PCI DSS Cardholder Data and PDQ Monthly Checklist

Monthly Checklist

SECURITY	STATUS	CHECKED BY	DATE	COMMENTS
In an Office Environment				
1. Is all sensitive Information EG: Card holder details (CHD) securely locked at close of business (CoB)?				
2. Is CHD storage accessible by authorised staff only?				
3. Is the storage of Security data and other CHD secured separately?				
4. Are keys to storage secured, accessible only to authorised staff?				
5. Has all data no longer required been shredded?				
6. Are the PDQ's machines secured at CoB?				
7. Have the weekly checks on the PDQ serial number been checked and the machines examined for tampering?				
8. Are your policies and procedures regarding PCI requirements up to date?				

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

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?				
Data in transit (out of normal operational activity EG: Graduation ceremony)				
1. Have the weekly checks on the PDQ serial number been checked and the machines examined for tampering?				
2. Are all the debit/credit receipts held securely at the venue?				
3. Have the receipts been secured in blue security pouches and ID number logged?				
4. Has the policy for handling /processing card payments been cascaded, understood and adhered by all authorised staff?				

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