IT assets and promote the most efficient use of technology resources.

The IT Department will submit a report to the Board of Directors at its monthly meeting of each calendar year, and submit interim reports at the request of the Board, on the current status of the company's technology policies and procedures.

#### **Data Protection Mechanism:**

All privileged data information will be protected by data protection mechanisms to ensure the highest levels of confidentiality, integrity and availability. Non-privileged information will be protected to ensure the highest levels of integrity and availability. Information systems will check entered information for accuracy, completeness, validity and authenticity. Information systems will be configured such that they prevent unauthorized and unintended information transfer.

#### **Responsibilities of IT Department:**

1. Determine appropriate security policy requirements based on its business objectives,
2. Assessment of risk, and interpretation of legal, regulatory and contractual obligations
3. Validate that the security controls meet the company requirements driven by security policy and risk acceptance
4. Notify security requirements of changes through a change request process
5. Facilitating training for improving better IT Security controls
6. Request exceptions to the documented information security controls, as necessary

All operating units within the company that use information technology (IT) are responsible for:

1. Adhering to the IT policies issued by the IT Department.

2. Developing and implementing, when appropriate, additional IT policies and procedures specific to their operating units.
3. Promoting IT policy adherence.
4. Complying with the requirements of the IT governance model adopted by the organization.
5. Ensuring the security of the IT systems and the network to which they are connected.
6. Informing the IT Department if there are any problems with a policy or if inputs from other sources do not comply with the defined policies.
7. Providing an annual "refresher" for current employees highlighting the changes made or problem areas during the previous year.
8. Maintaining the functionality of the IT systems within their area.
9. Facilitating training and the dissemination of information.
10. Preventing unauthorized access to company information, personal files and e-mail.
11. Developing and maintaining a plan for recovery of mission critical data and systems if a loss is sustained.

Sl. No.	Policy Name	Policy No	Effective Date
6	Cybersecurity Policy	ITP-006	1 <sup>st</sup> April 2021

#### **Purpose**

Objective of the Cyber Security Policy is to preserve confidentiality, integrity and availability of organizations information or system in the Cyberspace (internet) or connected to cyberspace. Cyberspace is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it". The purpose of this policy are to ensure the appropriate and inappropriate use of company internet resources, including the use of browsers, electronic mail, instant messaging, file upload and downloads and voice communications etc.

#### **Scope**

Is to protect organization, its information assets and its stake holders from cyber-attacks or internet boneattacks. All devices, systems connected to internet and all stakeholders in the scope.

#### **Policy**

1. IT Department must ensure:
  - a. Cyber security roles and responsibilities are defined, coordinated and aligned with internal roles and external partners
  - b. Must establish a cyber-security Framework which enable to identify, protect and detect, respond and recovery from Cyber-attacks.
  - c. The organization's place in its own industry ie NBFC sector is identified and communicated to all stakeholders
  - d. Dependencies and critical functions for delivery of critical services are established
  - e. Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
  - f. Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
  - g. Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed
  - h. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cyber security program
  - i. Response and recovery planning and testing are conducted with suppliers and third-party providers
  - j. Establish Computer Emergency Response Teams (CERT) and establish practices for sharing risk-related information (e.g., threat and vulnerability information) with external entities, including those with which the organizations have a risk relationship as well as those which could supply or receive risk-related information (Other CERTs)
  - k. The organization's personnel and partners are provided cyber security awareness education and are trained to perform their cyber security-related duties and responsibilities consistent with related policies, procedures, and agreements.
  
2. Technical Controls
  - a. File Integrity checking mechanisms are used to verify software, firmware,

and information integrity

- b. A baseline configuration of IT system is created and maintained incorporating security principles
  - c. A vulnerability management system is implemented
  - d. Mechanisms (eg. failsafe, load balancing, hot swap, DOS/DDOS protection) are implemented to achieve resilience requirements in normal and adverse situations
  - e. Establish SOC and baseline of network operations and expected data flows for users and systems is established and managed. The network is monitored to detect potential cyber security events
  - f. Event data are collected and correlated from multiple sources and sensors
  - g. Physical environment and Personnel activity are monitored to detect potential cyber security events
  - h. Setup Security Continuous Monitoring for unauthorized mobile code and malicious code detection
3. Incident Response
- a. Response processes and procedures are executed and maintained, to ensure response to detected cyber security incidents and Response plan is executed during or after an incident
  - b. Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness
  - c. Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
  - d. Analysis is conducted to ensure effective response and support recovery activities
  - e. Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. Newly identified vulnerabilities are mitigated or documented as accepted risks
  - f. Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities
4. Recovery
- a. Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cyber security incidents
  - b. Recovery planning and processes are improved by incorporating lessons learned into future activities
  - c. Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, Internet Service Providers, owners of attacking systems, victims, and vendors)



Sl. No.	Policy Name	Policy No	Effective Date
7	<b>Electronic channel security Policy for Mobile Financial Services, Social Media &amp; Digital Signature Certificates</b>	ITP-007	1 <sup>st</sup> April 2021

#### **Purpose**

The organization is committed to ensuring compliance to all requirements including legal, regulatory, organizational policies and ensures any changes in the security measures to enhance e-channel security must be carried out in a controlled manner with appropriate records maintained.

#### **Scope**

All electronic channel-based assets which are owned or leased or outsourced.

#### **Policy**

1. Implement adequate security measures on the internal networks and network connections to public network or remote parties. Segregate internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment
2. Maintain access security logs and audit trails. These should be analysed for suspicious traffic and/or intrusion attempts
3. Passwords shall be encrypted when stored on the databases and should not be readable when decrypted and should also be one way hashed
4. All connections to the Applications must go through firewalls
5. Conduct regular audit to assess the adequacy and effectiveness of the risk management process and the attendant controls and security measures.
6. Perform vulnerability test or assessment to evaluate the information security policies, internal controls and procedures, as well as system and network security
7. Conduct penetration testing at least annually
8. Any High value transaction and transfer of critical information must protect by strong digital signatures.
9. Implement "end-to-end" Secure Sockets Layer (SSL) encryption that is appropriate to the sensitivity and importance of data to protect confidentiality of information while it is stored or in passage over external and internal networks. TLS – recent versions secured encryption algorithm should be used.
10. Any communication occurring in a Social Media must be respectful to the company, fellow employees, our affiliates, and our business partners.
11. The company may request at any time that you cease any communication concerning the company in Social Media or require you to block access to such communication if the company believes that such action is necessary to ensure compliance with government regulations or other laws.

Sl. No.	Policy Name	Policy No	Effective Date
8	System Generated MIS Reports	ITP-008	1 <sup>st</sup> April 2021

#### **Purpose**

The purpose of MIS is reporting and is to provide the necessary information to the managers and supervisors at various levels to help them to discharge their functions of organising, planning, control and decision making are no more relevant and useful in the process of decision making.

#### **Scope**

Provide support and maintenance to existing management information systems (MIS). Generate and distribute management reports in accurate and timely manner. Develops MIS documentation to allow for smooth operations and easy system maintenance.

#### **Policy**

1. Collect the exact requirement from the concerned department.
2. Ensure that all departments are fulfil the decision-making capacity.
3. Easy to understand.

Sl. No.	Policy Name	Policy No	Effective Date
9	System Generated COSMOS Returns	ITP-009	31-Aug-18

**Purpose**

To know the extent of participation of NBFCs in Interest rate Future market. ... Concerned NBFCs are required to file the specified returns online through COSMOS application.

**Scope**

Cosmos is Microsoft's internal data storage/query system for analysing enormous amounts (as in petabytes) of data. ... The Scope article in particular provides an architectural overview of the system and breaks Cosmos into three parts: Storage, Execution Management and Query Language

**Policy**

1. Collect the exact requirement from the concerned department.
2. Ensure that all departments are fulfil the decision-making capacity.
3. Easy to understand.

Sl. No.	Policy Name	Policy No	Effective Date
10	Business Continuity Planning Policy	ITP-010	1 <sup>st</sup> April 2021

### **Purpose**

The purpose of this policy is to create and maintain a Business Continuity Plan (BCP) for the IT support of critical company processes. An effective plan allows the company to minimize the adverse effect of emergencies that arise. The Company has an ethical obligation to the organization's workforce, shareholders, and customer stakeholders to protect the continuing operations of the business.

### **Scope**

This policy encompasses all IT processes and technology that supports critical business functions.

### **Policy**

The IT Department is responsible for creating, maintaining, and testing the IT Business Continuity Plan. The following activities must be performed:

#### **Identify Critical Processes.**

To identify the business processes critical to the company's financial and legal well-being, a bi-annual Business Impact Analysis (BIA) is conducted. The result is a Recovery Time Objective—that point at which company losses become intolerable (Recovery Time Objective—RTO). The IT Business Recovery Plan must ensure that critical IT processes (equipment and software) can be recovered at a remote site within the RTO.

The IT Department initiates and submit the BIA. The BIA will:

1. Encompass all departments and areas of the company.
2. Identify the point in time that the financial and legal issues seriously threaten the company's survival.
3. Identify the processes required to meet all regulatory requirements.
4. Include a risk assessment of natural and man-made risks to the critical processes.

#### **Business Continuity Planning.**

The IT Department will assemble plans for every identified critical business function.

1. Develop the plan.
  - a. Develop plans for the recovery IT processes, equipment, and software for all critical business processes identified by the BIA. These plans must address steps necessary to re-establish the IT functions at an emergency recovery location.
  - b. Based on the BIA, publish a restoration priority list of all critical technologies.
  - c. Create an emergency notification program to ensure the prompt notification of executive management in a crisis

2. Maintain the plan.
  - a. Test all IT Business Continuity Plans at least bi-annually to demonstrate the ability to achieve the BIA determined Recovery Time Objective. Conduct a lessons-learned session with all participants to capture and incorporate improvements into the plans.
  - b. Report all test results to the management by IT Department within 30 days of the test's completion.
3. Training.
  - a. Train all members of the IT department in their roles in supporting the BCP.
  - b. Train all new employees on their roles within 30 days of joining the department

Coordinate with other company disaster plans. The IT manager will coordinate the IT BCP with:

1. The Facilities Disaster Recovery plan and the Security/Safety department's crisis plan.
2. The various business recovery plans of other departments.

Sl. No.	Policy Name	Policy No	Effective Date
11	Data Backups and Retention Policy	ITP-011	1 <sup>st</sup> April 2021

#### **Purpose**

This policy guides the frequency and type of data backups. It also addresses the length of time that backups must be retained.

#### **Scope**

The policy applies to all devices that hold or accumulate data in the support of critical company operations, to include servers, business applications, data base, surveillance systems, access controls, voice logger, Firewall devices, Telecommunications switches, PCs etc.

#### **Policy**

The IT Department is responsible for making and retaining an adequate number of data backup "safety" copies. To accomplish this, the IT Department may create further policies and procedures and delegate authority to implement them.

#### **Devices**

Data backups will be made of all devices that contain or collect data, to include at a minimum:

1. Servers and their internal disks
2. Storage Area Networks
3. Telecommunications switches (PBX)
4. surveillance systems
5. Desktop /Laptop PCs
6. Firewall

#### **Types of Data**

1. Personal data is not to be stored on company equipment.
2. Legal compliance data—must be identified. The label on the backup media must include what data it contains and the appropriate retention period. Care must be taken to ensure the data is securely stored.
3. Business critical data—must be identified. The label on the backup media must include what data it contains and the appropriate retention period. Quick access to this data is required in the event of a disaster.
4. Non-critical data—must be identified. Non-critical data is not legally required to be retained for a period of time. Typically this data is deleted after 13 months. The label on the backup media must include what data it contains and the appropriate retention period.

#### **Data Backup Frequency**

The frequency of data backups is determined by how frequently and how much a data storage element change.

1. Full backups weekly—all data is backed up weekly and retained for 12 months.
2. Incremental backups daily for changing data. These are retained for 30



days.

3. Off-site journaling is used for immediate backup of critical data that cannot be reconstructed from daily backups.

#### **Data Retention**

The organization retention period is determined by the data element with the longest required retention period on that backup media. If the contents of the media are not known, then the media must be retained for a minimum of seven years.

#### **Off-site Storage**

1. Data backups will be transported off site every week after the backups are created.
2. Once every calendar quarter, the IT Department will audit the off-site storage process to ensure that:
  - a. Media is kept in a climate-controlled environment during transit.
  - b. The storage facility is secure and fire proof.
  - c. The storage facility is climate controlled.
  - d. The data centre security is appropriate for media going out and for media coming in.
  - e. There is a documented chain of custody for backup media from the point it leaves the datacentre until it is returned.

#### **Data Destruction**

Data that has outlived its usefulness to the business, and whose age exceeds the legal limits for retention, must be properly destroyed.

1. The media must be rendered permanently unreadable. This is primarily accomplished through physical destruction. Paper documents are shredded, burned, and the ashes pulped. CDs and magnetic media are shredded.
2. When data is destroyed, it must be documented as to whom, by what means, when, and what the data consisted of data.



Sl. No.	Policy Name	Policy No	Effective Date
12	E-mail Usage and Retention Policy	ITP-012	1 <sup>st</sup> April 2021

### **Purpose**

This policy defines the acceptable use of the company's corporate e-mail system. The objectives of this policy are to outline appropriate and inappropriate use of JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED's e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

### **Scope**

The policy applies to all uses of company owned e-mail accounts and all company e-mail records.

### **Policy**

#### **Acceptable Uses of Company E-mail Accounts**

The company provides e-mail accounts for business usage only. Every staff member has the responsibility to maintain and enhance the company's public image and to use the company's e-mail system in a responsible and productive manner that reflects well on the company.

#### **Unacceptable Uses of Company E-mail Accounts**

Company e-mail accounts may not be used for transmitting, retrieving, viewing, or storage of any communications of a discriminatory or harassing nature or materials that are obscene. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference shall be transmitted. No excessively abusive, profane, or offensive language is to be transmitted through the company's e-mail system. E-mail messages or attachments may also not be used for any purpose that is illegal or against company policy or contrary to the company's best interests. Solicitation of non-company business, or any use of the company e-mail system for personal gain, is prohibited.

#### **Communications**

Each employee is responsible for the content of all text, audio, or images that he or she places or sends over the company's e-mail system. All e-mails must contain the identity of the sender and may not represent the sender as someone else or someone from another company.

Any messages or information sent by an employee to another individual outside the company via an electronic network (e.g., blog, IM, bulletin board, online service, or Internet) are statements that reflect on the company. While some users include personal "disclaimers" in electronic messages, there is still a connection to the company, and the statements may legally be tied to the company. Therefore, we require that all communications sent by employees via the company's e-mail system comply with all company policies and not disclose any confidential or proprietary company information.

#### **Privacy**

E-mails are not private. The company reserves the right to monitor e-mail content ensuring that the e-mail system is used for appropriate purposes. Also, no security is hundred percent hacker-proof; someone outside the company may intercept and read e-mail. Routing of e-mail is not without errors; someone other than the intended recipient may receive the e-mail. Do not send anything by e-mail that should not be placed on the company bulletin board.

#### **Personal E-mail Accounts**

Accessing personal e-mail accounts is prohibited from company-owned computers, as they are a potential source of computer viruses. No company-related communication is permitted using personal e-mail accounts, as the communication may be subject to the company's communication retention policy.

#### **Spam**





Sending unwanted e-mail of any kind (spam) using a company e-mail account is prohibited.

### **Copyright Issues**

Employees on the company's Internet system may not transmit copyrighted materials belonging to entities other than this company. Please note that non-adherence to this policy puts the company in serious legal jeopardy and opens the company up to significant lawsuits and public embarrassment. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify, or forward copyrighted materials, except with permission. Failure to observe copyright or

license agreements may result in disciplinary action up to and including termination. If you have questions about any of these legal issues, please speak with your manager or IT department before proceeding.

### **Monitoring**

The company routinely monitors usage patterns in its Internet communications. The reasons for this monitoring include cost analysis, security, bandwidth allocation, and the general management of the company's gateway to the Internet. All messages created, sent, or retrieved over the company's Internet are the property of the company and should be considered public information. Notwithstanding comments above regarding our present intention not to monitor content, the company must reserve the right to access and monitor the content of all messages and files on the company's Internet system at any time in the future with or without notice. Employees should not assume electronic communications are totally private and should transmit highly confidential data in other ways. Electronic messages regarding sensitive matters should warn that such communications are not intended to be secure or confidential. This is just good business sense.

### **Retention**

Company communications of any kind typically needs to be retained as you would any other corporate document. Please remember that e-mails deleted from your e-mail inbox are still saved on the company e-mail server. E-mails that are not managed as part of the corporate document retention policy are kept archived for seven years before being permanently deleted.

### **Attachments**

Attachments with the following file extensions are prohibited, as they are potential security and virusthreats:

.bat	Batch processing file used to execute system commands or programs.
.com	Windows command files.
.cpl	Control panel extension.
.exe	Windows binary executable files.
.js	Java script files.
.ocx	Object linking and embedding control.
.pif	Program information file used to tell Windows how to run non-Windows applications.
.scr	Screen saver programs; may include binary code.
.sys	System configuration files.
.vb	Visual Basic script files.



There is also a limit of 10MB of attachments for any e-mail message. Contact the IT Helpdesk if you have a need to transfer more than 10MB of files at any one time.

**Confidentiality**

Any e-mail message that is meant to be confidential must be labeled as such in the subject line. Forwarding of confidential messages requires the permission of the original sender. The corporate e-mail system will automatically attach a confidential message notification to all e-mails that are sent to addresses outside the organization. Do not attach your own individual confidentiality notice as this will be redundant and may be inconsistent with the official company message.

**Violations**

Any employee who abuses the privilege of company-facilitated access to the Internet will be subject to corrective action up to and including termination. If necessary, the company also reserves the right to advise appropriate legal officials of any illegal violations.

---

**BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE  
AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

- 25. Legal Department**
- 26. Administration Department**
- 27. HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**





**JEWL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023 (w.e.f. 19.04.2022)**

In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies Policy on loans and advances to directors and senior officers

**RBI/2022-23/29**  
**DOR.CRE.REC. No.25/03.10.001/2022-23**

**POLICY ON LOANS AND ADVANCES TO DIRECTORS AND SENIOR OFFICERS**

<b>S No</b>	<b>Particulars</b>	<b>Remarks</b>
1	Introduction	-
2	Definitions	
3	Regulatory Restrictions on Loans and Advances	
4	Loans and advances to Real Estate Sector	
5	Provisions of Companies Act, 2013	
6	Annexure- A & B	

Amendment Details, if any:



## **INTRODUCTION:**

In compliance with the Regulatory Framework for NBFCs introduced by the Reserve Bank of India ('RBI'), a Master Circular was issued on Scale Based Regulation (SBR)- A Revised Regulatory Framework for NBFCs. The said circular apart from the other scale-based regulations provided for certain regulatory restriction on the loans extended by NBFCs to their directors, senior officers and relatives thereof. As per the said circular the company is categorized as NBFC- Middle Layer and accordingly the regulations as applicable for NBFC- Middle layer shall be complied with.

In accordance with the above the "Board of Directors" ("Board") of JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED ("the Company") has formulated a Policy on grant of loans to directors, senior officers and relatives of directors and to entities where directors or their relatives have major shareholding.

## **DEFINITIONS**

- (i) "Board of Directors" or "Board" means the Board of Directors of the company, as constituted from time to time.
- (ii) "Company" means JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED.
- (iii) "Managing Director" as per clause (54) of Section 2 of the Companies Act, 2013, means a director who, by virtue of the articles of a company or an agreement with the company or a resolution passed in its general meeting, or by its Board of Directors, is entrusted with substantial powers of management of the affairs of the company and includes a director occupying the position of managing director, by whatever name called.
- (iv) "Senior Officer" shall have the same meaning as assigned to "Senior Management" under Section 178 of the Companies Act, 2013 which shall mean personnel of the company who are members of its core management team excluding Board of Directors comprising all members of management one level below the executive directors, including the functional heads.
- (v) "Employee" means those employees who are on the payroll of the company.
- (vi) "Control" as per Clause (27) of Section 2 of the Companies Act, 2013, shall include the right to appoint majority of the directors or to control the management or policy decisions exercisable by a person or persons acting Individually or in concert, directly or indirectly, including by virtue of their shareholding or management rights or shareholders agreements or voting agreements or in any other manner.
- (vii) "Relative" as per Clause (77) of Section 2 of the Companies Act, 2013, "relative", with reference to any person, means anyone who is related to another, if—
  - i) they are members of a Hindu Undivided Family;
  - ii) they are husband and wife; or
  - iii) one person is related to the other in such manner as may be prescribed;



- iv) **“Major shareholder”** shall mean a person holding 10 % or more of the paid-up share capital or five crore rupees in paid-up shares, whichever is lower.

### **REGULATORY RESTRICTIONS ON LOANS AND ADVANCES LOANS AND ADVANCES TO DIRECTORS**

Unless sanctioned by the Board of Directors, the Company shall not grant any loans and advances aggregating Rupees Five crores and above to —

- (i) its directors (including the Chairman/ Managing Director, if any) or relatives of the directors;
- (ii) any firm in which any of the Directors of the Company or their relatives are interested as a partner, manager, employee or guarantor; and
- (iii) any company in which any of the Directors of the Company, or their relatives are interested as a major shareholder, director, manager, employee or guarantor.

Provided that Director or his/her relatives shall be deemed to be interested in a Company, being the subsidiary or holding company, if they are major shareholder or in control of the respective holding or subsidiary company.

Provided that the Director who is directly or indirectly concerned or interested in any proposal shall disclose the nature of their interest to the Board of Directors when any such proposal is discussed. Such interested directors shall recuse themselves from the meeting, subject to their presence being required by the other directors for the purpose of eliciting information and the Director so required to be present shall not vote on any such proposal.

The proposals for credit facilities of an amount being less than Rupees Five crore, to the borrowers shall be sanctioned by the Financial Advisory and Asset & Liability Management Committee (committee) of the Company under powers vested by board. All the proposals approved by the committee shall be reported to the Board of Directors on quarterly basis.

In case any of the committee members is interested in the proposal for grant of loan, he/she shall rescue himself/ herself from the discussion over the said agenda and the remaining members forming the quorum shall consider the proposal.

The terms and conditions for loans amounting to Rs.10 Lakhs or more are covered as annexure-B. Further, any credit facility below the amount of Rs. 10 Lakhs shall continue to be governed by the terms and conditions as covered in the Loan Policy of the company.

Further the committee may approve interest free salary advances up to 20% of annual salary / incentive payable to the Managing Director and the Senior officers. However, any such approval shall be subject to the limits of the committee and the grant of such assistance shall be reported to the Board on quarterly basis. Further no subsequent advances shall be allowed, until the settlement of the previous advances extended.

For the purpose of grant of loan to the directors or senior officials, as previously mentioned:



- (i) The Company shall obtain a declaration from the borrower giving details of the relationship of the borrower with the directors/ senior officers of the Company for loans and advances aggregating Rupees Five crore and above. The Company shall recall the loan if it comes to their knowledge that the borrower has given a false declaration.
- (ii) These guidelines shall be duly brought to the notice of all directors and placed before the NBFC board of directors.
- (iii) The Company shall disclose in its Annual Financial Statement, aggregate amount of such sanctioned loans and advances in the format as annexed (Annexure A) to this policy

The above norms shall equally apply to awarding of contracts to the directors their relatives or the senior officials.

### **LOANS AND ADVANCES TO REAL ESTATE SECTOR**

While appraising loan proposals involving real estate, the company shall ensure that the applicant has obtained prior permission from government/ local government/ other statutory authorities for the project, wherever required. To ensure that the loan approval process is not hampered on account of this, while the proposals may be sanctioned in normal course, the disbursements shall be made only after the borrower has obtained requisite clearances from the government / other statutory authorities.

For the purpose application of regulatory restrictions on grant of Loans and Advances above, the term 'loans and advances' will not include loans or advances against -

- a) Government securities
- b) Life insurance policies
- c) Fixed deposits
- d) Stocks and shares
- e) Any loans granted to an employee of the company under any scheme applicable generally to employees.

Provided that company's interest/lien is appropriately marked with legal enforceability.

### **PROVISIONS OF COMPANIES ACT, 2013**

The policy, in addition to the foregoing provisions, shall also cover the provisions of the Companies Act 2013 with regard to Loans & Advances to the Directors. In compliance with the provisions of Section 185 of the Companies Act, 2013, the company shall not either directly or indirectly, advance any loan, to any of its directors or to any other person in whom the director is interested or give any guarantee or provide any security in connection with any loan taken by him or such other person.

The expression —"to any other person in whom director is interested" shall mean and include:

- a) any director of the lending company, or of a company which is its holding company or any partner or relative of any such director;
- b) any firm in which any such director or relative is a partner;
- c) any private company of which any such director is a director or member;



- d) any body corporate at a general meeting of which not less than twenty-five per cent. of the total voting power may be exercised or controlled by any such director, or by two or more such directors, together; or
- e) any body corporate, the Board of directors, managing director or manager, whereof is accustomed to act in accordance with the directions or instructions of the Board, or of any director or directors, of the lending company.

However, giving of any loan to a Managing or Whole-time director:

- (i) as a part of the conditions of service extended by the company to all its employees; or
- (ii) pursuant to any scheme approved by the members by a special resolution shall be exempted.

BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED

Director

---

**CC:**

- 28. Legal Department
- 29. Administration Department
- 30. HR Department

---

Dated this the 01<sup>st</sup> Day of April, 2023



## Loans to Directors, Senior Officers and relatives of Directors

Particulars	Current Year	Previous Year
Directors and their relatives		
Entities associated with directors and their relatives		
Senior Officers and their relatives		





**Annexure-B**  
**Terms and conditions**

Loans amounting to Rs. 10.00 Lakhs or more to directors & Senior Officers and their relatives shall be granted as per the following terms and conditions.

- 1) Purpose – as defined in the existing loan policy of the company duly approved by board of directors
- 2) Security –
  - (i) Third party guarantee / mortgaged property having means / value of proposal not less than 125% of loans.
  - (ii) Lien / Hypothecation on assets being financed.
  - (iii) Collaterals to be vetted by company's approved advocate & valuer if obtained.
- 3) Rate of Interest – The rate of interest chargeable from the director or Senior officers (including their relatives) shall be equal to the cost of funds (being the financial cost at which the funds are raised by the company) during the financial year previous to the year in which the loan is being given

BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED

Director

---

**CC:**

31. Legal Department
  32. Administration Department
  33. HR Department
- 

Dated this the 01<sup>st</sup> Day of April, 2023





**JEWL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies the guidelines to be followed while granting loan products and providing services of the company.

**RISK MANAGEMENT POLICY**

**7. Name:**

These guidelines may be called in The Risk Management Policy– 2023-24

**8. Effective Date**

They shall come into force on 01<sup>st</sup> April, 2023.

**9. Applicability:**

This policy is applicable to all loans sanctioned by the company

Risk Management Policy

<b>Policy Name</b>	Risk Management Policy
<b>Issue and Effective date</b>	01 <sup>st</sup> April, 2023
<b>Periodicity of review</b>	Annual
<b>Owner / Contact</b>	Compliance
<b>Approver</b>	Board of Directors
<b>Annexures</b>	Sample Risk Control Matrix Sheet- Annexure-A

**1. Preamble**

The Board of Directors (“Board”) of JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED (“Company” or “JEWEROCK” ), has adopted the following policy which encompasses practices relating to identification, assessment, monitoring and mitigation of various risks to the business. Risk Management Policy of the Company seeks to minimize unfavorable impact on the business objectives and develop stakeholder value. Further, the risk management practices seek to sustain and enhance long-term competitive advantage for the Company.

**2. Purpose**

This Policy has been framed in accordance with the Risk Management framework as issued by Reserve Bank of India (“RBI”) vide Master Direction DNBR. PD. 008/03.10.119/2016-17 dated September 01, 2016 (“RBI Circular”) and amendments thereon.

The purpose of this policy is to address unanticipated and unintended losses to the human resources & financial assets of the Company without unnecessarily limiting the activities that advance its mission and goals. JEWELROCK has introduced effective risk management systems that address the issues relating to various risks. The effective management of risk is vital to the continued growth of the Company.



### 3. Principles

For risk management to be effective, all operations/departments of the Company must apply the following principles to the context of the business and its objectives:

- Risk management must create and protect value
- Risk management is integrated into organisational processes.
- Explicit risk management helps decision-makers make informed choices.
- Risk management is focused on the sources of uncertainty around the achievement of objectives
- Risk management must be tailored to the context and fit for purpose

**Risk management is dynamic, iterative and responsive to change**

### 4. Definitions

- **“Board”** means Board of Directors of the Company.
- **“Company/ JEWEROCK”** means JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED
- **“Directors”** mean individual Director or Directors on the Board of the Company.
- **“Policy”** means Risk Management Policy
- **“RBI”** means Reserve Bank of India
- **“RCM”** means Risk Control Matrix

### 5. Policy

JEWELROCK recognizes that Risk management as one of the key drivers of growth and further to enhance corporate governance. Accordingly, the Board has framed the following Risk Management Policy:

- To continuously thrive for available risks in the organization which directly or indirectly effect the functioning of the organization.
- To ensure the protection of rights & values of Shareholders by establishing a well- organized Risk Management Framework.
- Selecting, maintaining and enhancing the risk management tools used by the Program to provide analyses that inform and support the investment actions of the entire Organization.

### 6. Identification, Measurement and Assessment of Risk

- Management’s responsibility, as delegated by the Board, is to operationalize the Risk Management Program and ensure that formal procedures are put in place to identify and define risk with input from representatives across the businesses.
- Measurement of risk is completed considering both quantitative and qualitative means using the likelihood and impact criteria as developed by Management and as reviewed by the Board.
- The management has identified certain inherent and residual risks which have been divided in accordance with likelihood and its impact on the business.

- Following risks have been identified by the organization:



S No	Types of Risks at JEWELROCK
1	Regulatory & Compliance Risk
2	Human Resource Risk
3	Reputational Risk
4	Strategic Risk
5	Operational Risk
6	Market Risk
7	Financial Risk
8	Credit & Concentration Risk

- **Strategic Risk** – This risk is related to the overall business strategies and the related economic/business environment
- **Operational Risk**- Arising out of technology failure, fraud, error, inadequate financial capacity to fulfil obligations and/ or to provide remedies, outsourcing of activities to vendors.
- **Market Risk**- Risks related to changes in various markets in which the Company operates.
- **Financial Risk**- These risks includes movement in interest rates and also liquidity risks inherent to the business
- **Reputational Risk** – Where the practices followed by the Company are not in consonance with industry as well as internally prescribed standards.
- **Credit & Concentration Risk** – Where the overall industry has considerable exposure to one service provider and hence the NBFC may lack control over the service provider.
- **Regulatory & Compliance Risk** – Where privacy, consumer and prudential laws are not adequately complied with by the service provider
- **Human Resource Risk**- Where the employee related factors are not handled cautiously such as safety, security, compensation, etc.

## 7. Risk Categorization and Mitigation Factors

The following broad categories of risks have been identified in our risk management framework along with possible mitigation factors:

### Strategic Risk

- **Risk:** It is the risk to earnings and capital arising from lack of responsiveness to changes in the business environment and/or adverse business decisions, besides adoption of wrong strategies and choices.
- **Mitigation:** The management is proactive in its approach towards changes in economic/business environment as the business strategies are regularly discussed with the senior officials of the organization so that adequate steps can be taken. Also, important strategic matters are referred to the Board, consisting of members with diversified experience in the respective fields, for intense deliberations, so as to derive the benefit of collective wisdom. The management has also obtained Director's and Officers liability insurance in order to protect the Board and Senior management from taking decisions during the course of their duties which might adversely affect the business.



### Reputational risk

- **Risk:** Reputational risk is related to adverse perception of the image or the company, on the part of customers, counterparties, shareholders, investors and regulators. It refers to the potential adverse effects, which can arise from the company's reputation getting tarnished due to factors such as unethical practices, regulatory actions, customer dissatisfaction and complaints leading to negative publicity. Presence in a regulated and socially sensitive industry can result in significant impact on Company's reputation and brand equity as perceived by multiple entities like the RBI, Central/State/Local authorities, banking industry and the customers. The risk can emanate from:
  - o Non-Compliance with Regulations
  - o Customer Dissatisfaction
  - o Misrepresentation of facts and figures in public
- **Mitigation:** Considering the business model the following aspects have been put in place to reduce vulnerability related to reputational risk:
  - o **Compliance with Fair Practices Code:** All employees are trained and instructed to follow fair practices as per RBI prescribed guidelines in all their dealings with the customers.
  - o **Grievance Redressal Mechanism (GRM):** The Company has a defined GRM in place and the same is communicated to all customers at the time of sanction of loan. This is also available on the website of the Company.
  - o **Delinquency Management:** The Company does not resort to any coercive recovery practices and all recoveries are made in accordance with the Recovery policy and Fair Practice Code of the Company.
  - o **Stringent Selection Criteria:** Vendors, employees and other associates of the Company are selected after confirming to the stringent criteria's prescribed by the management.
  - o **Reference Check:** The management carries out a reference check for all the vendors from the market before having them on Board so as to ensure utmost integrity while carrying out their duties.
  - o **Legal Obligations:** All employees, vendors and associates are required to sign legal contracts wherein specific clauses related to non-disclosure are entered so as to ensure the Company from any reputational risks.

- **Market Risk**

- **Risk:** Risks emanating out of the choices we make on markets, resources and delivery model that can potentially impact our long-term competitive advantage. Risks relating to inherent characteristics of our industry including competitive structure, technological landscape, extent of linkage to economic environment and regulatory structure
- **Mitigation:** Management regularly reviews its business model



including the areas it wants to operate. The management carries out regular competitive analysis of its peers in the industry so as to remain in competition and change its markets if required.

- **Operational Risk**

- **Risk:** Risks inherent to business operations including those relating to client acquisition, service delivery to clients, business support activities, information security, physical security, human resource and business activity disruptions.

- Mitigation:

- o **Document Storage and Retrieval:** JEWELROCK recognizes the need for proper storage of documents as also their retrieval for audit and statutory requirements. The Company is maintaining all the original documents in a fire proof vault at a dedicated space allocated for specific purpose.

- o **Physical Storage:** We have entered into an agreement with an established record management company, so all the physical loan documents are bar-coded

and stored in a specialized secure facility.

- o **Scanned Copies:** We have also started storing scanned copies of the loan documents for easy retrieval especially for audit purposes where physical documents are not required.

- o **Whistle Blower/Fraud Prevention Policy-** JEWELROCK encourages all its employees to report any non-compliance of stated company processes or policies without fear as we have a clearly stated “no-retaliation” policy. We have a formal policy that details the manner in which such issues are handled – background investigation, holding a hearing by a committee, and ensuring that action as per the committee’s recommendations is carried out. All issues reported are categorized for nature and severity:

- Financial or Non-Financial
- Major or Minor
- Procedural Lapse or Gross Violation
- Breach in Process or Disciplinary Issue

The Compliance Manager maintains a record of all the entire case history which is signed off by senior management on closure.

- o **Internal Audits:** Internal Audit at Branch Offices and at the Corporate/Regional Offices which were carried out on a half-yearly basis till FY15, are now carried out on a quarterly basis from FY16 by an independent audit firm appointed by the Board. The scope of this Internal Audit covers all key functions including HR, Operations, Credit, Administration, Finance and Accounts. All significant audit observations of Internal Audits and follow-up actions are presented to the Board Audit Committee.

- o **Internal Financial Control:** In compliance with requirement of the



new Companies Act 2013, the company has appointed an external advisory firm with key focus on Corporate Governance, IT Infrastructure, Enterprise Risk Management, Anti-Fraud Program and Financial Reporting, Process Flow Charts, Standard Operating Procedures, Risk Control Matrices, Control Design, Operating Effectiveness, Continuous Monitoring.

- **Technology Infrastructure:** The company has leverage of cloud-based technologies and all its business applications are hosted in secure data centers with mirrored redundancies such that in the event of any system going down, an alternate system is made operational within hours. At the facilities where back-office and financial operations take place, alternate/back-up connectivity has been provisioned such that in the event connectivity is lost with one service provider, the alternate connection can be utilized.
- **Outsourcing Policy:** The Company has established an Outsourcing policy in accordance with RBI guidelines wherein a detailed check is done for all the outside vendors before any work is outsourced.

- **Financial Risk**

**Interest Risk:** Interest rate risk is the risk where changes in market interest rates might adversely affect an NBFC's financial condition. The changes in interest rates affect company in some way. The immediate impact of changes in interest rates is on company's earnings (i.e. reported profits) by changing its Net Interest Income (NII). As such JEWELROCK is into funding of loans which are always fixed rate loans. The company manages this risk on NII by pricing its loan products to customers at a rate which covers interest rate risk. The risk from the earnings perspective can be measured as changes in the Net Interest Income (NII) or Net Interest Margin (NIM). Measurement of such risk is done at the time of deciding rates to be offered to customers. Once interest rate risk is measured, lending rates are finalized. Given the interest rate fluctuation, the company has adopted a prudent & conservative risk mitigation strategy to minimize interest risk.

**Liquidity Risk:** Measuring and managing liquidity needs are vital for effective operations of an NBFC. The importance of liquidity transcends individual institutions, as liquidity shortfall in one institution can have repercussions on the entire system. Board/ALM Committee should measure not only the liquidity positions of company on an ongoing basis but also examine how liquidity requirements are likely to evolve under different assumptions. Experience shows that assets commonly considered as liquid, like government securities and other money market instruments, could also become illiquid when the market and players are unidirectional. Therefore, liquidity has to be tracked through maturity or cash flow mismatches. For measuring and managing net funding requirements, the use of a maturity ladder and calculation of cumulative surplus or deficit of funds at selected maturity dates is adopted as a standard tool.

- **Maturity Mismatch:** Liquidity Risk arises largely due to maturity mismatch associated with assets and liabilities of the company. Liquidity risk stems from the inability of the company to fund increase in assets, manage unplanned changes in funding sources and meet financial commitments when required.
- **External Source of funds:** Due to the high reliance on external sources of funds, JEWELROCK is exposed to various funding and liquidity risks comprising:
- **Funding Concentration Risk**—Concentration of a single source of funds exposes the Company to an inability to raise funds in a planned and timely



manner and resort to high cost emergency sources of funds. Further, concentration of funding sources can also result in a skewed maturity profile of liabilities and resultant Asset-Liability mismatch.

- **Asset-Liability Mismatch**—A skewed asset-liability profile can lead to severe liquidity shortfall and result in significantly higher costs of funds; especially so during times of crises.
- **Market Perception Risk**—Due to inherent industry characteristics, the Company is exposed to perception risks, which can lead to decline in ability of a lender to increase exposure to the Microfinance sector and result lack of adequate and timely inflow of funds.
- **Leverage Risk**— A high degree of leverage can severely impact the liquidity profile of the company and lead to default in meeting its liabilities.

**Mitigation:** The key liquidity management policies being followed at JEWELROCK include:

- **Regular ALM Meetings:** This is done to identify any short term liquidity gaps and thereby take immediate corrective actions to bridge the same
- **Lender Exposure Updates:** The exposure profile to the lenders is regularly updated to ensure that skewness does not creep in in respect of the sources of external funds.
- **Floating Rates:** JEWELROCK currently borrows all its loans on a floating basis as against the entire lending on a fixed rate basis. This minimizes the impact of any adverse impact in the event of a credit shock in the banking system and any continuing effects of the same on overall interest rates in the economy and on JEWELROCK.
- **Defined Leverage Levels:** JEWELROCK targets a leverage of maximum 2x in light of the business model and adequately safeguard itself against the impact of adverse market conditions. It also affords JEWELROCK reasonable time to tie-up timely equity infusion.
- **Capital Adequacy:** JEWELROCK targets to maintain healthy levels of capital adequacy - historically, in excess of 50%. The Company maintains a strong capital position with the capital ratios well above the thresholds defined by the regulatory authorities through continuous and timely capital infusion.

- **Credit and Concentration Risk**

**Credit Risk:** Any lending activity by the Company is exposed to credit risk arising from repayment default by borrowers and other counterparties. Despite best efforts, there can be no assurance that repayment default will not occur and, in such circumstances, may have an effect on its results of operations. The Company and its subsidiaries may not be able to realize the full value of its collateral or be delayed in realizing such value, due to, among other things, legal proceedings by defaulting borrowers and/ or security providers, and stagnation or reduction in market value of collateral. A failure to recover the expected value of collateral security could expose the Company to a potential loss. Any such losses could adversely affect the Company's financial condition and results of operations.

**Mitigation:** A strong credit risk management process helps in containing the portfolio quality of the company. Key elements of the credit risk management include a structured and standardized credit approval process supported by a strong system, effective training programs, legal and technical due diligence, monitoring and robust credit risk management strategy at a senior management level.

**Portfolio Concentration Risk:** Portfolio Concentration Risk is the risk to the company due to a





very high credit exposure to a particular business segment, industry, geography, location, etc though in the context of micro finance, it pertains predominantly to geographical concentration.

**Mitigation:** JEWELROCK intends to maintain a diversified exposure in advances across various sectors and geographies but to mitigate the risks that could arise due to political or other factors within a particular state. The Company has steadily diversified into various sectors and geographies and consequently the portfolio has become diversified. The Company has also started lending for consumer durables, personal loans and consumption loans. As a part of credit appraisal process, before establishing any new relationship, various factors are taken including credit history, project size, other borrowings, etc. are considered. Various 3<sup>rd</sup> party verifications are also carried to secure credit facilities. Various loan covenants are also established in the documents to secure the loans.

- **Regulatory and Compliance Risk**

- **Risk:** The company is exposed to risk attached to various statutes and regulations. The company is mitigating the risk through regular review of legal compliances carried out through internal as well as external compliance audit. JEWELROCK is present in an industry where the Company has to ensure compliance with regulatory and statutory requirements. Non- Compliance can result in stringent actions and penalties from the Regulator and/or Statutory Authorities and which also poses a risk to Company's reputation. These risks can be:
  - Non-Compliance with RBI Regulations
  - Non-Compliance with Statutory Regulations
  - Non-Compliance with covenants laid down by Lenders

- Mitigation:

- The company has implemented AVANTIS, a Compliance Management System with in-built workflows to track, update and monitor compliances.
- Internal Audit also conducts audit of compliance function on a quarterly basis wherein all regulatory compliances are reviewed in detail.
- Quarterly Compliance Certificate certified by the CFO is submitted to the Board on quarterly basis.

- **Human Resource Risk**

- **Risk:** JEWELROCK's Human Resource adds value to the entire company by ensuring that the right person is assigned to the right job and that they grow and contribute towards organizational excellence. Our growth has been driven by our ability to attract top quality talent and effectively engage them in right jobs. Risk in matters of human resources are sought to be minimized and contained by following a policy of providing equal opportunity to every employee, inculcate in them a sense of belonging and commitment and also effectively train them in spheres other than their own specialization. Employees are encouraged to make suggestions on innovations, cost saving procedures, free exchange of other positive ideas etc. It is believed that a satisfied and committed employee will give of his best and create an atmosphere that cannot be conducive to risk exposure. Employee- compensation is always subjected to fair appraisal systems with the participation of the employee and is consistent with job content, peer comparison and individual performance

- Mitigation:

Human Resource Policy and initiatives: Various programs and initiatives are carried out by the HR to retain talent and motivate them on a regular basis.

## 8. Responsibility

Responsibility for risk management is shared across the organization. Key responsibilities include:



- Controlling the risks through a formal program is necessary for the well-being of the organization and everyone in it. The jobs and services the organization provides, the safety of the workplace and other benefits all depend to an extent on our ability to control risk.
- The Board is responsible for satisfying itself annually, or more frequently as required, that management has developed and implemented an effective risk management framework. Detailed work on this task is delegated to the Audit Committee and reviewed by the full Board.
- The Audit Committee assists the Board in overseeing the group's risk profile and is responsible for overseeing management's actions in the identification, management and reporting of material business risks.

**9. Reporting Requirements**

The Organization, Enterprise reporting process will evolve as requirements and risk management leading practice evolve. Annual content will include a risk profile setting out the most significant risks faced by the enterprise, and for each risk will:

- describe the risk;
- document the key activities and controls to mitigate/manage the risk;
- identify the residual risk;
- refer to action plans taken to address any weaknesses; and
- draft a risk appetite statement for each key strategic risk.

Further, on a quarterly basis, updated information materially affecting the risk profile (e.g. market developments) will be provided which will enable the Board to understand the likely future risk profile of the Enterprise. These will be reported to the Board by the Audit Committee as soon as practicable and at least quarterly. The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate risk level and type of mitigation to be applied. This assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies as and when required. In case of the change in perception the risk assessment in case of PEP borrower should be again done to ascertain whether it is prudent to continue with the exposure with such PEP borrower or not. In case it is felt that the funds are not safe, the funds should be recalled immediately without delay.

BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED

Director

---

**CC:**

- 34. Legal Department
  - 35. Administration Department
  - 36. HR Department
- 

Dated this the 01<sup>st</sup> Day of April, 2023





**JEWL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023 (w.e.f. 19.04.2022)**

In exercise of the powers of the board of directors conferred by the Articles of Association of the company and pursuant to the guidelines issued by the Reserve Bank of India, the board hereby notifies Policy on Prevention, Prohibition and Redressal of Sexual Harassment at Workplace

**POLICY ON PREVENTION, PROHIBITION AND REDRESSAL OF SEXUAL HARASSMENT AT WORKPLACE**

<b>Policy Name</b>	POLICY ON PREVENTION, PROHIBITION AND REDRESSAL OF SEXUAL HARASSMENT AT WORKPLACE
<b>Issue and Effective date</b>	01 <sup>st</sup> April, 2023
<b>Periodicity of review</b>	Annual
<b>Owner / Contact</b>	Compliance
<b>Approver</b>	Board of Directors
<b>Annexures</b>	Format of Compliant Letter



<b>INDEX</b>		
<b>S No</b>	<b>Particulars</b>	<b>Page No</b>
1	Commitment	3
2	Scope	3
3	Objectives	3
4	Responsibilities	3
5	Applicability	4
6	Words, Expression and Abbreviations	4
7	Legal Background	4
8	Policy Guidelines	4
9	Constitution of Internal committee	5
10	Procedures for filing complaint	5
11	Procedures to be followed post receipt of complaint	6
12	Guidelines to be kept in mind by ICC while recommending action	7
13	Employer (Management of Establishment) to ensure	7
14	Appeal by the aggrieved person	8
15	Awareness	8
16	False accusation	8
17	Miscellaneous	9
18	Conclusion	9
19	Annexure	10
20	ICC – MEMBERS LIST 2023-24	12



## **POLICY ON PREVENTION, PROHIBITION AND REDRESSAL OF SEXUAL HARASSMENT AT WORKPLACE**

This policy (hereinafter “the Policy”) has been framed in accordance with the provisions of “The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013” and rules framed thereunder (hereinafter “the Act”). Accordingly, while the Policy covers all the key aspects of the Act, for any further clarification reference shall always be made to the Act and in the event of any conflict between the Policy and the provisions of the Act, the provisions of the Act shall prevail.

### **1. Commitment**

JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED (hereinafter “the Company”) is committed to providing work environment that ensures every employee is treated with dignity and respect and afforded equitable treatment. The Company is also committed to promoting a work environment that is conducive to the professional growth of its employees and encourages equality of opportunity. The Company will not tolerate any form of sexual harassment and is committed to take all necessary steps to ensure that its employees are not subjected to any form of harassment.

### **2. Scope**

This policy applies to all categories of employees of the Company all over India, including permanent, management and workmen, temporary, trainee and contracted, at their workplace. This policy proposes a zero-tolerance attitude against any kind of Sexual Harassment or discrimination by any employee during their tenure in the Company towards any women employee of the Company or its Customers, Vendors and Contractors in the workplace.

### **3. Objective**

The objective of this Policy is to create and maintain a safe work environment, free from sexual harassment and discrimination for all its employees as per the guidelines of “The Sexual Harassment of Women at Workplace (Prevention, Prohibition & Redressal) Act, 2013. The Policy lays down the guidelines and the process to be followed in order to provide protection against sexual harassment of women at workplace and for the prevention and redressal of complaints of sexual harassment, in addition to the matters connected therewith or incidental thereto.

### **4. Responsibilities Regarding Sexual Harassment**

All employees of the Company have a personal responsibility to ensure that their behavior is not contrary to this Policy. All employees are encouraged to reinforce the maintenance of a work environment free from sexual harassment.



## 5. Applicability

This Policy is known as **Policy on Prevention, Prohibition and Redressal of Sexual Harassment at Workplace** and is applicable to all employees of JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED (and / or others coming under the Provisions of the Act), at all locations.

## 6. Words, Expressions & Abbreviations

In this policy document, unless there is anything repugnant to the subject or context thereof, the words and expressions as stated below shall have the following meaning: -

- a) CE – Complainant Employee – Refers to any woman employee (as per section 2(a) of the Act) who has lodged a complaint of sexual harassment at workplace by another employee (hereinafter referred to as 'respondent').
- b) ICC – Internal Complaints Committee.
- c) Management– Management includes the person or board or committee responsible for formulation and administration of policies for the Company.
- d) RE – Respondent Employee - Refers to any employee against whom the complaint for sexual harassment has been lodged.
- e) Workplace – Includes all offices, branches and workplace of the Company located anywhere in India. It also includes any places visited by the employees arising out or during the course of employment including transportation approved by the management of the establishment for undertaking the journey.

## 7. Legal Background

The Parliament of India enacted the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 to lay down mechanisms for prevention of sexual harassment and redressal of Complaints, beside matters connected therewith or incidental thereto. This policy has been framed in accordance with the provisions of "The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013".

## 8. Policy Guidelines

Sexual harassment is not only a serious misconduct but criminal offence also, which can destroy human dignity and freedom. To promote the well-being of all women employees at the workplace, this Policy envisages as under: -

- a) It shall be the duty of Management of the establishment to prevent or deter the commission of any act of sexual harassment at the workplace.
- b) Sexual harassment will be considered as misconduct and action will be taken based on the findings of enquiry in this context.
- c) The definition of sexual harassment is as per Section 2 (n) of the Act and which includes: -

"Sexual Harassment" includes any one or more of the following unwelcome acts or behavior (whether directly or by implication) namely: -



- (1).Physical contact and advances; or
  - (2).A demand or request for sexual favours; or
  - (3).Making sexually coloured remarks; or
  - (4).Showing pornography; or
  - (5).Any other unwelcome physical, verbal or non-verbal conduct of sexual nature.
- d) The following circumstances, among other circumstances, if it occurs or is present in relation to or connected with any act or behaviour is deemed sexual harassment: -
- (1).Implied or explicit promise of preferential treatment in her employment; or
  - (2).Implied or explicit threat of detrimental treatment in her employment; or
  - (3).Implicit or explicit threat about her present or future employment status; or
  - (4).Interference with her work or creating an intimidating or offensive or hostile work environment for her; or
  - (5).Humiliating treatment likely to affect her health or safety.

#### **9. Constitution of Internal Complaints Committee (hereinafter referred to as ICC)**

The Company has constituted an Internal Complaints Committee (ICC) in accordance with section 4 of the Act for redressal of sexual harassment complaint (made by the victim) and for ensuring time bound treatment of such complaints. The name of the committee members of ICC and changes therein will be notified from time to time.

#### **10. Procedure for filing a complaint**

Any aggrieved woman may make, in writing, a complaint of sexual harassment at workplace to ICC giving details of the sexual harassment meted out to her within a period of 3 months from the date of incident and in case of a series of incidents, within a period of 3 months from the date of last incident, which may be extended for a further period of 3 months, if circumstances warrant such extension, in the opinion of the Internal Complaints Committee. The complaint by an aggrieved woman shall be made to the ICC in writing and be sent either by post or e-mail on the id [posh@jewelrockfinance.com](mailto:posh@jewelrockfinance.com) or given in person to the ICC or any person authorized by ICC.

The ICC may, giving reasons to be recorded in writing, extend the time limit not exceeding 3 months, if it is satisfied that the circumstances were such which prevented the employee from filing a complaint within the set period. Where the employee is unable to make complaint on account of her physical or mental incapacity or death or otherwise, her legal heir or such other person as may be prescribed may register the complaint.



It is however, pertinent to state that where the aggrieved woman is unable to make complaint on account of her physical incapacity a complaint may be filed by:

- a) Her relative or friend; or
- b) Co-worker; or
- c) An officer of the National or State Commission for Women; or
- d) Any person who has knowledge of the incident, with the written consent of the aggrieved woman.

Where the aggrieved woman is unable to make complaint in case of mental incapacity, a complaint may be filed by:

- a) Her relative or friend; or
- b) A special educator; or
- c) A qualified psychiatrist or psychologist; or
- d) A guardian or authority under whose care she is receiving treatment or care; or
- e) Any person who has knowledge about the incident jointly with her relative or friend.

**Note:**

- a) Where the aggrieved woman is unable to make a complaint for any other reason, a complaint may be filed by any person who has knowledge of the incident, with her written consent.
- b) Where the aggrieved woman is dead, a complaint may be filed by any person who has knowledge of the incident, with the written consent of her legal heir.

**11. Procedure to be followed post receipt of complaint**

- a) The committee will go through the complaint and evaluate if there is or not prima- facie case of sexual harassment. While doing that, the ICC will keep in mind that the CE is not subjected to enquiry for more than once. However, if the complaint complexity requires that the CE is to be called more than once for the enquiry, then the utmost sensitivity would be displayed, and adequate precaution would be taken to ensure there is no loss of dignity to CE.
- b) The ICC will initiate a detailed enquiry as deemed fit.
- c) The ICC may, before initiating an enquiry and at the request of CE, take steps to settle the matter between her and the RE through conciliation, provided that no monetary settlement shall be made as a basis for conciliation. Where a settlement has been arrived during conciliation, the ICC shall record the settlement and forward to the Management for ensuring action as recorded under the settlement. The copies of the settlement as recorded shall be provided to both the parties. However, if the terms arrived during conciliation have not been complied with by the RE, the ICC shall proceed to make an enquiry into the complaint.





- d) The ICC shall after complete the enquiry, submit its recommendations to the Management with recommendations of the penalty to be imposed.
- e) In case no settlement is arrived the ICC, shall, where the Respondent is an employee, proceed to make enquiry into the complaint in accordance with the provisions of the service rules.
- f) Where both the parties are employees, the parties shall, during the course of inquiry, be given an opportunity of being heard and the copy of the findings shall be made available to both the parties enabling them to make representation against the findings before the Committee.
- g) The submission of the recommendations by the ICC to the Management shall be completed within a period of ninety (90) days from the date of receipt of complaint by the ICC.
- h) The HR Department will extend full cooperation in facilitating to conduct the proceedings by the ICC.

**Important:** For the purpose of making an inquiry under the Act, the Internal Complaints Committee shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) when trying a suit in respect of the following matters, namely:

- a) Summoning and enforcing the attendance of any person and examining on oath;
- b) Requiring the discovery and production of documents; and
- c) Any other matter which may be prescribed.

**12. Guidelines to be kept in mind by ICC while recommending action**

- a) To conduct the inquiry as per the principles of natural justice and in a confidential manner;
- b) In cases where the ICC has recommended to Management for compensation to be made to the CE, then the said amount shall be deducted from the salary of the RE and paid to the CE or her legal heir/s;
- c) In case the employer is unable to deduct from the salary, then he RE may be directed to pay such sum to the CE and if RE fails to pay the sum referred as above, the ICC may forward the order for recovery as an arrear of land revenue to the concerned District Officer and such District Officer shall act within 60 days of receipt by him.

**13. Employer (Management of the establishment) to ensure**

- a) That in case there is a complaint against any of the ICC members, Management will have to reconstitute the ICC by removing from the ICC the member against whom there is complaint. In all cases, guidelines as defined by the above clauses would be exclusive of the time taken to reconstitute the said committee.
- b) The Management will provide assistance to the CE if she so chooses to file a police complaint in relation to the offence under the Indian Penal Code or any other law for the time being in force.



- c) The Management will also initiate action under the Indian Penal Code or any other law for the time being in force, against a perpetrator who is not an employee of the Establishment and there is complaint of Sexual Harassment against the said perpetrator in the workplace.
- d) The ICC will submit an annual report to the Management as outlined in the Act and the Management shall record the requisite information in the Company's Annual Report in the applicable format.
- e) The Management will assist in ensuring the attendance of the RE and witnesses before the ICC as the case may be.
- f) The Management will monitor the timely submission of the reports. For this the Management will conduct periodic update meetings with the ICC and the HR dept. to ensure that the said policy is being implemented in letter and spirit.

#### **14. Appeal by the aggrieved person**

Any person aggrieved by any of the following may file an Appeal to the Managing Director of the Company (MD) or an official authorized by him against:

- (i) the finding of the ICC that the allegations against the respondent has not been proved during the enquiry, or
- (ii) if the Management fails to take action on a complaint under the Act, or
- (iii) if the Management fails to implement the decisions based on the recommendations of the ICC,
- (iv) if the Management fails to recover from the RE the amount determined to be payable to the aggrieved employee or legal heir, or
- (v) if the ICC arrived at a conclusion that during the enquiry any witness has given false evidence or produced any forged or misleading document, or
- (vi) when persons entrusted with the duty to handle or deal with the complaint, the enquiry or recommendations, publish the contents of the complaint and the enquiry proceedings in contravention of Sec 16 of the Act. In case the aggrieved employee is not still satisfied by the outcome of the Appeal, he / she may proceed with legal action as provided under the Act or generally.

#### **15. Awareness**

All the Employees, Agents, Customers, Vendors, Partners and Visitors shall have access to this Policy at any given point of time and clarification related to this Policy shall be addressed by the HR team. The Company shall comply with all other details as set out under Section 19 of the Act to ensure that all employees are provided with the safe working environment at the workplace.

#### **16. False Accusations**



The complaint of sexual harassment made by any employee shall be taken up with utmost seriousness by the Company. However, there shall be zero tolerance for any false accusation. If the Internal Complaints Committee comes to a conclusion that the allegation was made with malicious intent or the aggrieved person or any other person making the complaint on behalf of the aggrieved person produced false or forged or misleading documents to prove his/her case, the Internal Complaints Committee may recommend action to be taken against the person who has made the complaint. In such a case, malicious intent has to be established after an inquiry, before any action is recommended. A mere inability to substantiate a complaint or provide adequate proof would not attract action as provided herein. A similar recommendation for taking action would be recommended against any witness whom the Internal Complaints Committee concludes has given false evidence or produced forged or misleading documents.

#### **17. Miscellaneous**

Company may make any alteration or amendment or rescind any of the clauses of this Policy as and when it finds it necessary to do so, as long as it complies with the Act. Any such alterations or amendment or rescinding will be intimated to the employees.

Nothing contained in these rules shall operate in derogation of any law for the time being in force or to the prejudice of any right of any employee under any other Rules or Law.

#### **18. Conclusion**

Complaints relating to Sexual Harassment shall be handled and investigations will be conducted under the principles of natural justice, basis of fundamental fairness, in an impartial and confidential manner so as to protect the identity of all viz., the person bringing the charge, potential witnesses, and the person accused of improper behaviour. Also, all efforts shall be taken to ensure objectivity and thoroughness throughout the process of investigation. The identity and address of the aggrieved person, respondent and witnesses must not be published or disclosed to the public or media. The decision of the Company shall be final and binding on all. However, the same is without prejudice to any recourse that the Company or any individual concerned may have against any other concerned person and it shall not limit or restrict the rights of any of the concerned persons including the Company to pursue, nor shall they be precluded from pursuing, such further and other legal actions as may be available.

#### **Note:**

The policy will be overall governed by “The Sexual Harassment of Women at the Workplace (Prevention and Redressal) Act, 2013”. The copy of the Act is



available at our Corporate HR office. A format of the complaint is annexed which can be used for preparing complaint.



**Annexure**

**Format of Complaint regarding sexual harassment at workplace**

To,  
Internal Complaints Committee,  
JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED  
First Floor, Sreepadam Arcase, West Nada, Guruvayur  
Thrissur, Kerala, India - 680101

Madam,  
I am working as a \_\_\_at\_\_\_ in the establishment. I am constrained to make a complaint of sexual harassment against\_(full name, designation, place of work)

ADD THE DETAILS OF THE INCIDENT.

I am making the above complaint for appropriate action as contemplated under “The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013” and rules framed thereunder, and the Company’s policy framed thereunder.

Dated this the \_\_\_\_\_ day of \_\_\_\_\_

Yours’ Faithfully  
Signature  
Name

Name, Status (Relationship) and  
address of the Complainant.

BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED

Director

---

**CC:**

1. Legal Department
2. Administration Department
3. HR Department

---

Dated this the 01<sup>st</sup> Day of April, 2023



**ICC – COMMITTEE MEMBERS FOR THE FY 2023-24**

<b>Sl. No.</b>	<b>Name</b>	<b>Designation</b>	<b>Position in the Committee</b>	<b>Contact Details Address Mobile No. &amp; Email ID</b>
1.			Presiding Officer	
2.			Member (External)	
3.			Member and Convener	
4.			Member	
5.			Member	
6.			Member	
7.			Member	





**THE RESERVE BANK –  
Integrated Ombudsman Scheme, 2021:**

---

**JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED**

Reg. Office: 23/112-1,23/112-6(OLD NO.5/89-13) THRISSUR CORPORATION 23RD DIVISION, JESWAYBLDG, CHEMBUKKAVU NA KIZHAKKUMPATTUMPATTUKARA THRISSUR KL 680005 IN | E-mail : [jewelrockleasing@gmail.com](mailto:jewelrockleasing@gmail.com) | [headoffice@jewelrock.com](mailto:headoffice@jewelrock.com) | [www.jewelrockgoldloan.com](http://www.jewelrockgoldloan.com) | Phone 0487 2998988 | CIN: 65921KL1996PTC009845

## The Reserve Bank – Integrated Ombudsman Scheme, 2021:

### Salient Features

#### Scheme covers customers of the following Regulated entities: -

- Any Bank
- Any NBFCs, other than Core Investment Company (CIC), an Infrastructure Debt Fund-Non Banking Financial Company (IDF-NBFC), a Non-Banking Financial Company - Infrastructure Finance Company (NBFC-IFC), a company in resolution or winding up/liquidation, or any other NBFC specified by the Reserve Bank
- Any System participant as defined under Payment and Settlement Systems Act, 2007

#### Grounds for filing a complaint by a customer:

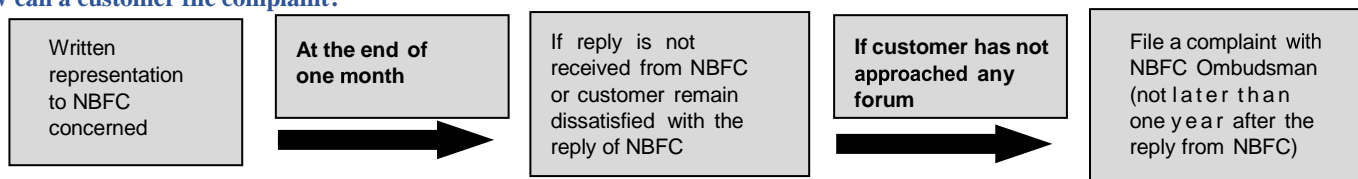
Any act or omission of above-mentioned regulated entities resulting in deficiency in Service

#### Grounds for non-maintainability of a Complaint:

No complaint for deficiency in service shall lie under the Scheme in matters involving:

- commercial judgment/commercial decision of a Regulated Entity
- a dispute between a vendor and a Regulated Entity relating to an outsourcing contract
- a grievance not addressed to the Ombudsman directly
- general grievances against Management or Executives of a Regulated Entity
- a dispute in which action is initiated by a Regulated Entity in compliance with the orders of a statutory or law enforcing authority
- a service not within the regulatory purview of the Reserve Bank
- a dispute between Regulated Entities; and
- a dispute involving the employee-employer relationship of a Regulated Entity

#### How can a customer file complaint?



#### How does Ombudsman take decision?

- Proceedings before Ombudsman are summary in nature
- Promotes settlement through conciliation. If not reached, can issue Award/Order

#### Can a customer appeal, if not satisfied with decision of Ombudsman?

**Yes**, If Ombudsman's decision is appealable. Appellate Authority: Executive Director in-Charge of the Department of the Reserve Bank administering the scheme.

#### Note:

- This is an Alternate Dispute Resolution mechanism
- Customer is at liberty to approach any other court/forum/authority for the redressal at any stage
- Refer to [www.rbi.org.in](http://www.rbi.org.in) for further details of the Scheme



ദ റിസർവ് ബാങ്ക് - ഇൻഗ്രേറ്റഡ് ഓംബുഡ്സ്മാൻ , 2021:
പ്രധാന സവിശേഷതകൾ
താഴെ പറയുന്ന നിയന്ത്രിത സ്ഥാപനങ്ങളിലെ കസ്റ്റമർമാരാണ് ഈ സ്കീമിൽ പെടുന്നത്
<ul style="list-style-type: none"> <li>• ഏത് ബാങ്കും</li> <li>• കോർ ഇൻവെസ്റ്റ്മെന്റ് കമ്പനി (CIC) അല്ലാത്ത ഏത് NBFC യും ഒരു ഇൻഫ്രാസ്ട്രക്ചർ ഡെവ്ലപ്മെന്റ് ഫണ്ട് ബാങ്കിംഗ് ഇതര ഫിനാൻഷ്യൽ കമ്പനി IDF-NBFC ഒരു ബാങ്കിംഗ് ഇതര ഫിനാൻഷ്യൽ കമ്പനി - ഇൻഫ്രാസ്ട്രക്ചർ ഫിനാൻഷ്യൽ കമ്പനി NBFC-IFC - തീർപ്പ് ആയതോ ഫിനാൻസ് കമ്പനി അടച്ചുപൂട്ടൽ / ലിക്വിഡേഷനിൽ ഉള്ളതോ ആയ കമ്പനി അല്ലെങ്കിൽ റിസർവ് ബാങ്ക് നിഷ്കർഷിച്ചതുപോലുള്ള മറ്റേതെങ്കിലും NBFC</li> <li>• 2007 ലെ പെയ്മെന്റ് ആന്റ് സെറ്റിൽമെന്റ് സിസ്റ്റത്തിൽ നിർവചിച്ചിരിക്കുന്ന പ്രകാരമുള്ള ഏതെങ്കിലും സിസ്റ്റം പാർട്ടിസിപ്പന്റ്</li> </ul>
കസ്റ്റമർമാർക്ക് ഒരു പരാതി ഫയൽ ചെയ്യാൻ കാരണങ്ങൾ
സേവനത്തിൽ അപര്യാപ്തത വരുത്തുന്നതിലേക്ക് വഴി തെളിക്കുന്ന, മുകളിൽ പ്രതിപാദിച്ചിരിക്കുന്ന നിയന്ത്രിത കമ്പനികളുടെ ഏതെങ്കിലും പ്രവൃത്തിയോ വിട്ടു പോകാലോ
ഒരു പരാതി കൈകാര്യം ചെയ്യാതിരിക്കാനുള്ള കാരണങ്ങൾ :
താഴെപ്പറയുന്ന കാര്യങ്ങളിൽ സേവനങ്ങളിലെ അപര്യാപ്തതയെക്കുറിച്ചുള്ള പരാതികൾ സ്കീമിനു കീഴിൽ വരുന്നില്ല.
<ul style="list-style-type: none"> <li>• ഒരു റെഗുലേറ്റഡ് / നിയന്ത്രിത സ്ഥാപനത്തിന്റെ കമേർഷ്യൽ വിധി / വാണിജ്യ വിധി / കമേർഷ്യൽ തീരുമാനം വാണിജ്യ തീരുമാനം</li> <li>• ഒരു കോൺട്രാക്ട് / ഉടമ്പടി ഔട്ട്സോഴ്സ് ചെയ്യുന്നതുമായി</li> </ul>

ബന്ധപ്പെട്ട ഒരു വെൻഡറും നിയന്ത്രിത സ്ഥാപനവും തമ്മിലുള്ള തർക്കം.
<ul style="list-style-type: none"> <li>• നേരിട്ട് ഓംബുഡ്സ്മാൻ നൽകുന്നതല്ലാത്ത പരാതി</li> </ul>
<ul style="list-style-type: none"> <li>• ഒരു നിയന്ത്രിത സ്ഥാപനത്തിന്റെ മാനേജ്മെന്റ് അല്ലെങ്കിൽ എക്സിക്യൂട്ടീവ്മാർക്ക് പരാതിയുള്ള പൊതു പരാതി</li> </ul>
<ul style="list-style-type: none"> <li>• ഒരു സ്റ്റാറ്റൂട്ടറി അല്ലെങ്കിൽ നിയമം നടപ്പിലാക്കുന്ന അധികാരിയുടെ ഉത്തരവുകലനുസരിച്ചു നിയന്ത്രിത സ്ഥാപനം തുടങ്ങിവെച്ച പ്രവർത്തനത്തിന്മേലുള്ള തർക്കം</li> </ul>
<ul style="list-style-type: none"> <li>• റിസർവ് ബങ്കിന്റെ നിയന്ത്രിത പരിധിക്കുള്ളിലല്ലാത്ത സേവനം</li> </ul>
<ul style="list-style-type: none"> <li>• നിയന്ത്രിത സ്ഥാപനങ്ങൾ തമ്മിലുള്ള തർക്കം</li> </ul>
<ul style="list-style-type: none"> <li>• ഒരു നിയന്ത്രിത സ്ഥാപനത്തിലെ ജീവനക്കാരും തൊഴിൽദാതാവും തമ്മിലുള്ള തർക്കം</li> </ul>
<b>ഒരു കസ്റ്റമർ പരാതി നൽകുന്നതെങ്ങനെ ?</b>
ബന്ധപ്പെട്ട NBFC ക്കുള്ള എഴുതി തയ്യാറാക്കിയ നിവേദനം
ഒരു മാസത്തിന്റെ അവസാനം
NBFC യിൽ നിന്നും മറുപടി ലഭിച്ചില്ലായെങ്കിൽ അല്ലെങ്കിൽ NBFC യുടെ മറുപടിയിൽ കസ്റ്റമർ തൃപ്തരല്ലെങ്കിൽ
<b>കസ്റ്റമർ ഒരു ഫോറത്തിനെയും സമീപിച്ചിട്ടില്ലെങ്കിൽ</b>
NBFC ഓംബുഡ്സ്മാന്റെ ഫയൽ പരാതി നൽകുന്നു (NBFC യിൽ നിന്നുള്ള മറുപടിക്കുശേഷം ഒരു വർഷത്തിനുള്ളിൽ)
<b>ഓംബുഡ്സ്മാൻ തീരുമാനമെടുക്കുന്നതെങ്ങനെ ?</b>
<ul style="list-style-type: none"> <li>• ഓംബുഡ്സ്മാന്റെ മുന്നിലുള്ള നടപടി ക്രമങ്ങൾ .....</li> </ul>
<ul style="list-style-type: none"> <li>• സമവായത്തിലൂടെയുള്ള തീർപ്പ് പ്രോത്സാഹിപ്പിക്കുന്നു. ഒത്തുതീർപ്പിലെത്തി ചെർന്നില്ലെങ്കിൽ അവാർഡ് / ഓർഡർ പുറപ്പെടുവിക്കും</li> </ul>
ഓംബുഡ്സ്മാന്റെ തീരുമാനത്തിൽ തൃപ്തിയില്ലെങ്കിൽ കസ്റ്റമാർമാർക്ക്

<p><b>അപ്പീൽ പോകാമോ?</b></p> <p>അതെ, ഓംബുഡ്സ്മാന്റെ തീരുമാനത്തിൽ അപ്പീൽ പോകാമെങ്കിൽ അപ്പെലേറ്റ് അതോറിറ്റി / അധികാരി റിസർവ് ബാങ്കിലെ സ്കീം നടപ്പിലാക്കുന്ന വകുപ്പിന്റെ ചാർജുള്ള എക്സിക്യൂട്ടീവ് ഡയറക്ടർ</p>
<p><b>കുറിപ്പ്:</b></p> <ul style="list-style-type: none"> <li>• ഇത് പകരം വയ്ക്കാവുന്ന പരാതി പരിഹാര സംവിധാനമാണ്.</li> <li>• കസ്റ്റമർക്ക് ഏത് ഘട്ടത്തിലും പരാതി പരിഹാരത്തിനായി മറ്റേതൊരു കോടതിയും / ഫോറത്തെയും / അധികാരിയും സമീപിക്കാനുള്ള സ്വാതന്ത്ര്യമുണ്ട്</li> <li>• സ്കീമിനെക്കുറിച്ച് ചുറ്റുമുള്ള കൂടുതൽ വിവരങ്ങൾക്കായി <a href="http://www.rbi.org.in">www.rbi.org.in</a> റെഫർ ചെയ്യുക.</li> </ul>



**JEWEL/LEGAL/NOTIFICATION**  
**Thrissur, April 01, 2023**

**CUSTOMER SECURITY TIPS**

**Mobile Security Precautions**

**Do's**

1. Password protect the mobile phone and never give your mobile phone to anyone.
2. Choose a strong password to keep your account and data safe.
3. Review your account statements frequently to check for any unauthorised transactions.
4. Change your PIN regularly.
5. Report a lost or stolen phone immediately to your service provider and law enforcement authorities.

**Don'ts**

1. Never give your PIN or confidential information over the phone or internet. Never share these details with anyone.
2. Don't click on links embedded in emails/social networking sites claiming to be from JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED or representing JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED.
3. Don't transfer funds without due validation of the recipient, as funds once transferred cannot be reversed.
4. Don't store sensitive information such as credit card details, mobile banking password and user ID in a separate folder on your phone.
5. Don't forget to inform JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED of changes in your mobile number to ensure that SMS notifications are not sent to someone else.
6. Never reveal or write down PINs or retain any email or paper communication from JEWEL ROCK HIRE PURCHASE AND LEASING PRIVATE LIMITED with regard to the PIN or password
7. Be cautious while accepting offers such as caller tunes or dialer tunes or open/download emails or attachments from known or unknown sources
8. Be cautious while using Bluetooth in public places, as someone may access your confidential data/information
9. Be careful about the websites you are browsing. If it does not look authentic, do not download anything from it.



### **Secure Phone Banking**

1. While talking to the Phone Banking officer, never disclose the following:
  - 4 digit ATM/IVR PIN
  - OTP
  - Net Banking password
  - CVV (Card Verification Value)
2. Ensure that no one see you entering you PIN (personal identification number).
3. Avoid giving verification details to the Phone Banking officer while in public places.
4. The Phone Banking channel is meant to be used by the account holder only. Do not transfer the line or hand over the phone to any other person after you complete self-authentication.

### **Secure Computer Usage**

1. Use licensed software. Software purchased from untrustworthy sources could have virus or trojans that could corrupt your files and reveal your confidential data.
2. Protect your computer accounts with strong passwords
3. Update your computer with latest security patches for your operating system, browser and email client.
4. Use anti-virus, anti-spyware and personal firewalls

### **Creating Safe and Secure Passwords – Do's**

1. Keep alphanumeric passwords that are at least 8 characters long. Mix upper and lowercase letters, and special characters like \$, @, \*, etc.
2. Be creative and think of a password that is really different as well as difficult to guess. You can use phrases in sentences such as "nature's wrath tsunami" to frame your passwords as they are easy to remember and difficult to crack.
3. Place punctuation or numbers randomly.

### **Don'ts**

1. Don't use dictionary-based words, your spouse's name or your date of birth. These are easy to crack or guess.
2. Don't use sequences of letters or numbers. E.g.: abcd1234. asdfg123 etc.
3. Do not keep the same passwords for multiple accounts. Once hackers have guessed one password, they'll often try to see if it works on other accounts.
4. Do not write down your passwords.



5. Don't use personal information like your name, date of birth, PAN number, etc.
6. Change your passwords once in every three months.

### **Protecting Your Password**

1. Memorize your PIN. Don't write down your password or PIN anywhere especially not on your card.
2. Change your PIN/passwords at regular intervals.
3. If you suspect that someone knows your PIN/Password, change it immediately.
4. Don't send your password or PIN to anyone via email or text message.
5. Don't say your password or PIN aloud in public where other people can hear you.
6. Don't have your browser remember your card/account password.

### **Secure Internet Browsing**

1. Observe click discipline while browsing through different websites. You may land up clicking on to malicious link that could download malicious code / software or virus on to your computer.
2. Downloading software from non-trustworthy sites including torrent sites may lead to infecting your computer with virus.
3. Read privacy policy of the website before entering personal information such as name and email ID. Be aware of how your information would be used by the website owner.
4. Do not share copies of KYC documents with unidentified persons, unverified/unauthorized Apps. You are requested to report such Apps/Bank Account information associated with the Apps to concerned law enforcement agencies or can file complaint using Sachet portal through the link : <https://sachet.rbi.org.in/Complaints/Add>

**BY THE ORDER OF THE BOARD  
For JEWEL ROCK HIRE PURCHASE  
AND LEASING PRIVATE LIMITED**

**Director**

---

**CC:**

1. **Legal Department**
2. **Administration Department**
3. **HR Department**

---

**Dated this the 01<sup>st</sup> Day of April, 2023**



# BE(A)WARE



**A BOOKLET  
ON  
MODUS OPERANDI  
OF  
FINANCIAL FRAUDSTERS**



**RESERVE BANK OF INDIA**







## Table of Contents

	Subject	Page No.
	<a href="#"><u>Preface</u></a>	1
	<a href="#"><u>Part A - Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks</u></a>	2
1	<a href="#"><u>Phishing links</u></a>	3
2	<a href="#"><u>Vishing calls</u></a>	4
3	<a href="#"><u>Frauds using online sales platforms</u></a>	5
4	<a href="#"><u>Frauds due to the use of unknown / unverified mobile apps</u></a>	6
5	<a href="#"><u>ATM card skimming</u></a>	7
6	<a href="#"><u>Frauds using screen sharing app / Remote access</u></a>	8
7	<a href="#"><u>SIM swap / SIM cloning</u></a>	9
8	<a href="#"><u>Frauds by compromising credentials through search engines</u></a>	10
9	<a href="#"><u>Scam through QR code scan</u></a>	11
10	<a href="#"><u>Impersonation on social media</u></a>	12
11	<a href="#"><u>Juice jacking</u></a>	13
12	<a href="#"><u>Lottery frauds</u></a>	14
13	<a href="#"><u>Online job frauds</u></a>	15
14	<a href="#"><u>Money mules</u></a>	16
	<a href="#"><u>Part B - Modus Operandi and Precautions to be taken against Fraudulent Transactions - NBFCs</u></a>	17
1	<a href="#"><u>Fake advertisements for grant of loans</u></a>	18
2	<a href="#"><u>SMS / Email / Instant Messaging / Call scam</u></a>	19
3	<a href="#"><u>OTP based frauds</u></a>	20
4	<a href="#"><u>Fake loan websites / App frauds</u></a>	21
5	<a href="#"><u>Money circulation / Ponzi / Multi-Level Marketing (MLM) scheme frauds</u></a>	22
6	<a href="#"><u>Loans with forged documents</u></a>	23
	<a href="#"><u>Part C - General precautions to be taken for financial transactions</u></a>	24
	<a href="#"><u>Glossary</u></a>	32



## Preface

There has been a surge in usage of digital modes of payment in the recent years. This gained further momentum during the Covid-19 induced lockdowns. While enhancing customer convenience, it also furthered the national objective of financial inclusion. However, as the speed and ease of doing financial transactions has improved, the number of frauds reported in retail financial transactions have also gone up. Fraudsters have been using innovative methods to defraud the common and gullible people of their hard-earned money, especially the new entrants in the use of digital platforms who are not entirely familiar with the techno-financial eco-system.

This booklet has been compiled from various incidents of frauds reported as also from complaints received at the offices of RBI Ombudsmen to provide maximum practical information of value, especially to those who are inexperienced, or not so experienced, in digital and electronic modes of financial transactions. The booklet is intended to create awareness among the members of public about the modus operandi adopted by fraudsters to defraud and mislead them, while also informing them about the precautions to be taken while carrying out financial transactions. It emphasizes the need for keeping one's personal information, particularly the financial information, confidential at all times, be-ware of unknown calls / emails / messages, practicing due diligence while performing financial transactions and changing the secure credentials / passwords from time to time. Hence the title **BE(A)WARE** – Be Aware and Beware!

This booklet is part of the public awareness initiative by the Consumer Education and Protection Department, Reserve Bank of India and has been conceptualized by the office of Ombudsman, Mumbai-II.



## Modus Operandi and Precautions to be taken against Fraudulent Transactions - Banks





## 1. Phishing links

### Modus Operandi

- Fraudsters create a third-party phishing website which looks like an existing genuine website, such as - a bank's website or an e-commerce website or a search engine, etc.
- Links to these websites are circulated by fraudsters through Short Message Service (SMS) / social media / email / Instant Messenger, etc.
- Many customers click on the link without checking the detailed Uniform Resource Locator (URL) and enter secure credentials such as Personal Identification Number (PIN), One Time Password (OTP), Password, etc., which are captured and used by the fraudsters.



### Precautions

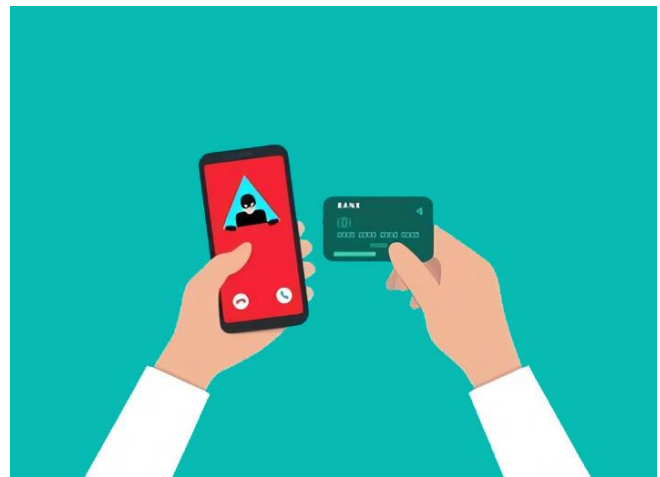
- Do not click on unknown / unverified links and immediately delete such SMS / email sent by unknown sender to avoid accessing them by mistake in future.
- Unsubscribe the mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.
- Always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
- Check URLs and domain names received in emails for spelling errors. In case of suspicion, inform



## 2. Vishing calls

### Modus Operandi

- Imposters call or approach the customers through telephone call / social media posing as bankers / company executives / insurance agents / government officials, etc. To gain confidence, imposters share a few customer details such as the customer's name or date of birth.
- In some cases, imposters pressurize / trick customers into sharing confidential details such as passwords / OTP / PIN / Card Verification Value (CVV) etc., by citing an urgency / emergency such as - need to block an unauthorised transaction, payment required to stop some penalty, an attractive discount, etc. These credentials are then used to defraud the customers.



### Precautions

- Bank officials / financial institutions / RBI / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP.
- Never share these confidential details with anyone, even your own family members, and friends.



### 3. Frauds using online sales platforms

#### Modus Operandi

- Fraudsters pretend to be buyers on online sales platforms and show an interest in seller's product/s. Many fraudsters pretend to be defence personnel posted in remote locations to gain confidence.
- Instead of paying money to the seller, they use the "request money" option through the Unified Payments Interface (UPI) app and insist that the seller approve the request by entering UPI PIN. Once the seller enters the PIN, money is transferred to the fraudster's account.



#### Precautions

- Always be careful when you are buying or selling products using online sales platforms.
- Always remember that there is **no need to enter PIN / password** anywhere to **receive** money.
- If UPI or any other app requires you to enter PIN to complete a transaction, it means you will be sending money instead of receiving it.



#### 4. Frauds due to the use of unknown / unverified mobile apps

##### Modus Operandi

- Fraudsters circulate through SMS / email / social media / Instant Messenger, etc., certain app links, masked to appear similar to the existing apps of authorised entities.
- Fraudsters trick the customer to click on such links which results in downloading of unknown / unverified apps on the customer's mobile / laptop / desktop, etc.,
- Once the malicious application is downloaded, the fraudster gains complete access to the customer's device. These include confidential details stored on the device and messages / OTPs received before / after installation of such apps.



##### Precautions

- Never download an application from any unverified / unknown sources or on being asked/ guided by an unknown person.
- As a prudent practice before downloading, check on the publishers / owners of the app being downloaded as well as its user ratings etc.
- While downloading an application, check the permission/s and the access to your data it seeks, such as contacts, photographs, etc. Only give those permissions which are absolutely required to use the desired application.



## 5. ATM card skimming

### Modus Operandi

- Fraudsters install skimming devices in ATM machines and steal data from the customer's card.
- Fraudsters may also install a dummy keypad or a small / pinhole camera, well-hidden from plain sight to capture ATM PIN.
- Sometimes, fraudsters pretending to be other customer standing near-by gain access to the PIN when the customer enters it in an ATM machine.
- This data is then used to create a duplicate card and withdraw money from the customer's account.



### Precautions

- Always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction.
- Cover the keypad with your other hand while entering the PIN.
- NEVER write the PIN on your ATM card.
- Do NOT enter the PIN in the presence of any other / unknown person standing close to you.
- Do NOT give your ATM card to anyone for withdrawal of cash.
- Do NOT follow the instructions given by any unknown person or take assistance / guidance from strangers / unknown persons at the ATMs.
- If cash is not dispensed at the ATM, press the 'Cancel' button and wait for the home screen to appear before leaving the ATM.





## 6. Frauds using screen sharing app / Remote access

### Modus Operandi

- Fraudsters trick the customer to download a screen sharing app.
- Using such app, the fraudsters can watch / control the customer's mobile / laptop and gain access to the financial credentials of the customer.
- Fraudsters use this information to carry out unauthorised transfer of funds or make payments using the customer's Internet banking / payment apps.



### Precautions

- If your device faces any technical glitch and you need to download any screen sharing app, deactivate / log out of all payment related apps from your device.
- Download such apps only when you are advised through the official Toll-free number of the company as appearing in its **official website**. Do not download such apps in case an executive of the company contacts you through his / her personal contact number.
- As soon as the work is completed, ensure that the screen sharing app is removed from your device.



## 7. SIM swap / SIM cloning

### Modus Operandi

- Fraudsters gain access to the customer's Subscriber Identity Module (SIM) card or may obtain a duplicate SIM card (including electronic-SIM) for the registered mobile number connected to the customer's bank account.
- Fraudsters use the OTP received on such duplicate SIM to carry out unauthorised transactions.
- Fraudsters generally collect the personal / identity details from the customer by posing as a telephone / mobile network staff and request the customer details in the name of offers such as - to provide free upgrade of SIM card from 3G to 4G or to provide additional benefits on the SIM card.



### Precautions

- Never share identity credentials pertaining to your SIM card.
- Be watchful regarding mobile network access in your phone. If there is no mobile network in your phone for a considerable amount of time in a regular environment, immediately contact the mobile operator to ensure that no duplicate SIM is being / has been issued for your mobile number.



## 8. Frauds by compromising credentials on results through search engines

### Modus Operandi

- Customers use search engines to obtain contact details / customer care numbers of their bank, insurance company, Aadhaar updation centre, etc. These contact details on search engines often do NOT belong to the respective entity but are made to appear as such by fraudsters.
- Customers may end up contacting unknown / unverified contact numbers of the fraudsters displayed as bank / company's contact numbers on search engine.
- Once the customers call on these contact numbers, the imposters ask the customers to share their card credentials / details for verification.
- Assuming the fraudster to be a genuine representative of the RE, customers share their secure details and thus fall prey to frauds.



### Precautions

- Always obtain the customer care contact details from the official websites of banks / companies.
- Do not call the numbers directly displayed on the search engine results page as these are often camouflaged by fraudsters.
- Please also note that customer care numbers are never in the form of mobile numbers.



## 9. Scam through QR code scan

### Modus Operandi

- Fraudsters often contact customers under various pretexts and trick them into scanning Quick Response (QR) codes using the apps on the customers' phone.
- By scanning such QR codes, customers may unknowingly authorise the fraudsters to withdraw money from their account.



### Precautions

- Be cautious while scanning QR code/s using any payment app. QR codes have account details embedded in them to transfer money to a particular account.
- Never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc.



## 10. Impersonation on social media

### Modus Operandi

- Fraudsters create fake accounts using details of the users of social media platforms such as Facebook, Instagram, Twitter, etc.
- Fraudsters then send a request to the users' friends asking for money for urgent medical purposes, payments, etc.
- Fraudsters, using fake details, also contact users and gain users' trust over a period of time. When the users' share their personal or private information, the fraudsters use such information to blackmail or extort money from the users.



### Precautions

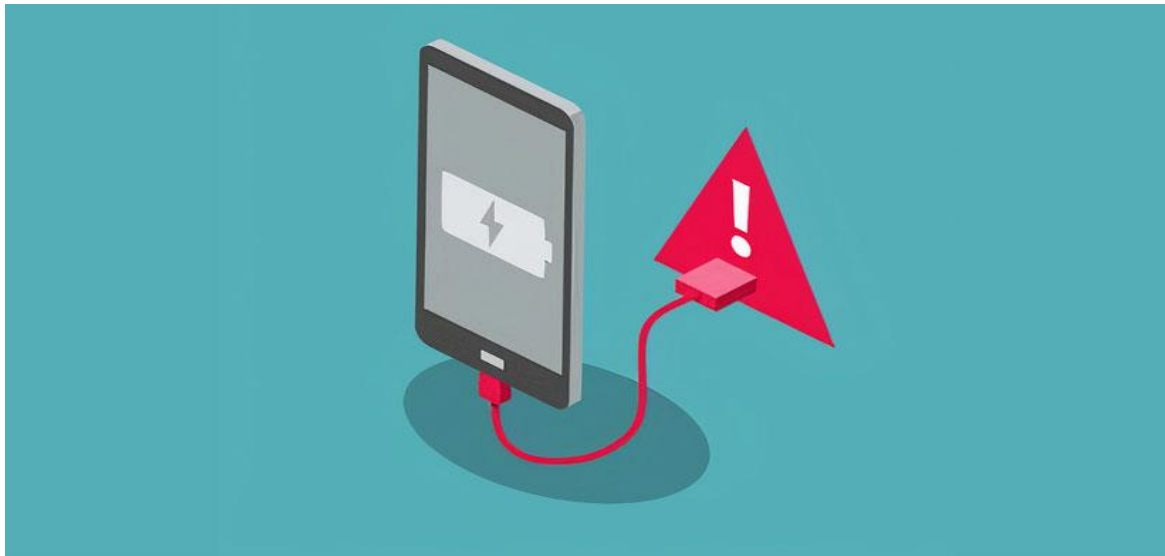
- Always verify the genuineness of a fund request from a friend / relative by confirming through a phone call / physical meeting to be sure that the profile is not impersonated.
- Do not make payments to unknown persons online.
- Do not share personal and confidential information on social media platforms.



## 11. Juice jacking

### Modus Operandi

- The charging port of a mobile, can also be used to transfer files / data.
- Fraudsters use public charging ports to transfer malware to customer phones connected there and take control / access / steal data sensitive data such as emails, SMS, saved passwords, etc. from the customers' mobile phones (Juice Jacking).



### Precaution

- Avoid using public / unknown charging ports / cables.



## 12. Lottery fraud

### Modus Operandi

- Fraudsters send emails or make phone calls that a customer has won a huge lottery. However, in order to receive the money, the fraudsters ask the customers to confirm their identity by entering their bank account / credit card details on a website from which data is captured by the fraudsters.
- Fraudsters also ask the customers to pay taxes/ forex charges / upfront or pay the shipping charges, processing / handling fee, etc., to receive the lottery / product.
- Fraudsters in some cases, may also pose as a representative of RBI or a foreign bank / company / international financial institution and ask the customer to transfer a relatively small amount in order to receive a larger amount in foreign currency from that institution.
- Since the requested money is generally a very small percentage of the promised lottery / prize, the customer may fall into the trap of the fraudster and make the payment.



### Precautions

- Beware of such unbelievable lottery or offers - nobody gives free money, especially such huge amounts of money.
- Do not make payments or share secure credentials in response to any lottery calls / emails.
- RBI never opens accounts of members of public or takes deposits from them. Such messages are fraudulent.
- RBI never asks for personal / bank details of members of public. Beware of fake RBI logos and messages.
- Never respond to messages offering / promising prize money, government aid and Know Your Customer (KYC) updation to receive prize money from banks, institutions etc.



### 13. Online job fraud

#### Modus Operandi

- Fraudsters create fake job search websites and when the job seekers share secure credentials of their bank account / credit card / debit card on these websites during registration, their accounts are compromised.
- Fraudsters also pose as officials of reputed company(s) and offer employment after conducting fake interviews. The job seeker is then induced to transfer funds for registration, mandatory training program, laptop, etc.



#### Precautions

- For any job offer, including from overseas entities, first confirm the identity and contact details of the employing company / its representative.
- Always remember that a genuine company offering a job will never ask for money for offering the job.
- Do not make payments on unknown job search websites.





## 14. Money mules

### Modus Operandi

- Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen / illegal money via their bank account/s.



- Fraudsters contact customers via emails, social media, etc., and convince them to receive money into their bank accounts (money mule), in exchange for attractive commissions.
- The money mule is then directed to transfer the money to another money mule's account, starting a chain that ultimately results in the money getting transferred to the fraudster's account.
- Alternatively, the fraudster may direct the money mule to withdraw cash and hand it over to someone.
- When such frauds are reported, the money mule becomes the target of police investigation for money laundering.

### Precautions

- Do not allow others to use your account to receive or transfer money for a fee / payment.
- Do not respond to emails asking for your bank account details.
- Do not get carried away by attractive offers / commissions and give consent to receive unauthorised money and to transfer them to others or withdraw cash and give it out for a handsome fee.
- If the source of funds is not genuine, or the rationale for underlying transaction is not proved to authorities, the receiver of money is likely to land in serious trouble with police and other law enforcement agencies.



## Modus Operandi and Precautions to be taken against Fraudulent Transactions – Non Banking Financial Companies (NBFCs)





## 1. Fake advertisements for extending loans by fraudsters

### Modus Operandi

- Fraudsters issue fake advertisements offering personal loans at very attractive and low rates of interest or easy repayment options or without any requirement of collateral/ security, etc.
- Fraudsters send emails with such offers and ask the borrowers to contact them. To gain credibility with the gullible borrowers and to induce confidence, these email-ids are made to look-like the emails IDs of senior officials of well-known / genuine Non-Banking Financial Companies (NBFCs).
- When borrowers approach the fraudsters for loans, the fraudsters take money from the borrowers in the name of various upfront charges like processing fees, Goods and Services Tax (GST), intercity charge, advance Equated Monthly Instalment (EMI), etc., and abscond without disbursing the loans.
- Fraudsters also create fake website links to show up on search engines, when people search for information on loans.



### Precautions

- Loan processing fee charged by NBFCs / banks is deducted from the sanctioned loan amount and not demanded upfront in cash from the borrower.
- Never pay any processing fee in advance as NBFCs / banks will never ask for an advance fee before the processing of loan application.
- Do not make payments or enter secure credentials against online offer of loans at low interest rates, etc., without checking / verifying the particulars through genuine sources.



## 2. SMS / Email / Instant Messaging / Call scams

### Modus Operandi

- Fraudsters circulate fake messages in instant messaging apps / SMS / social media platforms on attractive loans and use the logo of any known NBFC as profile picture in the mobile number shared by them to induce credibility.
- The fraudsters may even share their Aadhaar card / Pan Card and fake NBFC ID card.
- After sending such bulk messages / SMS / emails, the fraudsters call random people and share fake sanction letters, copies of fake cheques, etc., and demand various charges. Once the borrowers pay these charges, the fraudsters abscond with the money.



### Precautions

- Never believe loan offers made by people on their own through telephones / emails, etc.
- Never make any payment against such offers or share any personal / financial credentials against such offers without cross-checking that it is genuine through other sources.
- Never click on links sent through SMS / emails or reply to promotional SMS / emails.
- Never open / respond to emails from unknown sources containing suspicious attachment or phishing links.



### 3. OTP based Frauds

#### Modus Operandi

- Fraudsters impersonating as NBFCs, send SMS / messages offering loans or enhancement of credit limit on NBFC/bank customers' loan accounts, and ask the customers to contact them on a mobile number.
- When the customers call such numbers, fraudsters ask them to fill forms to collect their financial credentials. Fraudsters then induce / convince the customers to share the OTP or PIN details and carry out unauthorised transfers from the customers' accounts.



#### Precautions

- Never share OTP / PIN / personal details, etc., in any form with anyone, including your own friends and family members.
- Regularly check SMS / emails to ensure that no OTP is generated without your prior knowledge.
- Always access the official website of bank / NBFC / e-wallet provider or contact the branch to avail their services and / or seek product and services related information and clarifications.



#### 4. Fake loan websites / App frauds

##### Modus Operandi

- Fraudsters create unscrupulous loan apps which offer instant and short-term loans. These apps dupe the borrowers and may also charge significantly higher interest rates.
- To attract gullible borrowers, the fraudsters advertise “limited period offers” and ask borrowers to make urgent decisions using pressure tactics.



##### Precautions

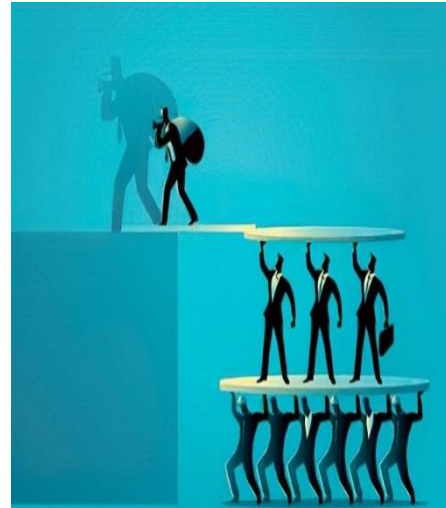
- Verify if the lender is registered with the Government / Regulator / authorised agencies
- Check whether the lender has provided a physical address or contact information to ensure it is not difficult to contact them later.
- Beware if the lender appears more interested in obtaining personal details rather than in checking credit scores.
- Remember that any reputed NBFC / bank will never ask for payment before processing the loan application.
- Genuine loan providers never offer money without verifying documents and other credentials of the borrowers.
- Verify if these NBFC-backed loan apps are genuine.



## 5. Money circulation / Ponzi / Multi-Level Marketing (MLM) schemes fraud

### Modus Operandi

- Fraudsters use MLM / Chain Marketing / Pyramid Structure schemes to promise easy or quick money upon enrolment / adding of members.
- The schemes not only assure high returns but also pay the first few instalments (EMIs) to gain confidence of gullible persons and attract more investors through word of mouth publicity.
- The schemes encourage addition of more people to the chain / group. Commission is paid to the enroller for the number of people joining the scheme, rather than for the sale of products.
- This model becomes unsustainable after some time when number of persons joining the scheme starts declining. Thereafter, the fraudsters close the scheme and disappear with the money invested by the people till then.



### Precautions

- Returns are proportional to risks. Higher the return, higher is the risk.
- Any scheme offering abnormally high returns (40-50% p a) consistently, could be the first sign of a potential fraud and caution needs to be exercised.
- Always notice that any payment / commission / bonus / percentage of profit without the actual sale of goods / service is suspicious and may lead to a fraud.
- Do not be tempted by promises of high returns offered by entities running Multi-Level Marketing / Chain Marketing / Pyramid Structure schemes.
- Acceptance of money under Money Circulation / Multi-level Marketing / Pyramid structures is a cognizable offence under the Prize Chits and Money Circulation Schemes (Banning) Act, 1978.
- In case of such offers or information of such schemes, a complaint must be immediately lodged with the State Police.



## 6. Fraudulent loans with forged documents

### Modus Operandi

- Fraudsters use forged documents to avail services from financial institutions.
- Fraudsters commit identity thefts, steal personal information of customers such as identity cards, bank account details etc., and use this information or credentials to avail benefits from a financial institution.
- Fraudsters pose as NBFC employees and collect KYC related documents from customers.



### Precautions

- Exercise due care and vigilance while providing KYC and other personal documents, including the National Automated Clearing House (NACH) form for loan sanction / availing of credit facility from any entity, especially individuals posing to be representatives of these entities.
- Such documents should be shared only with the entity's authorised personnel or on authorised email IDs of the entities.
- Follow up with the concerned entities to ensure that the documents shared by you are purged immediately by them in case of non-sanction of loan and/ or post closure of the loan account.





## General Precautions to be taken for financial transactions





## General precautions

- Be wary of suspicious looking pop ups that appear during your browsing sessions on internet.
- Always check for a secure payment gateway (<https://> - URL with a pad lock symbol) before making online payments / transactions.
- Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV, etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.
- Avoid saving card details on websites / devices / public laptop / desktops.
- Turn on two-factor authentication where such facility is available.
- Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links.
- Do not share copies of chequebook, KYC documents with strangers.



## For device / computer security

- Change passwords at regular intervals.
- Install antivirus on your devices and install updates whenever available.
- Always scan unknown Universal Serial Bus (USB) drives / devices before usage.
- Do not leave your device unlocked.
- Configure auto lock of the device after a specified time.
- Do not install any unknown applications or software on your phone / laptop.
- Do not store passwords or confidential information on devices.





### For safe internet browsing

- Avoid visiting unsecured / unsafe / unknown websites.
- Avoid using unknown browsers.
- Avoid using / saving passwords on public devices.
- Avoid entering secure credentials on unknown websites/ public devices.
- Do not share private information with anyone, particularly unknown persons on social media.
- Always verify security of any webpage (https:// - URL with a pad lock symbol), more so when an email or SMS link is redirected to such pages.

### For safe internet banking

- Always use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc.
- Log out of the internet banking session immediately after usage.
- Update passwords on a periodic basis.
- Do not use same passwords for your email and internet banking.
- Avoid using public terminals (viz. cyber cafe, etc.) for financial transactions.





### **Factors indicating that a phone is being spied**

- Unfamiliar applications are being downloaded on the phone.
- There is a faster than usual draining of phone battery.
- Phone turning hot may be a sign of someone spying by running a spyware in the background.
- An unusual surge in the amount of data consumption can sometimes be a sign that a spyware is running in the background.
- Spyware apps might sometimes interfere with a phone's shutdown process so that the device fails to turn off properly or takes an unusually long time to do so.
- Note that text messages can be used by spyware and malware to send and receive data.

### **Actions to be taken after occurrence of a fraud**

- Block not only the debit card / credit card but also freeze the debit in the bank account linked to the card by visiting your branch or calling the **official customer care number** available on the bank's website. Also, check and ensure the safety of other banking channels such as Net banking, Mobile banking etc., to prevent perpetuation of the fraud once the debit/ credit cards, etc., are blocked following a fraud.
- Dial helpline number 155260 or 1930 or report the incident on National Cybercrime Reporting Portal ([www.cybercrime.gov.in](http://www.cybercrime.gov.in)).  
Reset Mobile: Use (Setting-Reset-Factory Data) to reset mobile if a fraud has occurred due to a data leak from mobile.

### **Precautions related to Debit / Credit cards**

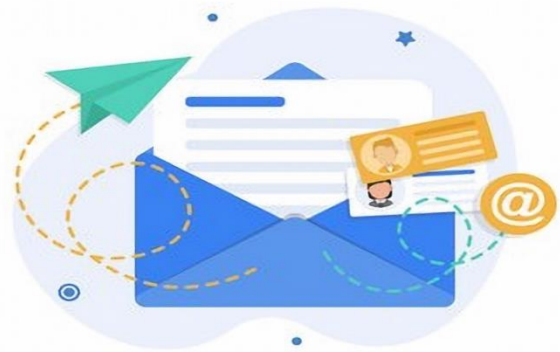
- You should deactivate various features of credit / debit card, viz., online transactions both for domestic and international transactions, in case you are not going to use the card for a while and activate the same only when the card usage is required.
- Similarly, Near Field Communication (NFC) feature should be deactivated, if the card is not to be used.
- Before entering PIN at any Point of Sale (POS) site or while using the card at an NFC reader, you must carefully check the amount displayed on the POS machine screen and NFC reader.



- Never let the merchant take the card away from your sight for swiping while making a transaction.
- Cover the keypad with your other hand while entering the PIN at a POS site / ATM.

#### **For E-mail account security**

- Do not click on links sent through emails from unknown addresses / names.
- Avoid opening emails on public or free networks.
- Do not store secure credentials / bank passwords, etc., in emails.



#### **For password security**

- Use a combination of alphanumeric and special characters in your password.
- Keep two factor authentication for all your accounts, if such facility is available.
- Change your passwords periodically.
- Avoid having you date of birth, spouse name, car number etc. as passwords.





### How do you know whether an NBFC accepting deposit is genuine or not?

- Verify whether the name of NBFC appears in the list of deposit taking NBFCs entitled to accept deposits, available at <https://rbi.org.in> and to ensure that it is not appearing in the list of companies prohibited from accepting deposits.
- NBFCs must prominently display the Certificate of Registration (CoR) issued by the Reserve Bank on its site / in its office. This certificate should also reflect that the NBFC has been specifically authorised by RBI to accept deposits. Scrutinize the certificate to ensure that the NBFC is authorised to accept deposits.
- NBFCs cannot accept deposits for a period less than 12-months and more than 60 months and the maximum interest rate that an NBFC can pay to a depositor should not exceed 12.5%.
- The Reserve Bank publishes the change in the interest rates on <https://rbi.org.in> → Sitemap → NBFC List → FAQs.





### Precautions to be taken by depositors

- When depositing money, insist on a proper receipt for each and every deposit made with the bank / NBFC / company.
- The receipt should be duly signed by an officer authorised by the company and should state, *inter alia*, the date of the deposit, the name of the depositor, the amount in words and figures, rate of interest payable, maturity date and amount.
- In the case of brokers / agents, etc., collecting public deposits on behalf of NBFCs, verify that the brokers / agents are duly authorised for the purpose by the concerned NBFC.
- Remember that the Deposit Insurance facility is not available to depositors of NBFCs.





## File a complaint

### Complaint to RBI Ombudsman

- For filing complaints online, please visit the link at <https://cms.rbi.org.in/>
- Complaints in physical / paper form can be sent to CRPC, Reserve Bank of India, Central Vista, Sector -17, Chandigarh -160 017.

### Complaint to Securities and Exchange Board of India (SEBI)

- Please visit the link at <https://www.sebi.gov.in/>

### Complaint to Insurance Regulatory and Development Authority of India (IRDAI)

- Please visit the link at <https://www.irdai.gov.in/>

### Complaint to National Housing Bank (NHB)

- Please visit the link at <https://nhb.org.in/>

### Complaint to Cyber Police Station

- Please visit <https://cybercrime.gov.in/>

\*\*\*\*\*





## Glossary

- **Advance fee/Processing fee/Token fee:** These include preliminary payments such as documentation charges, meeting expenses, processing fees, other charges that may be applicable for disbursement of the loan to a borrower.
- **Two-factor authentication:** Authentication methodologies involve three basic 'factors'- something the user knows (e.g., password, PIN- either static or one time generated); something the user has (e.g., ATM/ smart card number, expiry date and CVV that is printed on the card); and something the user is (e.g., biometric characteristic, such as a fingerprint). Two-factor authentication (also known as 2FA) provides identification of users by means of a combination of two different components - what the user has and what the user knows/is to complete a transaction.
- **Authorisation:** The response from a card-issuing bank to a merchant's transaction authorisation request indicating that the payment information is valid and funds are available on the customer's credit card.
- **Card number:** The number assigned by a credit card association or card issuing bank to a card. This information must be provided to a merchant by a customer in order to make a credit card payment but should not be shared with anyone else. The string of digits is printed on the card.
- **Credit card:** A card that allows paying for products or services by availing unsecured/secured credit from a financial institution.
- **Credit limit:** The term refers to the maximum amount of credit a financial institution extends to a customer. A lending institution extends a credit limit on a credit card based on the analysis of the information given by the credit-seeking applicant. The credit limit can affect the customer's credit scores and their ability to obtain credit in the future.
- **CVV:** Stands for Card Verification Value. This is a 3-digit number printed on the card which is mandatory for completing most online transactions. These details are confidential and must NEVER be shared with anyone.
- **Debit card:** A card that allows paying for products or services by deduction of available funds in a bank account of the cardholder.



- **E-commerce platform:** It is a platform/website that enables buying and selling of goods and services including digital products over digital and electronic network.
- **EMI:** It stands for Equated Monthly Instalment. This is a fixed monthly payment (includes principal and interest) to be made by a borrower to his lender/creditor (like bank/NBFC) each month till the loan/credit, along with interest, taken from the lender/creditor is paid off by the borrower in full.
- **Encryption:** The process of transforming processing information into an electronic code to maintain its secrecy.
- **Expiry date:** The date on which the validity of a card, contract, agreement, document, etc. expires. Transactions will be approved only in respect of cards or documents which have not yet expired.
- **Gateway:** It is an intermediary that provides technology infrastructure to route and facilitate processing of services such as transactions base management, risk management, etc. without its involvement directly. Payment Gateways are entities that provide technology infrastructure to route and facilitate processing of online payment transactions without any involvement in handling of funds.
- **Immediate payment services (IMPS):** It is an instant interbank electronic fund transfer service (up to a limit) through mobile phones, provided by National Payments Corporation of India (NPCI).
- **KYC:** Stands for Know Your Customer. It is a process in which the financial institution makes an effort to verify the identity, suitability, and risks involved with maintaining a relationship with a customer by obtaining a set of documents and carrying out due diligence.
- **Money mule:** It is a term used to describe victims who are exploited by fraudsters into laundering stolen / illegal money via their bank account(s).
- **Multi-Level Marketing:** The practice of selling goods or services on behalf of a company in a system whereby participants receive commission on their sales as well as the sales of any participants they recruit.



- **National Automated Clearing House (NACH):** It is a centralised Electronic Clearing Service (ECS) system operated by National Payments Corporation of India (NPCI).
- **Near Field Communication (NFC):** It is a communication technology used to transmit data from a NFC equipped device to a capable terminal. The NFC technology is used to make a contactless payment that is carried out by keeping the smartphone/card near the NFC enabled machine.
- **National Electronic Fund Transfer (NEFT):** It is a nation-wide centralised payment system owned and operated by RBI, which enables bank customers in India to transfer funds between any two NEFT-enabled bank accounts.
- **OTP:** One Time Password is one of the factors in the authentication methodology, which the customer knows and is often used for carrying out online transactions. This is CONFIDENTIAL and should not be shared with anyone.
- **Phishing:** It refers to spoofed emails and / or SMSs designed to dupe customers into thinking that the communication has originated from their bank / e-wallet provider and contain links to extract confidential details.
- **Point of Sale device (POS) / Acceptance Device (mPOS):** It refers to any device / terminal / machine installed at Merchant Establishments which enables the merchants to accept payments through payment cards (credit cards, debit cards, gift cards etc.).
- **Quick Response (QR) code:** The QR Code is type of a two-dimensional bar code. It consists of black squares arranged in a square grid on a white background. Imaging devices such as smartphone cameras can be used to read and interpret these codes. QR code contains information about the payee and is used to facilitate mobile payments at the point-of-sale by debiting the customers' account.
- **Remote Access:** It refers to luring customer to download an application on their mobile phone / computer which is able to access all the customers' data on that customer device.



- **UPI:** Unified Payment Interface is a platform that allows transfer of money from one bank / wallet account to other using a mobile phone which has access to the Internet. Once a customer registers for UPI with the bank, a unique virtual identifier is created and mapped to the customer's mobile phone to initiate the payment. It uses authentication in the form of UPI-PIN, which is CONFIDENTIAL and should not be shared with anyone.
- **Vishing:** It refers to phone calls pretending to be from bank / non-bank e-wallet providers / telecom service providers luring customers into sharing confidential details in the pretext of KYC-updation, unblocking of account / SIM-card, crediting debited amount, etc.
- **Wallet:** A wallet is like an account which can be used for purchase of goods and services against the stored value in it. A wallet can be virtual (e.g. mobile wallet) or physical (prepaid cards).

\*\*\*\*\*



## **RED FLAG INDICATORS (RFIs)**

### **1. Rule Based Monitoring**

#### **Monitoring Based on Multiple Scenarios/ Rules based alert generated for MTSS**

Considering the nature of service, it is requested to generate an MIS for “Inward Remittance Transactions” based on the conditions given below,

1. Customers with high number of transactions
2. Customers with high aggregate value of transactions
3. Transactions of foreigners (Visiting India)
4. Concentration of customers in branches
5. Customers receiving fund from multiple senders
6. Customers receiving fund from multiple countries
7. Single sender sending to multiple receivers
8. Single sender sending from multiple countries
9. Single customer transaction in Multiple Branches/Regions/States
10. Low value transaction with high frequency.
11. Transactions from FATF notified countries (High/medium risk)
12. Transactions from Pakistan and China.
13. Number of days involved in transaction
14. Total Transaction value is lower than average transaction value

#### **Monitoring Based on Single Scenario/ Rule based alert generated**

SN	Scenario / Rule	Risk Severity
1	Loan disbursed to the customer through banking channels and the loan repayment done in cash (If more than XX% of loan amount is repaid in cash)	High
2	Loan disbursed to the customer in cash and repayment done using non-cash modes	Medium
3	Having inventory count of XX or more	Low
4	Performed more than XX repledges during XX days	Medium
5	Number of transactions is in excess of XX Nos during XX days	Medium
6	Distinct count of Transaction Date in excess of XX Days (Date on which payment is made)	Medium
7	Amount involved in repayment (In Aggregate) is in excess of XX Lakhs during XX days	Low
8	No of branches where inventory is pledged in more than XX Branches.	Medium
9	Wallets receiving more than average transactions from multiple number of bank accounts/ wallets in a single day	Medium
10	Wallets receiving more than average transactions from multiple number of bank accounts/ wallets (more than average transactions, either by count or by amount)	Medium
11	Single beneficiary (Based on bank account) receiving funds from multiple wallets / bank accounts in a single day	High
12	Single beneficiary (Based on bank account) receiving funds from multiple wallets / bank accounts (more than average transactions, either by count or by amount)	Medium
13	Customers who are transacted in more than XX currencies in a month	Medium
14	Customers who has transacted in more than XX currencies during every XX months	Low

Reports generated covering all products,

1. High Value cash transaction in a day
2. High Value cash transaction in a Calendar month
3. Unscheduled High Value repayments in a day
4. Unscheduled High Value repayments in a calendar month
5. Splitting of cash transaction just below Rs.XX by a Customer in a month
6. High value transactions by High Risk Customers
7. Cash repayments greater than INR XX for individuals and greater than INR XX for non-individuals in a day
8. Top 10 cash repayments in a day.
9. Non-Cash repayments greater than INR XX for individuals and greater than INR XX for non-individuals in a day
10. Top 10 non-cash repayments in a day
11. Cash repayments greater than INR XX for individuals and greater than INR XX for non-individuals in a month
12. Top 10 cash repayments in a month.

13. Non-Cash repayments greater than INR XX for individuals and greater than INR XX for non-individuals in a month.
14. Top 10 cash repayments in a month
15. Value of transaction is more than XX percent of the previous largest transaction for the client (or client profile)
16. Value of transactions in a month is more than XX percent of the average value for the client (or client profile)
17. Number of transactions in a month is more than XX percent of the average number for the client (or client profile)
18. Cash transactions greater than INR XX by customer with low cash requirements such as Students, Housewife, Pensioners, Wages and salary person and Minor Accounts
19. Cash repayments in amounts ranging between INR XX/- to INR XX in multiple accounts of the customer greater than XX times in a month
20. Common address/telephone used by multiple unrelated customers. Common Ids used by multiple customers. Group of individuals conducting transactions.
21. Loan repayments in cash greater than INR XX in XX months.
22. Transaction involving a location considered to be high risk from the terrorist financing perspective.
23. Receipt of any notice of enquiry from any enforcement authority, calling for information about any Customer.
24. Customer provided different IDs or Date of Birth at different instances
25. Receipt of enquiry/attachment notice from any enforcement authority such as CBI, Police, Enforcement Directorate, Department of Vigilance and Anti-corruption, Income tax or Service Tax Authorities etc. for violation of revenue/regulatory laws.

### **Escalation from Branch / Field staff**

<b>SN</b>	<b>Category</b>	<b>Detailed description</b>
1	Behavioral indicators	<ol style="list-style-type: none"> <li>1. Customer did not open account after being informed about KYC requirements</li> <li>2. Customer uses complex legal structures or where it is difficult to identify the beneficial owner.</li> <li>3. Customer is hurried or nervous.</li> <li>4. Customer is over cautious in explaining genuineness of the transaction.</li> <li>5. Customer changes the information provided after more detailed information is requested. Customer provides information that seems minimal, possibly false or inconsistent.</li> <li>6. Multiple customers arrive together but pretend to ignore each other.</li> <li>7. Customer travels unexplained distances to conduct transactions</li> <li>8. Customer could not explain source of funds satisfactorily.</li> <li>9. Not sharing the details of transaction/purpose of loan</li> </ol>
2	Service Request Indicators	<ol style="list-style-type: none"> <li>1. Customer frequently requests for change of address</li> <li>2. Customer did not complete transaction after queries of source of funds etc.</li> <li>3. Customer has vague knowledge about amount of money involved in the transaction. Customer taking instructions for conducting transactions.</li> </ol>



		<p>Customer is accompanied by unrelated individuals.</p> <ol style="list-style-type: none"> <li>4. Customer makes inquiries or tries to convince staff to avoid reporting.</li> <li>5. Relaxing due diligence process by offering tips/gifts</li> <li>6. Forcing to open Multiple IDs</li> </ol>
3	Transactional Indicators	<ol style="list-style-type: none"> <li>1. Transaction is unnecessarily complex for its stated purpose.</li> <li>2. The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer.</li> <li>3. Transaction involving movement of which is inconsistent with the customer's business.</li> <li>4. High volume of transactions without apparent explanation</li> <li>5. Transaction in small amounts</li> <li>6. Exchange of currency does not match the country where the client is travelling</li> <li>7. Felt to be Benami Transaction</li> <li>8. Third parties (ie, persons other than customer) is approaching the branch for repayment/settlement of loans</li> <li>9. Receiving multiple transactions from different senders in similar amounts in a short amount of time.</li> <li>10. Receiving unusual number of transactions in a short period of time</li> <li>11. Receiving fund from multiple senders with no apparent family relationship</li> <li>12. Receiving transactions from multiple states, provinces or countries</li> </ol>
4	Legal/Social Indicators	<ol style="list-style-type: none"> <li>1. Customer has been the subject of inquiry from any law enforcement agency relating to criminal offences.</li> <li>2. Customer has been the subject of inquiry from any law enforcement agency relating to Terrorism Financing or terrorist activities.</li> <li>3. Match of customer details with persons reported in local media / open source of criminal offences.</li> <li>4. Match of customer details with persons reported in local media / open source for terrorism or terrorist financing related activities.</li> <li>5. Complaint received from public for abuse of account for committing fraud etc.</li> <li>6. Alert raised by agents about suspicion.</li> <li>7. Alert raised by other institutions, subsidiaries or business associates including cross-border referral.</li> </ol>
5	Documentation Indicators	<ol style="list-style-type: none"> <li>1. Customer gave false identification documents or documents that appear to be counterfeited, fabricated, altered or inaccurate.</li> <li>2. Identity documents presented are not verifiable i.e. Foreign documents etc.</li> <li>3. Address provided by the customer is found to be non-existent.</li> <li>4. Customer not staying at address provided during account opening.</li> <li>5. Customer offers different identifications on different occasions with an apparent attempt to avoid linkage of multiple transactions.</li> <li>6. Giving hotel address / other addresses rather than home / permanent address</li> </ol>
6	Others	<ol style="list-style-type: none"> <li>1. Others (specify the details in "Other information")</li> </ol>