|  |  |
| --- | --- |
| C:\Users\garryrob\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\ICRV480M\UoE_Horizontal Logo_CMYK.JPG | **Departmental PCI DSS Declaration** |

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

The University has to maintain PCI DSS compliance for its card payment activities. This is a mandatory compliance 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 PCI DSS Compliance Policy (available from the Finance Department website) and that your department can confirm that:

|  |  |  |
| --- | --- | --- |
|  | **Please confirm the following:** | **Yes/ No \*** |
| 1 | All staff dealing with credit card data are aware of the importance of cardholder data security and the requirements of the University PCIDSS Compliance policy.  |  |
| 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 authorised 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. |  |
| 5 | Access to credit card information, including the full credit card number, is limited to authorised staff whose jobs require this access. |  |
| 6 | Credit/debit card details are NOT sent or accepted via email or other messaging technology. |  |
| 7 | Credit/debit card details are NOT requested on paper forms. |  |
| 8 | Credit/debit card numbers are not recorded on any computer or storage device. |  |
| 9 | Staff do not use non-authorised e-commerce solutions (https://www.wiki.ed.ac.uk/display/Finance/Online+Payment+Policy). |  |
| 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 by the end of January of the following financial year using secure onsite cross-cut shredding.  |  |
| 12 | Credit/debit card paperwork is separately classified, by for example by using colored paper, to distinguish it from other paperwork. It is NOT labelled as ‘credit card data’. |  |
| 13 | We do not take, or store, photocopies of credit cards. |  |
| 14 | \*If you have answered **NO** 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 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: |  |  |  |

|  |  |
| --- | --- |
| C:\Users\garryrob\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\ICRV480M\UoE_Horizontal Logo_CMYK.JPG | **PCI DSS Staff List** |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Staff Member Name** | **Email** | **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. |
|
|