1.0 Policy Objectives

- To direct the design, implementation and management of an effective Information Security Management System (ISMS), which ensures that **the Company's** information assets are properly identified and recorded, and afforded suitable protection at all times.
- To ensure the confidentiality, integrity and availability of **the Company's** information assets, and supporting assets (including information systems) as defined within the Inventory of Assets.
- To ensure that all vulnerabilities, threats and risks to information assets and supporting assets are formally identified, understood, assessed and controlled in accordance with **the Company's** documented Risk Assessment Methodology.
- To ensure that **the Company's** employees, contractors and third party users comply with this Information Security Policy, and all other ISMS documentation, through the provision of effective information security training, awareness and ongoing monitoring activities.

2.0 Policy Scope

The Company's Information Security Policy shall include the following:

2.1 Information Assets

All information assets (data) either owned by **the Company** or entrusted to **the Company** by a third party under an agreement which specifically details **the Company's** responsibility for that data, and including:

- Information assets held, processed or stored on **Company** premises
- Information assets held, processed or stored at approved off-site premises or locations

2.2 Supporting Assets

All supporting assets (non-data) which by direct or indirect association are an integral part of ensuring the confidentiality, integrity or availability of the information assets described in Section 2.1, including:

- Premises (including offices, factories, data centres and computer rooms storage facilities, recovery sites etc.)
- Hardware (including servers, network infrastructure, laptop computers, desktop computers, storage infrastructure and mobile devices)
- Software (including operating systems, commercially available software applications and software applications developed internally by **the Company**)

- **Company** personnel (including permanent, temporary, full-time and part-time employees, authorised contractors and any third party users of information systems)

2.3 Documentation and Records

All policies, processes, procedures, work instructions and records related to the management, use, control and disposal of the information assets and their supporting assets detailed above.

3.0 Policy Statements

The Company shall be committed to the protection of the information assets and supporting assets as defined within the Scope of this Policy. **The Company** has created its Information Security Management System (ISMS): this framework shall be followed for all information security related activities.

To effectively manage and deliver its ISMS, **the Company** shall:

3.1 Inventory of Assets

Define and maintain a comprehensive Inventory of Hardware and Software 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 this Policy.

3.2 Information Classification and Handling

Company information will be classified into two categories:

- Open - should have no serious or detrimental effect on the organisation in the event of its unauthorised or accidental disclosure or its loss. Consider whether you are comfortable with all of your staff / customers / suppliers / competitors seeing this information. Is it reasonable to assume it's in the public domain
- Company Information - could have a detrimental effect in the event of it's unauthorised or accidental disclosure or loss. Consider it as anything not in the public domain, both structured data (eg orders and financial data in our business systems) and unstructured data (eg documents like contracts, emails and presentations you create or are shared on). All Company Information should
    - only ever be stored on an AG Barr system or computer
    - only be shared externally with a third party in the course of legitimately performing our business and never using a public file sharing service (eg personal email \ social media account or file sharing service like Dropbox

3.3 Access to Information and Systems

Ensure that an **Access Control Policy (**see **HERE)** is in place to protect all **Company** networks, information systems and information assets from any unauthorised access. Legitimate remote access shall only be granted in accordance with the policy to bona-fide personnel, contractors and third party users, and only applies to access from **Company** approved access methods. Remote connections shall be used strictly in accordance with the Acceptable Use Policy. Remote access shall be regularly reviewed and any connections that are no longer required shall be removed.

3.4 Acceptable Use

Ensure that all personnel, contractors and third party users comply with the **Company** IT Acceptable Use Policy (see **HR Services Connect: Policies & Procedures**) 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 Information Security Training

Develop a regular training and education programme which shall be mandatory for all relevant **Company** employees who use Company's Information Assets, which details their individual responsibilities to fully adhere to the requirements of the ISMS policies, processes and work instructions to meet the objectives of this Policy.

3.6 Risk Assessment

Perform regular risk assessments on all information assets, and their supporting assets, as detailed within **the Company's** Risk Assessment Methodology. The documented results of risk assessments shall be reviewed to understand the level of risk to information and supporting assets, and appropriate controls implemented to address any unacceptable risks that have been identified.

3.7 Information Security Incidents

Provide a mechanism for the prompt identification, reporting, investigation and closure of information security incidents to **the Company**, in accordance with the **IT Incident Management Policy** , 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.

3.8 Change Management

Ensure that information security is a key consideration within the IT Change Management Policy and Process so that the security of **Company** information assets is not compromised through system changes.

3.9 Business Continuity Management

Ensure that information security is a key consideration within the Business Continuity Management Policy so that the security of **Company** information assets is not compromised even when faced with a wide variety of unplanned business interruptions.

3.10 Management, Monitoring and Review

Continually monitor, review and improve the **Company** ISMS by undertaking regular reviews, internal audits and other related activities, and taking prompt corrective actions and implementing improvement opportunities in response to the findings of these activities.

3.11 Managing Third Party Risk

Ensure that a process exists for managing third party risks including a register of third parties who have access to, host or manage **Company** Assets is maintained and regularly risk assessed. Appropriate contractual provisions should be made to ensure these Third Parties Information Security responsibilities are clearly defined and can be reviewed regularly through the term of the contract.

3.12 Legislative Compliance

Ensure that, at all times, its Information Security Management System shall support full compliance with the following UK legislation and regulations, including but not limited to:

- Data Protection Act 2018
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Waste Electrical and Electronic Equipment Regulations 2013

- Payment Card Industry Data Security Standard (if applicable)

4.0 ISMS Responsibilities

4.1 Employees, Contractors and Third Party Users

Within **the Company**, all employees, contractors and third party users shall understand their role in ensuring the security of information assets (and their supporting assets) in accordance with the IT Acceptable Use Policy and any further Information Security training provided.

4.2 Senior Management

The Management Committee shall be responsible for the following activities within the **Company** ISMS:

- Agreeing the business need for this ISMS, and communicating their ongoing commitment to it
- Reviewing and signing off this Information Security Policy
- Setting and reviewing **the Company's** Information Security Objectives
- Assigning appropriate resources necessary to manage and operate the ISMS effectively
- Agreeing the level of acceptable risk
- Approving any decisions not to address any unacceptable residual risks, where identified
- Having ultimate responsibility for actions related to information security incidents/breaches
- Overseeing any disciplinary action resulting from information security incidents/breaches

4.3 Information Security Team

The Information Security Team shall have functional responsibility for the **Company** ISMS, and shall be responsible for the daily operational tasks of the ISMS, including:

- Ensuring an appropriate structure of ISMS policies, processes and work instructions
- Ensuring that appropriate records are created and maintained for all ISMS activities
- Ensuring the ISMS operates in accordance with the current requirements
- Arranging a programme of risk assessments, risk treatments and internal audits
- The provision of an appropriate user training and awareness programme for employees

4.4 Department/Function Managers

Managers within **the Company** shall be responsible for:

- Ensuring their team members are aware of and remain compliant with all information security policies, processes and work instructions, and that they receive appropriate training
- The provision of a user training and awareness programme for applicable third party users
- Supporting reviews, internal audits and risk assessments within their area of responsibility

4.5 Asset Owners

Designated Asset Owners shall be responsible for:

- Assessing the value of their asset(s) to **the Company**
- Undertaking detailed risk assessments on their asset(s), including the identification of controls and assessing their effectiveness
- Addressing any unacceptable risks
- Assisting in the investigation, resolution and closure of any information security incident which directly or indirectly affects the security of their asset(s)
- Reviewing and authorising the levels of access to their asset(s) which are granted to others (as per the **Access Control Policy**
- Contributing to the Acceptable Use Policy, specifically for the use of their asset(s)

Last Reviewed : April 2022

Last Updated : April 2021