General Security Guidelines For Safe Online Banking

*** Keep your passwords confidential**

*** Avoid using simple passwords and use strong passwords**

*** Change the passwords periodically and whenever you feel that your password has been compromised or made known to anybody accidentally**

*** Destroy the password/pin mailer after changing the password/pin**

*** Avoid accessing online banking websites from cybercafés/shared networks**

*** Upgrade the Operating System (OS) of the computer system promptly as newer/upgraded versions would help make your system more secure.**

*** Use newer/upgraded versions of browsers as they are regularly updated to block and alert you from accessing the phishing sites**

*** Install Antivirus software on your computer systems and update them continuously as this will reduce the risk of virus attacks**

*** Installation of personal firewall would provide added level of security**

*** Any potential risk caused through pop up windows may be eliminated by removing spy ware or ad ware installed on your system by using spyware/adware removing tools.**

*** Avoid downloading from unknown/unfamiliar sources. They may contain Trojans/malicious programs or worms/viruses that may compromise your system security.**

*** Disconnect your internet connection when not in use. This would avoid unnecessary access to the information on your systems and help protect yourself even if you have a personal firewall installed in your system.**

*** Logout completely after using the online application, i.e., by clicking the logout button and closing the browser windows.**