Model job description

# BYOD Security Administrator

## Scope, purpose and nature of role

The Bring Your Own Device program (BYOD) involves the use of Mobile Device Management (MDM) software to monitor and manage the security of corporate information on the devices. The BYOD Security Administrator is responsible for installing and using MDM and other software on Personally Owned Devices (PODs) belonging to workers, configuring the devices, and administering security on the devices (*e.g*. checking that antivirus software is running, and recovering then deleting corporate data when appropriate). From time to time, the BYOD Security Administrator develops and implements suitable procedures and standards for implementing MDM and securing new types of POD, and may be involved in testing the security of MDM, PODs *etc*.

## Distinguishing characteristics of the ideal candidate

The following personal traits and competencies are high on our wish-list:

* Deeply interested in mobile and portable technologies;
* Competent at administering technologies *e.g*. installing and configuring software on portable ICT devices following technical procedures and standards, and general troubleshooting;
* Trustworthy, with an unblemished record and exemplary ethical character;
* Methodical *e.g*. able to keep good records, check authorizations *etc*.;
* Able to write and implement suitable technical procedures and standards in relation to security of mobile/portable ICT devices, in conformance with information security policies and advice;
* Presentable, personable and diplomatic *i.e*. able to interact with and assist employees (including senior managers, non-technical and technical people) competently and professionally, even when the organization’s interests appear to conflict with those of the POD owners.

## Qualifications, skills and experience

The following are relevant and desirable for this role:

* **IT administration/support:** at least 2 years’ work experience in an IT administration, PC support or similar role;
* **IT degree** or a similar technical qualification *e.g*. CISSP;
* **General:** trustworthy and diligent, able to work without close supervision (after initial training anyway).

Candidates must be willing to undergo background checks to verify their identity, character, competence, qualifications, skills and experience.