## Protection of Personal Information Policy and Procedure

1. **Abbreviations, acronyms and definitions**

| **Term** | **Description** |
| --- | --- |
| **Data subject** | The person whose personal information is processed by the Organisation. |
| **HR** | Human Resources |
| **Information officer** | The person appointed in terms of the POPI Act. The owner, chief executive officer (CEO), the equivalent officer of the juristic person, any person duly authorised by that officer or the person who is acting as such, or any person duly authorised by such acting person. |
| **IS** | Information System(s) |
| **IT** | Information Technology |
| **PC** | Personal Computer |
| **Personal information (PI)** | Means a person’s name (including a juristic person e.g. an Organisation), contact details, race, gender, age, marital status, language spoken, religion, sexual orientation, personal and political views, private correspondence, health records, employment records, financial records, views held by others on the person, biometrics (DNA, fingerprints, etc.). |
| **POPI** | Protection of Personal Information |
| **POPIA** | Protection of Personal Information Act (No. 4 of 2013) |
| **Processing** | Any action or operation – whether automated or not – concerning personal information that is collected, collated, recorded, filed, organised, stored, retrieved, updated, disseminated by physical or electronic means, merged, linked, restricted, erased or destroyed. |
| **Social media** | Any form of online publication or presence that allows interactive communication, including, but not limited to, social networks, blogs, internet websites, internet forums, intranet and wikis. Examples of social media include, but are not limited to, Facebook, Twitter, Instagram, YouTube, Periscope, LinkedIn, Pinterest, Snapchat, Google+, Tumblr and Flickr. |
| **Regulator** | The office, as set out in the POPI Act. |
| **Special personal information** | Personal information over which additional safeguards are imposed by the POPI Act. Race, religion, biometrics, trade union membership, political affiliation, sexual orientation, health records and unproven criminal behaviour are defined as “Special personal information”.  |

1. **Purpose**
	1. SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_ seeks to balance the constitutional right to privacy with commercial requirements to use and process personal information (PI).
	2. As an employer, SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_ has a legal obligation to inform employees about the manner in which their personal information is used, disclosed and destroyed.
	3. SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_ is committed to protecting its employees’ privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.
	4. This policy seeks to regulate and formalise how SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ collects, stores, protects, assesses and distributes information and to protect the on-going integrity and sensitivity of personal data and private information.
2. **Scope**
	1. This Policy is relevant and applicable to all SHERIFF\_\_\_\_\_\_\_\_\_\_\_ employees; in addition, the good practice principles advocated in the Policy should also be extended to others external to SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	2. The Policy sets out the key approaches to the management of the good protection of personal information and uses the language of the Protection of Personal Information Act(POPIA) of 2013 (e.g. the Data Subject would be the person whose information has been collected which, in most cases, would be an employee).
	3. The policy covers all means and mechanisms for storing information including paper and electronic records, laptops and PCs, mobile phones and USB memory sticks.
	4. It includes, but is not limited to. Human Resources and payroll records, applications for employment, contracts, and CCTV records.
3. **Policy**
	1. Organisation of employees’ and stakeholders’ personal information
		1. SHERIFF\_\_\_\_\_\_\_\_\_\_ will collect PI for specific, explicitly defined and lawful purposes related to the function or activity of the responsible party. The Data Subject will be made aware of the purpose of collecting their PI and new employees will be alerted to this in the employment contract prior to joining the Organisation.
		2. Personal information will not be collected indiscriminately, and will be limited to what is necessary to fulfil the specific purpose for which the PI is being collected.
		3. When collecting PI, the responsible party shall obtain expressed consent from the Data Subject, to use, collect, retain or disclose said PI. The SHERIFF\_\_\_\_\_\_\_\_\_\_\_ undertakes to obtain written consent wherever possible; alternatively, a recording must be kept of the verbal consent. The consent must be clear and verifiable.
		4. When collecting PI, the responsible party shall ensure that the Data Subject understands what information is collected, why it will be used, how it will be processed and to whom the information will be given.
		5. Data Subjects may request to be given a copy of their PI and, unless there are statutory restrictions, the information is to be given to the Data Subject.
		6. The Data Subject is to be informed that they may request that their PI be corrected, updated or deleted. SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_ will comply with such a request if it is merited and to notify the Data Subject what changes have been made.
		7. The Data Subject may at any time object or withdraw their consent, subject to legal and contractual restrictions by giving reasonable notice. The responsible party may then no longer process the PI.
		8. Data subjects are to be advised promptly of any breaches of security regarding their personal information. They are to be informed of the data affected, the impact of the breach on the Data Subject, steps taken to prevent any further breaches, recommended steps that the Data Subject could take to protect themselves and who has such information(if this is known).
		9. In instances where SHERIFF\_\_\_\_\_\_\_\_\_\_\_ intends to undertake additional processing of PI, it will firstly seek the voluntary consent from the relevant Data Subjects for such further processing.
		10. SHERIFF\_\_\_\_\_\_\_\_\_\_\_ will only process information if:
			1. The data subject has consented;
			2. Processing is necessary for the conclusion or performance of a contract to which the data subject is a party;
			3. There is a legal obligation to do the processing;
			4. Processing protects the legitimate interests of the Data Subject;
			5. Processing is necessary for the proper performance of a public law duty by a public body;
			6. Processing is necessary for the pursuit of legitimate interests of the responsible party;
			7. Personal information will be collected directly from the Data Subject except if:
				1. The information is contained in a public record or has deliberately been made public by the Data Subject
				2. The Data Subject has consented to the collection from another source.
				3. Collection from another source would not prejudice a legitimate interest of the Data Subject.
				4. Collection from another source is necessary:

To maintain law and order.

To enforce legislation concerning the collection of revenue;

For the conduct of court or tribunal proceedings; and

As outlined in POPIA.

* + 1. The responsible party must take reasonably practical steps to ensure that PI is complete, accurate, not misleading and updated where necessary. Whenever employees’ PI changes they are required to inform the responsible person so that their records remain accurate.
		2. Special Personal Information (SPI) would not be processed unless a general authorisation or, alternatively, a specific authorisation relating to the different types of SPI applies or it is allowed by the law.
		3. Processing of PI of children will only be conducted within the guidelines of Section 35 of the POPIA and is only allowed under the following circumstances:
			1. Carried out with the prior consent of a competent person;
			2. Necessary for the establishment, exercise or defence of a right or obligation in law;
			3. Necessary to comply with an obligation of international public law;
			4. For historical, statistical and research purposes to the extent that:
				1. The purpose serves a public interest and the processing is necessary for the purpose concerned; or
				2. It appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the individual privacy of the child is not disproportionately affected; or
				3. The PI of the child has been deliberately made public by the child with the consent of a competent person.
		4. Processing of trans-boarder PI will comply with Chapter Nine, Section 72 of POPIA and adhere to the requirements below:
			1. The receiving country has similar laws in place;
			2. The organisations have binding corporate rules (corporate group information processing policies);
			3. A contract has been concluded between the controller/processor sending data and the controller / processor receiving data;
			4. The Data Subject consents;
			5. Transfer is necessary for performance of a contract to which the Data Subject is a party;
			6. The transfer is necessary for a contract in the interest of a Data Subject;
			7. Transfer is for the benefit of the Data Subject and obtaining consent is impractical
	1. Information Officer
		1. SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_ will appoint an Information Officer with employees as agreed with the Board. The Information Officer reports to the Board and the Regulator. All persons collecting, processing or using PI are accountable to the Information Officer.
		2. All responsible parties will sign a confidentiality agreement, and
		3. The main responsibilities of the Information Officer are:
			1. To review procedures for processing personal information and ensure all such procedures are lawful and only the minimum amount of information is processed; and that due controls are in place for “special personal information”;
			2. To ensure that, before any personal information can be processed, the purpose of such processing is clearly defined;
			3. To audit and maintain the accuracy and integrity of processes used to collect, collate, record, file, organise, store, retrieve and update personal information;
			4. That the Organisation can distinguish between employees’ and external stakeholders’ personal information;
			5. To ensure SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ have systems to detect and report on any breach of security of personal information;
			6. To ensure procedures to obtain the consent of Data Subjects are implemented;
			7. To be able to respond to data subjects if they request access to their personal information;
			8. That all employment and other third party contracts are amended to comply with POPI;
			9. To ensure that any complaints are investigated and that the complainant has been informed of the findings and the corrective action taken;
			10. To ensure all SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_ employees who might collect, use or retain PI have been adequately trained;
			11. To ensure That all statutory requirements are met in terms of reporting to the Regulator.
	2. Safeguarding PI:
		1. SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ will take all reasonable steps practicable to secure and safeguard the integrity and confidentiality of the PI in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss, damage or unauthorised destruction, unlawful access to, or processing of the PI.
		2. Records will not be retained any longer than is necessary for achieving the purpose for which it was collected unless:
			1. further retention is required by law;
			2. the responsible party reasonably requires to keep it;
			3. retention is required by a contract between the parties, or
			4. the Data Subject consents to the further retention.
		3. The responsible person is responsible to ensure that PI is destroyed, deleted or de-identified as soon as is reasonably practical. Destruction or deletion must be done in a manner that prevents its reconstruction in an intelligible form.
		4. Any breach of any of the terms of this policy will be subject to disciplinary action in line with the SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ disciplinary code.
	3. Incident Response
		1. Will be dealt with in line with the applicable Code of Conduct.
		2. All complaints must be submitted in writing to the Information Officer who will attend to them as outlined in the SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Grievance Procedure
1. **References**
	1. The SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Employment Contract.
	2. Constitution of the Republic of South Africa Act, 108 of 1996.
	3. Protection of Personal Information Act (POPIA) 4 of 2013
2. **Procedure**
	1. All employees are required to sign the SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ POPIA policy acknowledgement form when they commence employment and annually, thereafter.
	2. Annual compliance audits will be conducted on security measures to safeguard PI and all the findings will be presented to the Information Officer.
3. **Templates**
	1. POPI Consent Addendum to the Employment Contract.
	2. POPI Acknowledgement Form .

SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date Adopted: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Protection of Personal Information Act (POPIA) Policy Acknowledgement Form

Protection of Personal Information Act (POPIA)Policy Acknowledgment

By signing this document, I **[insert employee’s name]** hereby:

1. Confirm that I have read the SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ POPI policy and that I have been given the opportunity to refer any aspects that are unclear to me or questions I might have to the Information Officer.
2. Give consent that my personal information (PI) may be collected, processed and stored in line with the policy and my employment contract.
3. Acknowledge that SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_ endeavours to keep my PI up to date, and that it is my responsibility to keep SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ informed of any changes to my PI and to provide the relevant details timeously. I understand that I have the right to check my PI retained by SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to ensure that it is correct, complete and current. All this information is supplied voluntarily, without undue influence from any party and not under any duress.
4. Accept that I have the right to:
5. Know what information is being kept and how that information is being used;
6. Access the information at any reasonable time to rectify and correct my PI details;
7. Revoke my consent given to SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_\_ in terms of this form at any time. This revocation must be in writing and addressed to the Information Officer. Any such action would require SHERIFF\_\_\_\_\_\_\_\_\_\_ to review the impact this may have on the employment relationship. Withdrawal of consent is not retroactive and will not affect use of my information already made.
8. Lodge a complaint to the SHERIFF\_\_\_\_\_\_\_\_\_\_\_\_ Information Officer or Information Regulator.

I agree to report any breach with regards to this policy to the Management promptly and to comply with the policy and the procedures described therein.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name Employee Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

Witness Name Witness Signature Date