What is the PCI DSS?

The **PCI DSS** 1.2.1 stands for **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard. **PCI-DSS** is aiming to improve the quality of work and maintain the confidentiality, integrity and availability of data and Information. This comprehensive standard is intended to help organizations proactively protect customer account data.

TeBAS is always seeking to bring the best of breed values to its clients hence a decision has been taken to comply and meet **PCI-DSS** application development requirement and implement it across **IMAS** systems.

TeBAS is proudly announcing that the following are the new features that are implemented across **IMAS** systems in order to meet the required and applied **PCI-DSS**:

New Features	PCI-DSS Requirement
Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	8.4
Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	8.5.1
Set first-time passwords to a unique value for each user and change immediately after the first use.	8.5.3
Remove/disable inactive user accounts at least every 90 days.	8.5.5
Enable accounts used by vendors for remote maintenance only during the time period needed.	8.5.6
Do not use group, shared, or generic accounts and passwords.	8.5.7
Change user passwords at least every 90 days.	8.5.8
Require a minimum password length of at least seven characters.	8.5.10
Use passwords containing both numeric and alphabetic characters.	8.5.11
Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	8.5.12
Limit repeated access attempts by locking out the user ID after not more than six attempts.	8.5.13
Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	8.5.14
If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	8.5.15
Implement automated audit trails for all system components to reconstruct the following events:	10.2
All individual accesses to cardholder data	10.2.1
All actions taken by any individual with root or administrative privileges	10.2.2
Access to all audit trails	10.2.3
Invalid logical access attempts	10.2.4
Use of identification and authentication mechanisms	10.2.5
Initialization of the audit logs	10.2.6
Record at least the following audit trail entries for all system components for each event:	10.3
User identification	10.3.1
Type of event	10.3.2
Date and time	10.3.3.
Success or failure indication	10.3.4
Origination of event	10.3.5
Identity or name of affected data, system component, or resource	10.3.6