Omeath District Development Company

Information Technology Internal Controls

Version Number 1

Adoption by Board: ____/ ____/ ____

Information Technology Internal Controls Checklist

This checklist can be used as a stand-alone self-evaluation tool, or used as a preparatory document, when developing a compliance tracker.

Is each of the Controls listed below in place?	Yes	No
A written information and communications technology policy is in place		
An I.T. risk assessment is conducted at least once every three years		
System security and application access logs are enabled and reviewed for unauthorised access and anomalies on a regular basis		
Back-ups of operating systems, critical data and key software programs are made on a regular basis		
Strong passwords are issued to all employees and volunteers accessing the organisation's systems, data, cloud applications and software programs		
User access to I.T. systems is revoked when that user ceases employment with the organisation or when the user ceases volunteering with the organisation		
Sensitive and restricted data is password protected on all I.T. systems and applications where the data is stored		
Users may only access I.T. systems using the individual passwords assigned to them by the organisation		
Security updates and patches are applied to all servers, workstations and laptops on a timely basis		
A written 'Bring Your Own Device' policy is in place		
All violations and security activities must be logged, reported, reviewed and appropriately escalated to identify and resolve incidents involving unauthorised activities.		
Usage of pirated software within the office premises should not be permitted at all times.		