Risk Assessment – Mobile Devices

Mobile devices such as smartphones, laptops and tablets require special security controls owing to the increased threat to data that working on the move presents. At a minimum the following controls should be implemented on any mobile device used to store or access internal or confidential data:

1. Protected from unauthorised access by at least a 4 digit PIN or a password
2. Configured to ensure they automatically lock after a period of inactivity
3. Configured in such a way that they can be remotely wiped in the event of loss
4. Data is encrypted at rest
5. Only have trusted applications from reputable sources installed
6. Currently receiving software updates from the manufacturer and other third parties
7. Receive software updates for security patches within a reasonable timeframe

Please complete the information below for all portable devices that you use to store or access internal or confidential data. Please add additional rows if required.

**Name: . . . . . . . . . . . . . . . . . . . . . . . . . . .**

**Date of Assessment: . . . . . . . . . . . . . . . . . . . . . . . . . . .**

**Do you use mobile devices to store/access data:** Yes/No

(If yes please complete the table below)

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Serial Number(If applicable) | Type of Data Stored or Accessed (i.e patient data, animal data, email) | Is the Device Secure as per the list detailed in 1-7 above (Yes/No) |
| University Laptop |  |  |  |
| Personal Laptop |  |  |  |
| Mobile phone |  |  |  |
| USB |  |  |  |
| Other(Please specify) |  |  |  |
| Other(Please specify) |  |  |  |

\*Confidential Data would be considered, but not limited to: student or staff records, unpublished research data, patient data, animal data