Company Internal Audit Policy

This policy template should be used to communicate how an organisation uses internal audits to determine the level of compliance with standards, policies and processes. It is common to find a single Internal Audit Policy covering multiple Management Systems (e.g. ISO9001, ISO14001, ISO18001, ISO20000, ISO27001, etc.) as the internal audit methodology will fundamentally be the same. If this is to be the case, the Policy Scope in Section 2.0 will need to be updated accordingly.

1.0 Policy Objectives

- Company operates a rolling programme of internal audits, in order to assess the performance and effectiveness of all of the Company's Management Systems by determining whether:
  - each conforms to the documented requirements of applicable British or International Standards, and any applicable legislation or regulations
  - they continue to align with the Company's goals and objectives
  - they are being properly managed, implemented and maintained
  - any identified corrective or preventive actions required are implemented

2.0 Policy Scope

- Company's Information Security Management System (ISMS), and all related activities that are necessary to allow the Company to continue to conform to the ISO27001 international standard, including all policies, processes, control objectives, controls and supporting records.

- Repeat the above paragraph (if applicable) for the organisation's …
  - *Quality Management System (ISO9001)*
  - *Environmental Management System (ISO14001)*
  - *Occupational Health & Safety Management System (ISO18001)*
  - *IT Service Management System (ISO20000) etc.*

3.0 Policy Statements

- The Company shall compile and communicate in advance a programme of internal audits, which shall include details of those audits which have been arranged to cover the activities, functions and processes detailed within the Scope of this Policy.

- The frequency of internal audits for each activity, function or process shall be determined by the organisation after full consideration of:
  - The activity's level of criticality to the organisation
  - The documented results of previous internal audits
  - The existence of any known issues, incidents or operational challenges
  - Whether the activity is new and has not been subject to a previous internal audit

- All software assets intended to be installed on Company information systems shall be submitted to formal change management approval, and shall only be authorised if:
    - they have been fully and properly evaluated for information security vulnerabilities
    - they have received specific authorisation from change management for the installation
    - the company holds a valid software license for the intended installation
    - they are to be installed strictly in accordance with the vendor's software license
    - the company has the ability to support the software with updates and security patches

- Company reserves the right to monitor and audit instances of installed software on Company assets and systems. Any attempts by users to prevent or interfere with such monitoring or audits will be subject to disciplinary action (see Section 3.1).

- Company shall not permit the connection of any external storage device, including external hard drives, USB memory sticks and memory cards to any Company system without prior permission from Senior Management issued against a valid business requirement. Dependent upon each individual request and the permission granted, sensitive or protectively marked information shall be protected by appropriate encryption. Any such data shall be securely and permanently removed and the device cleansed to acceptable levels at the first available opportunity: simple file deletion shall not be acceptable for this purpose.

- The Computer Misuse Act 1990 covers the offences of illegal accessing and using computer systems without authority, and also the unauthorised introduction of software into a computer system with the intention of either (a) affecting the normal operation of the computer system, or (b) interfering with any data or program stored or installed on the computer system. Users shall maintain awareness of the offences covered by this law.

3.3 Acceptable Use of "Mobile Devices"

- Users of Company issued mobile devices, including laptops, mobile telephones and Personal Electronic Devices (PEDs) shall at all times comply with the issued documented requirements detailing how they are to be accessed, used, stored and protected. Such devices shall be protected by passwords which comply with the requirements of the Company Password Management Policy (see **ISDL03**). Any actual or suspected loss, theft or misuse shall be promptly reported as an Information Security Incident (see **ISDL04**).

- Information on mobile devices, including laptops, mobile telephones and Personal Electronic Devices (PEDs) shall be kept to an absolute minimum to ensure that in the event of loss, theft, misuse or damage then the exposure and liability has been kept to an absolute minimum. Any data which is to be stored on mobile devices shall be encrypted in accordance with Company requirements: if encryption is technically not possible the data storage shall not be permitted. Users of mobile devices shall periodically review the device to purge all unnecessary or historic data. Mobile devices shall never be used to store confidential or secret information, such as password details or electronic bank statements.

- Mobile devices, including laptops, mobile telephones and Personal Electronic Devices (PEDs) which are not Company assets and have not been issued by the company shall not be connected to any information system or network owned by Company.

and to effectively manage and deliver its ISMS, Company shall:

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 authorised business activities, and Company has adopted the principle that "access is forbidden unless it has been specifically and formally pre-authorised".

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 analyse reported incidents to identify the root cause of issues and take advantage of any improvement opportunities which may have been identified.