### 3.1 Inventory of Assets

Define and maintain a comprehensive Inventory of Assets, including all information assets and supporting assets as defined within Section 2.0 of this Policy. The Inventory of Assets shall detail a named owner for each asset, who shall fully understand their responsibilities for the protection of the asset in accordance with the documented Company Asset Management Policy (see **ISDL05**).

### 3.2 Access Control Policy

Ensure that all information assets, and their supporting assets, are protected so as to ensure their confidentiality, integrity and availability is maintained. Access to information assets and supporting assets shall be in accordance with Company's Access Control Policy (see **ISDL07**), and be restricted to the minimum required to undertake authorized business activities, and Company has adopted the principle that "access is forbidden unless it has been specifically and formally pre-authorized".

### 3.3 Information Classification and Handling

Ensure that all information assets shall be classified and handled in accordance with the Company Information Classification and Handling Guide (see **ISDL52**), which details how information assets of different sensitivities shall be managed, handled, processed, encrypted, stored, transmitted, dispatched and disposed of when no longer required. This Guide also details the appropriate levels of personnel screening or clearances necessary to access information of different classifications.

### 3.4 Acceptable Use

Ensure that all personnel, contractors and third party users comply with the Company Acceptable Use Policy (see **ISDL06**) which details how information assets and their supporting assets should be used in an acceptable manner and in accordance with all ISMS related policies and processes. This policy shall detail the acceptable methods of use of information processing systems, networks (including, for example, the internet and telephone systems) and other resources within the Scope of this Policy.

### 3.5 Risk Assessment

Perform regular risk assessments on all information assets, and their supporting assets, as detailed within Company's Risk Assessment Methodology (see **ISDL31**), and using the control objectives and controls as documented within Annex A of ISO/IEC27001:2013. The documented results of risk assessments shall be reviewed to understand the level of risk to information and supporting assets, and appropriate controls implemented as appropriate to address any unacceptable risks that have been identified. A Statement of Applicability (SoA) shall be produced to record which controls have been selected and the reasons for their selection, and the justification for any controls not selected.

### 3.6 Information Security Incidents

Provide a mechanism for the prompt identification, reporting, investigation and closure of information security incidents to Company, in accordance with the Information Security Incident Policy (see **ISDL04**), and to fully analyze reported incidents to identify the root cause of issues and take advantage of any improvement opportunities which may have been identified.

### 3.7 Access to Information and Systems