Khuseti
HOLDINGS

DATA CLASSIFICATION POLICY	
Classification	POPIA / 03
Responsible person	Information Officer / deputy information officers
Version	2021/06
Review date	2022/06
Guideline documents	Werksmans Attorneys
Author	Nawhal Kock
CEO Approval	**Andre Els**
Signature	

1 OVERVIEW AND PURPOSE

1.1 Khuseti uses a variety of data in order to conduct its business. This data ranges from manufacturing information, bills of material to financial, customer and human resource information. All this information is important to the business of Bidvest and must be protected against unauthorized disclosure, destruction or alteration.

1.2 The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value and criticality to Khuseti to ensure that sensitive corporate and customer data/information (these terms are used interchangeably herein) can be secured appropriately.

2 APPLICABILITY

This policy applies to all employees of King Pie, BMO and third party agents authorised by the companies to access the data. In addition, ***this policy applies to any form of data, including physical and electronic data stored on any type of media.***

3 DATA CLASSIFICATION

3.1 Data classification is the classification of data based on its level of sensitivity and impact it has should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding the data.

3.2 King Pie and BMO utilizes a three-tiered system for classifying data as follows –

CLASSIFICATION	DEFINITION
Restricted	• Data should be classified as restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to Khuseti.. • This may include information that is considered trade secrets, strategic planning as well as special personal information as recognised by POPIA.
Private	• Data should be classified as private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to Khuseti. • This includes information that is contractually protected and any other information that requires protection from the public.
Public	• Data should be classified as public when the unauthorised disclosure, alteration or destruction of that data would result in little or no risk to Bidvest. • While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorised modification or destruction of Public data.

3.3 Notwithstanding the classification of data, all data is considered to be the property of King Pie and BMO. The data must not be used in any manner not associated with the business.

4 ROLES AND RESPONSIBILITIES

For purposes of this policy, roles and responsibilities are defined as follows –

4.1 **Data Owner** – The individual who is ultimately responsible for the data and information being collected and maintained by his or her department. The Data Owner shall be responsible for the following –

4.1.1 Understanding how the data is used in the business and appropriately evaluating its value to the business. This responsibility may reside with one individual or it can be shared or delegated to a number of individuals;

4.1.2 Making business decisions relating to the classification and the appropriate protection, dissemination, retention and use of the data;

4.1.3 Ensuring that the appropriate operational processes and procedures are in place to establish and maintain the confidentiality, integrity and availability of the data;

4.1.4 Reviewing usage information for compliance purposes; and

4.1.5 Approving access to the data (and/or delegating this permission).

4.2 **Data Custodian** – These are employees who have administrative and/or operational responsibility over proprietary information of King Pie and BMO. For example, this may include technicians and or the IT Manager from the IT Department. They are responsible for –

4.2.1 implementing owner-specified controls over the data on the server with specific access;

4.2.2 maintaining detailed knowledge of the data on server within their trust;

4.2.3 providing physical and procedural safeguards for detecting, reporting, and investigating information security breaches; For example VPN access from outside.

4.2.4 assisting owners in evaluating the cost-effectiveness of controls; and

4.2.5 Monitoring and ensuring that users comply with security procedures.

4.3 **Data User** – These are employees, contractors or third parties who are authorised to access data and/or the systems of the company. They are responsible for –

4.3.1 using data only for purposes specified by the owner;

4.3.2 complying with security measures specified by the owner or custodian;

4.3.3 protecting the data from unauthorised access and reporting information security information violations to the owner or the custodian; and

4.3.4 Maintain the confidentiality of the data.

5 DATA CLASSIFICATION PROCEDURE

The classification of data should be performed by an appropriate Data Owner. Please refer to Annexure A containing a flowchart for the classification of data. In what follows, we set out the procedure to be followed in respect of classifying data –

5.1 **Data Owners must review each piece of data they are responsible for and determine its overall impact level as follows –**

5.1.1.1 if the data is the same or similar to any of the predefined types of restricted information listed in Annexure B, the Data Owner assigns it an overall impact level of "*High*";

5.1.1.2 if the data does not match any of the predefined types in Annexure B, the Data Owner should determine its information type and impact levels with reference to paragraph 6 and Annexure C;

5.1.1.3 if the information type and overall impact levels still cannot be determined, the Data Owner must work with the data custodians to resolve the classification of the data.

5.2 **The Data Owner assigns each piece of data classification label based on the overall impact level as follows –**

OVERALL IMPACT LEVEL	CLASSIFICATION LABEL
High	Restricted
Moderate	Confidential
Low	Public

5.3 **The Data Owner shall record the classification label and overall impact level for each piece of data in a data classification table either in a database or on paper (see Annexure C);**

5.4 **The Data Custodians shall apply appropriate security controls to protect each piece of data according to the classification label and overall impact level recorded in the data classification table (see Annexure C).**

5.5 The following questions should be kept in mind when classifying data –

Does the document contain information that originated from an open and publicly accessible source?	Provided the document contains information that was not obtained in breach of any confidentiality or secrecy obligation and is in the public domain, the document may be classified as open or public depending on the other questions to be considered below.
Does the document contain personal data?	See the Data Protection Policy for a definition of "personal data", but as a general guide, this is any information that may directly or indirectly identify an individual (called a ("**Data Subject**"). Documents that contain personal data should be classified as Confidential.

Does the document contain special categories of personal data or personal data relating to criminal convictions and offences?	See the Data Protection Policy for a definition of these categories of personal data. This information requires additional procedures to be followed and safeguards applied and should be classified as Strictly Confidential.
Does the document contain any information of commercial or competitive value for Bidvest or any other third party?	The document may contain commercially sensitive information or trade secrets relating to Bidvest or entrusted to Bidvest by a third party or information relating to Bidvest's strategic plans and market opportunities.
If the document was accidentally disclosed, would it pose a risk to any individual(s) or Bidvest?	The document may contain information that would have an adverse impact on one or more individuals or groups within Bidvest, Bidvest as a whole (including reputational harm) or Bidvest's agents, suppliers or other partners.

6 IMPACT LEVEL DETERMINATION

The purpose of the table below is to assess the potential impact to Bidvest arising from a loss of the confidentiality, integrity or availability of data that does not fall into any of the information types described in 5 above. This table is also intended to assist in classifying data based on the impact of disclosure.

SECURITY OBJECTIVE	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality Restrict access to and disclosure of data to authorised users in order to protect personal privacy and secure proprietary information.	Unauthorised disclosure of the information is expected to have **limited** adverse effects on operations, organizational assets, or individuals.	Unauthorised disclosure of the information is expected to have a **serious** adverse effect on operations, organizational assets, or individuals.	Unauthorised disclosure of the information is expected to have a **severe or catastrophic** adverse effect on operations, organizational assets, or individuals.
Integrity Guard against improper modification or destruction of data, which includes ensuring information nonrepudiation and authenticity.	Unauthorised modification or destruction of the information is expected to have a **limited** adverse effect on operations, assets, or individuals.	Unauthorised modification or destruction of the information is expected to have a **serious** adverse effect on operations, assets, or individuals.	Unauthorised modification or destruction of the information is expected to have a **severe or catastrophic** adverse effect on operations, assets, or individuals.
Availability	Disruption of access to or use of the information or	Disruption of access to or use of the information or	Disruption of access to or use of the information or

Ensure timely and reliable access to and use of information.	information system is expected to have a **limited** adverse effect on operations, assets, or individuals.	information system is expected to have a **serious** adverse effect on operations, assets, or individuals.	information system is expected to have a **severe or catastrophic** adverse effect on operations, assets, or individuals.

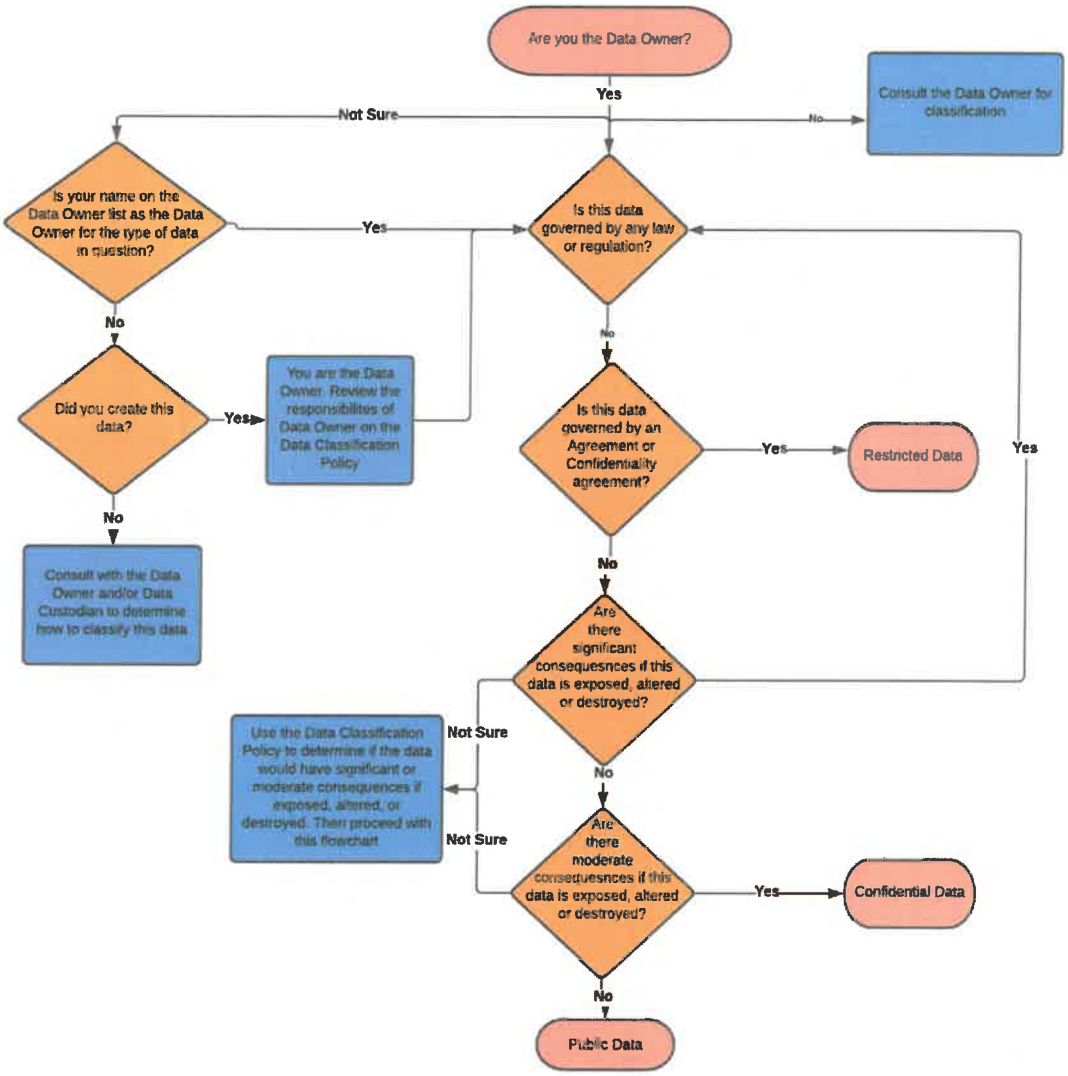
7 POLICY REVISION

This Policy is subject to review and amendment without prior notice. However, we undertake to ensure that any amendments hereto are communicated clearly and effectively, for the benefit of our employees and any other persons who may be affected by this Policy.

8 VERSION CONTROL

Last updated **May 2021**.

ANNEXURE A – DATA CLASSIFICATION FLOWCHART



ANNEXURE B – TYPES OF INFORMATION THAT MUST BE CLASSIFIED AS RESTRICTED

RESTRICTED DATA	
Authentication information	Authentication information is data used to prove the identity of an individual, system or service. Examples include – • passwords; • share secrets; • cryptographic private keys; and • hash tables.

Special personal information	Section 26 of POPIA creates a general prohibition on processing special personal information. This information includes –
	• the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of an individual; or
	• the criminal behaviour of an individual to the extent that such information relates to –
	  • the alleged commission by an individual of any offence; or
	  • any proceedings in respect of any offence allegedly committed by an individual or the disposal of such proceedings.

Personally identifiable information ("PII")	PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements – • identity number; • driver's license number; • financial account number in combination with a security code, access code or password that would permit access to the account; and/or • medical aid and/or insurance information.
Payment card information	Payment card information means a credit card number in combination with one or more of the following data elements –

	• cardholder name; • service code; • expiration date; • CVC2, CVV2 or CID value; • PIN or PIN block; and • contents of a credit card's magnetic stripe.

ANNEXURE C – DATA CLASSIFICATION TABLE

DATA DESCRIPTION	RESTRICTED (HIGH)	CONFIDENTIAL (MODERATE)	PUBLIC (LOW)
Corporate			
Strategic planning	X	X	
Projects	X		
Management discussions and analysis (MD&A)	X		
Unpublished financial information	X	X	
Human Resources			
Employee information	X	X	
Suppliers, contractors, 3rd party agents		X	
Identity numbers of employees	X		
Employee health	X		
Employee disciplinary record	X		
Employee remuneration		X	
Bidvest policies		X	
Employee criminal records	X		
Finance			
Service providers		X	
Suppliers		X	
Accounts payable		X	
Accounts receivable		X	
Tax		X	
Purchase order		X	
Product pricing		X	
Sales		X	
Business opportunities		X	
Customers		X	
Budget plan	X	X	
Financial forecast	X	X	
Production			
Suppliers		X	
Service providers		X	
Procurement		X	
Purchase orders		X	
Sales		X	
Customers		X	
Products		X	
Product pricing		X	
Strategic planning	X	X	

Public			
Publicly posted content on all external-facing social media interfaces			X
Publicly-posted press releases			X
Publicly-posted newsletters			X
Maps to offices			X
General			
Full names		X	
Date of birth		X	
Marital status		X	
current and previous address		X	
Landline and/or mobile number		X	
Email address		X	
Bank details			
Marketing strategy		X	
Data entrusted to Bidvest by other companies or data subjects	X	X	
Patents, formulas or new technologies	X	X	
Undisclosed mergers and acquisitions	X	X	

ANNEXURE D – INTEPRETATION

1 INTERPRETATION

In this Policy, the following words and expressions bear the meaning assigned to them below -

1.1 **"Data Subject"** means the natural or juristic person to whom Personal information relates;

1.2 **"Document"** means information and its supporting medium, and includes, without limitation, a wide range of both hard copy and digital formats including letters, emails, policies, guidance notes, meeting papers, minutes, reports, contracts, presentations, and official communications. It is not limited to written information, but can also take the form of a photograph, video or audio record of an event. Voicemail, text or instant messages, however, do not constitute documents for the purposes of this Policy, unless recorded or retained for specified purposes in accordance with legal requirements;

1.3 "**Employees**" means any such person as defined in the Labour Relations Act 66 of 1995, under the employ of Bidvest, and any other such person who may conduct work for or on behalf of Bidvest on a once off or ongoing basis, as the case may be;

8.1 "**Individual**" means a Data Subject as defined in terms of section 1 of POPIA;

1.4 "**Organisation**" means Bidvest and all of its affiliates and subsidiaries;

1.5 "**Personal Information**" bears the same meaning as defined in POPIA;

1.6 "**POPIA**" means the Protection of Personal Information Act No. 4 of 2013.