|  |  |
| --- | --- |
| **I:\Hope Logo.png** | **Departmental PCI DSS Declaration** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department:** |  |  | **Primary Credit/ debit card machine holder:** |  |

The University is working to achieve external approval and a compliance certificate for its procedures for processing credit/ debit cards. This is a mandatory process and is required by credit card providers such as Visa and MasterCard as a way of combatting fraud.

As the primary administrator of a credit/ debit card terminal which is located in your department you are required to confirm that all staff who use this machine have read the University Training Documentation (available on the Staff finance Website) and, in particular, that your department can confirm that:

|  |  |  |
| --- | --- | --- |
|  | **Please confirm the following:** | **True/False/Not applicable\*** |
| 1 | **ALL** staff dealing with credit/debit card data **are aware of the importance of cardholder data security** and the requirements of the **Payment Card Security Policy & Training documentation** and the training has been completed in the last 12 months.    |  |
| 2 | A **list is kept of ALL staff** dealing with any form of card data and payment devices. (Completed list to be submitted with this declaration) |  |
| 3 | Payment card devices **are protected from physical access** by those not authorized to use the equipment; when not in use they are **physically locked away** or locked down in the tills environment. |  |
| 4 | Payment card devices **are inspected each day**, before use, for signs of tampering. ***(Only answer if Q3 above is answered FALSE)*** |  |
| 5 | Access to credit card information, including the full credit card number, **is limited to authorized staff** whose jobs require this access. |  |
| 6 | Credit/debit card details **are NOT sent or accepted** via email or other messaging technology. |  |
| 7 | We **do not** request the 3 digit security code from the back of the credit/debit card***. (Only answer if NOT using Virtual Keypad)*** |  |
| 8 | Where the card owner has included the 3 digit security code on a form, it is **immediately** rendered unreadable by blacking it out with a ballpoint pen, Photocopied and original destroyed |  |
| 9 | Credit/debit card numbers **are not recorded** on any computer or storage device. |  |
| 10 | Credit/debit card forms & merchant copies of receipts are **securely stored** whilst in the department. Secure storage includes storage prior to shredding. |  |
| 11 | Credit/debit card forms & merchant copies of receipts are destroyed using secure onsite crosscut shredding. ***Please state how long the receipts are stored for in Months/years*** |  |
| 12 | All Credit/Debit card paperwork is kept in an unmarked file |  |
| 13 | We **do not** take, or store, photocopies of credit cards. |  |
| 14 | You have checked in the past 12 months that the 16 Digit PAN no does not appear on retained receipts |  |
| 15 | The Vendor supplied passwords have been changed on any new machines/PDQ’s etc |  |
| 16 | You have changed your PDQ/machine passwords in the last 12 months |  |
| 17 | \*If you have answered false to any of the above, disagree, or have any additional concerns related to credit/debit card security, please provide explanations below: |

I confirm on behalf of my department that the University policy on PCI DSS has been read and understood by **ALL staff** using the credit debit card machine. Completed Departmental PCI DSS staff list attached.

|  |  |  |  |
| --- | --- | --- | --- |
| Signed: |  | Print Name: |  |
|  |  |  |  |
| Job Title: |  | Department: |  |
|  |  |  |  |
| Date: |  |  |  |

|  |  |
| --- | --- |
| Hope Logo | **PCI DSS Staff List** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department** |  |  | **Primary Credit/ debit card machine holder** |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Staff Member Name** | **Email** | **Online Store Training Y/N** | **Date Completed** | **Signature Confirmation\* (See Below)** | **Date** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |
| 16 |  |  |  |  |  |  |

|  |
| --- |
| \***Confirmation -** By signing this form you are confirming that: (a) you have read and understood the PCI DSS policy; and (b) you will ensure that you follow the policy when involved in taking credit and debit card transactions and/or handling data from such transactions. |
|
|