1   Purpose

This framework guides the creation, use and management of the company's information assets. Regarding all paper and electronic information and its associated systems within the organisation, as well as information held outside the company that affects its regulatory and legal obligations.

2   Scope

The company regards information generated as a vital asset, and the framework is created to:
- Direct all staff and leadership who generate information (i.e. either create or receive), use and distribute information, store and manage information, share information, as well as the disposal thereof.
- Determine the procedures for the management of information in the complete lifecycle as it is shared with all relevant stakeholders, partners and suppliers.
- Distinguish between peculiarities in regard to the management of all paper as well as electronic information and their associated systems within as well as, where relevant, outside the organisation.

3.   References

Protection of Personal Information Act 4 of 2013 (POPI)

Policy: Biddulphs International views information governance as a responsibility. Aiming at governing all information management activities that are performed to ensure value from Information while complying with all regulatory requirements and international best practices.

4.   Information Governance

4.1   Is a strategic, approach to manage all aspects of information within the organisation in accordance with the objectives of the company.

4.2   Provides the framework, systems and processes for ensuring the value of information is maximized, and risks are minimized.

4.3   Considers all information, regardless of its format and includes structured information such as databases and unstructured information such as documents and e-mails.

4.4   Is a subset of corporate governance – it is a strategic rather than tactical discipline, which aligns information management with business strategy and processes and includes, but is not limited to, the following elements:

Cyber Security	Information Management	Records Management	Data Governance
Is about protecting the systems and information security used for business.	Focuses on the management of unstructured information.	Is the activities required to provide evidence of business activities and processes.	Is the management of the integrity, security, availability, and usability of data.

- Information that is already structured in fields such as "date", "title", "subjected", and can be identified by metadata tags.
- Information that does not have a pre-defined information model or is organised in a pre-determined manner.
- A piece of written, printed or electronic matter that provides information or evidence or that serves as an official record.
- The technique of protecting computers, networks, programs, data and information from unauthorised access that are designed for theft or exploitation.
- Data applied to some purpose and adding value for the recipient.
- Information management plans, builds, runs and monitors the practices, projects and capabilities that acquire, control, deliver and enhance the value of data and information assets in alignment with the direction set by the governance structure.
- Information that has been translated into a form that is efficient for movement or processing / facts and statistics collected together for reference or analysis purposes.

- Merging of data quality, data management and risk management surrounding the handling of data. Data governance exercises positive control over the processes and methods used by data stewards and data custodians to handle and make best use of their data assets.

Privacy	Data Analytics	Risk & Compliance
Is the legal obligation of the company to protect personally identifiable information.	Uses systems and software to examine data sets to provide insights from the information within.	Monitors and audits enterprise risk and compliance to meet regulatory requirements.

5. This Framework Ensures That:

5.1 Stakeholder needs are evaluated to determine balanced, agree-on company objectives, which are to be achieved through the acquisition and management of information resources.

5.2 The direction is set for information management capabilities through prioritization and decision making.

5.3 Performance and compliance of the information resources are monitored against agreed-on direction and objectives.

5.4 Clear roles and responsibilities for information management and security are in place, supported by robust policies and procedures, including a framework to protect company information against unauthorized use, compromise of assets and interruption of company activities.

5.5 Information procedures comply with the relevant legislation.

5.6 Information risks are assessed appropriately.

5.7 Appropriate training is available to all staff members.

5.8 Robust arrangements for, and learning from, information related incidents such as data breaches or losses.

5.9 Adequate and appropriate records are maintained, and the sharing of information is carried out in an appropriate manner.

6. Management

6.1 Management oversees the integration of the technology and information strategy into the organisation's strategic agenda and all relevant business processes to ensure and maintain overall compliance, cost effectiveness, sustainability and proper role clarification in regard of the roles and responsibilities.

6.2 Day-to-day responsibility for administration and compliance with this framework is the responsibility of line managers, who need to ensure that:
- Employees under their direction and control are aware of the policies and procedures in their respective departments and applying the policies and procedures carried out their dayto-day work.
- Mitigate information risks.
- Implement security authorization of information.
- Ensure that all staff attend the relevant training sessions related to information management.

6.3 All employees have a responsibility to adhere to the relevant information governance and management standards, policies and procedures. This framework applies to all employees who create, store, share and dispose information.

7. Informing Policies and Rules

7.1 Information governance covers a wide range of policies. To assist the organisation in complying with its duties, the following company policies and rules, amongst others, will be developed that are relevant to information governance:
- Information security policy
- Records management policy
- Retention and disposal schedules i.e. Biddulphs International'sIT asset disposal schedule
- ICT (Information Communication Technology) policy
- Information sharing policy
- Remote Working policy
- Sharing of information with third parties
- Confidentiality policy
- Bring your own device policy

- E-mail management policy
- Data storage and storage devices policy

8.   Informing procedures

8.1   Procedures such as the following will be developed as needed:
- Legal and regulatory compliance procedures
- Creating and receiving information
- Storing and archiving information
- Disposing of information
- Acceptable content types
- Managing the volume of information
- Remote working procedure
- Bring your own device procedure
- Minimum metadata standards
- Reporting information losses
- Reporting information/security breaches
- Information backup and disaster recovery
- Managing personal information
- Collaboration and sharing information

9.   Legislation and external directives

9.1   Instances of statutory directives such as the following steer the process by means of which sound and effective information governance and management are to be established, maintained and monitored by the company& not linked to(This list is non exhaustive)
- The Constitution of South Africa
- Consumer Protection Act, No 68 of 2008
- Protection of Personal Information, No Act 4 of 2013
- Companies Act, No 71 of 2008 and Companies Regulations 2011
- National Credit Act, No 34 of 2005 and National Credit Regulations
- Electronic Communication and Transaction Act, No 25 of 2002
- Regulation of Interception of Communication Act, No 70 of 2002
- Financial Intelligence Centre Act, No 38 of 2001
- Banks Act, No 94 of 1990 ● Compensation for Occupational Injuries and Diseases Act, No 130 of 1993
- Occupational Health and Safety Act, 85 of 1993
- Basic Conditions of Employment Act, No 75 of 1997
- Employment Equity Act, No 55 of 1998
- Labour Relations Act, No 66 of 1995
- Unemployment Insurance Act, No 63 of 2002
- Income tax Act, No 58 of 1962
- Tax Administration Act, No 28 of 2011
- Value Added Tax Act, No 89 of 1991
- Public Finance Management Act, No 1 of 1999
- Health Act, No 63 of 1977
- National Archives and Records Services Act, No 43 of 1996
- National Payment Systems Act, No 78 of 1998
- Skills Development Act, No 97 of 1998
- Copyright Act of 1978
- Various ISO standards, ITIL, TOGAF, COBIT, Val IT, ISO/IEC 20000, ISO/IEC 27002 (formerly 17799), ISO/IEC 38500, ISO 9002, ISO/15489

10.   Information Management

10.1   The company continuously oversees the information management practices that support good decision making, integrity, accountability and transparency which are essential to delivering good business outcomes.

10.2 He company determines how all stakeholders work with the company's information, thus weighing up the practicalities of how to handle it, as well as taking into account the ethical considerations of managing what is at times sensitive and private information.

10.3 The company acknowledges that information management is the organization's responsibility, and needs to be considered not only by the most senior levels of management but by all employees.

10.4 Information management creates value and ensures that the statutory and regulatory requirements can be maintained at all times.

11. Knowledge Management

11.1 Knowledge is information in action as it evolves from information management.

11.2 The company recognizes that it is critical that the knowledge must be managed effectively.

11.3 The company will ensure that processes be defined to manage and measure knowledge flows.

12. Information Security Management

12.1 Physical Security: The company's systems protect information on equipment and premises from unauthorised physical interaction through measures that can be seen or touched, such as:

Keeping Filing Cabinets Locked	Shredding Paper	Locking Office Doors
Deployment of Security Staff	Utilizing Reactive and live CCTV Systems snd Video Surveillance	Hiring Security Personnel
Automated Fire Alarms	Office Alarm Systems	

13. Digital Security

13.1 The company's system protects information on systems and networks from unauthorised electronic interaction through electronic and digital measures, such as:

Effective password management	Anti-virus software up-to-date Software	Ensuring firewalls are locked down
Encrypting, files and e-mails	Hiring cybersecurity experts to conduct penetration testing	On premise servers replicating daily between branches for IT redundancy

14. Operational Security

14.1 The company's system protects information from operational risks inside the organisation through measures that relate to routine functions and operations, such as:

Fostering a culture of security	Adding communication messages when staff log in to the company network	IT providing in-house staff training and awareness regarding security
IT monitoring workstations of staff in the background to ensure the correct application of policies and procedures	Implementing employee on boarding and exit procedures	Providing external staff training

15 Administrative Security

15.1 The company systems protect information from business risks outside of the organization through measures that originate from key decision-makers or formal structures, such as:

Providing awareness training about business risks	Planning around security	Drafting privacy, incident response, and information security policies
Conducting due diligence of subcontractors	Implementing audit controls	Business continuity planning

- The company establishes and maintains policies for the effective and secure management of its information assets and resources;
- The company undertakes or commissions annual assessments and audits of its information and IT security arrangements;
- The company promotes effective confidentiality and security practice to its employees through policies, procedures and training;
- The company establishes and maintains incident reporting procedures and will report, monitor and investigate all reported instances of actual or potential breaches of confidentiality and security by IT and protection services.

16.   IT Architecture and Technology

16.1   The company is concerned about the effective and efficient leveraging of IT technologies and resources to facilitate the achievement of strategic objectives.

16.1.1   Remote Working
- The company develops and maintains policies and procedures to manage the manner how staff should manage information when working remotely.
- The company has a secure network, but when information is taken out of the office, security and confidentiality is at risk and policies and procedures should be developed to address this issue. Architecture can also be called a high-level map or plan of the information assets in an organisation, including the physical design of the building that holds the hardware.
- Employees need to be extremely careful when doing work in public places, working on public Wi-Fi.

16.1.2   Bring Your Own Device (BYOD)
Personal devices could include smart phones, personal computers, tablets, or USB drives. The company will develop and maintain policies and procedures which will:
- Manage how information is going to be kept secure when employees use a personal device for official business.
- Manage the higher risks for the organization in terms of confidentiality and the potential loss of employee and employer privacy.
- Establish a register of users that use a personal device for official business.

16.1.3   E-mail Management
- The company develops and maintains policies and procedures which:
- Ensure data protection though the management of e-mail as information resources.
- Provide standards to all employees on the management of e-mails.

16.1.4   Protection of Personal Information
- The company recognizes the need for the ongoing management of information to ensure that it results in the protection of personal information.
- The company will establish and maintain policies to ensure compliance with the Protection of Personal Information Act 4 of 2013 (POPI)
- The integrity of information will be developed, monitored and maintained to ensure that the information is processed only for the purpose for which it is intended.
- All records of personal information will not be retained any longer than is necessary for achieving the purpose for which the information was collected and subsequently processed.
- The company will have clear procedures and arrangements regarding the lawful processing of information in a reasonable manner that does not infringe the privacy of all stakeholders.
- The company will have clear procedures and arrangements regarding the handling of evidence in litigation, administrative processes and disciplinary actions, labour matters, criminal matters and enquiries.
- The company regards all personally identifiable information relating to employees and clients as confidential except where legislation and/or policy requires otherwise
- In the event of the transfer of personal information to countries outside South African borders, this will be undertaken in accordance with the POPIA and relevant guidelines
- Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

17.   Digital Transformation

17.1   The company explores digital technologies to create new, or modify existing business processes, culture, and customer experiences to meet changing business and market requirements.

17.2   The company develops and maintains policies and standard operating procedures which:
- Emphasize the importance of digitisation
- Set standards for digitising information

18.   Monitoring Risk, Compliance and Effectiveness

Disaster recovery, contingency and business continuity:
- The company implements adequate business continuity through clear policies and standard operating procedures in the event of a disaster.
- The relevant contingency plans (preventative and proactive) and backup strategies are developed and implemented.
- Business continuity is addressed in relevant procedures in order to indicate per business activity and / or process what measures will be put in place to ensure business continuity.

19.   Quality Assurance

- The company establishes and maintains policies and procedures to ensure and improve the quality of information and assessing and minimising risks to the company.
- The company undertakes or commissions annual assessments and audits of its information quality and records management arrangements.
- All managers are expected to take ownership of, and seek to improve, the quality of information within their respective services.
- Wherever possible, information quality should be assured at the point of collection and / or generation.
- Data standards will be set through the clear consistent definition of data items, in accordance with international and / or national standards.

20.   Revision

This framework will be revised or as the need arises.

21.   Change / Revision History

Change History			
Rev No	**Changes**	**Pages**	**Effective date**
0	Cyber Security Information Governance POLICY	All	February 2023

22.   Approval

Designation	**Name**	**Signature**
Managing Director	O Farmerey	