PCI DSS Cardholder Data and PDQ Monthly Checklist

Monthly Checklist

Location_____ Date_____ Signature_____

SECURITY	STATUS	CHECKED BY	DATE	COMMENTS
In an Office Environment				
1. All sensitive Information e.g. Cardholder details (CHD) securely locked at close of business.				
2. CHD storage accessible by authorised staff only.				
3. Storage of Security data and other CHD secured separately.				
4. Keys to storage secured, accessible only to authorised staff.				
5. All data no longer required has been shredded.				
6. All PDQ's machines secured at close of business.				
7. Weekly checks on the PDQ serial numbers / terminal ID's carried out along with PDQ machines examined for tampering.				
8. Are your policies and procedures regarding PCI requirements up to date?				

SECURITY	STATUS	CHECKED BY	DATE	COMMENTS
9. Do you have an escalation plan in place to inform Finance/Information services should a breach be identified?				
10. Have all staff handling/processing debit card transactions read and understood the PCI requirements?				

It is the responsibility of the Manager of the area/outlet to print, complete, and file this to comply with audit requirements