



STATE BANK OF INDIA South Africa

PROMOTION OF ACCESS TO INFORMATION MANUAL

Compiled in terms of Section 51 of the Promotion of Access to Information Act,
2 of 2000 ('the Act')

State Bank of India South Africa Operations PAIA- 2022-2023

Version Number	3
Applicable for Year	2022-2023

Document Information

Document Owner	Country Head & Chief Executive Officer, State Bank of India, Johannesburg Bank Branch, South Africa
Document Prepared By	Chief Operating Officer South Africa
Document Reviewed By	Branch Compliance Committee
Document Approved By	Compliance/ Risk Management Committee

Contents

1. PURPOSE OF THE MANUAL.....	4
2. STATE BANK OF INDIA CONTACT DETAILS	4
3. ORGANOGRAM.....	5
4. STATE BANK OF INDIA PRIVACY PRACTICES.....	6
5. SAFEGUARDING CLIENTS INFORMATION	12
6. CATEGORIES OF RECORDS	13
7. CONSIDERATIONS BEFORE SUBMITTING A REQUEST.....	15
8. REQUEST PROCEDURE.....	15
9. TIMELINES FOR CONSIDERATION OF THE REQUEST	16
10. GROUNDS FOR REFUSAL OF ACCESS TO RECORDS.....	16
11. REMEDIES AVAILABLE TO A REQUESTOR ON REFUSAL OF ACCESS.....	17
ANNEXURE 1:.....	18
ANNEXURE 2:.....	22

1. Purpose of the manual

This guide to accessing records held by State Bank of India is intended to provide guidelines to members of the public who wish to exercise their constitutional right to access to information.

This manual will provide information on how a request may be lodged; a description of the types of records that will be made available; grounds for refusal; what procedure will be followed in considering the request; the applicable fee structure; and information on the appeals procedure should the requestor of the information not be satisfied with the outcome request.

2. State Bank of India contact details

Information Officer: Chief Executive Officer

Physical Address: 11 Cradock Avenue
Rosebank
Johannesburg

Postal: PO Box 2538
Saxonworld
2132

Tel: +27 011 778 4507

Fax: +27 011 788 6769

Email: ceo.rsa@statebank.com
Website: za.statebank

Deputy Information Officer: Chief Operating Officer

Physical Address: 11 Cradock Avenue
Rosebank
Johannesburg

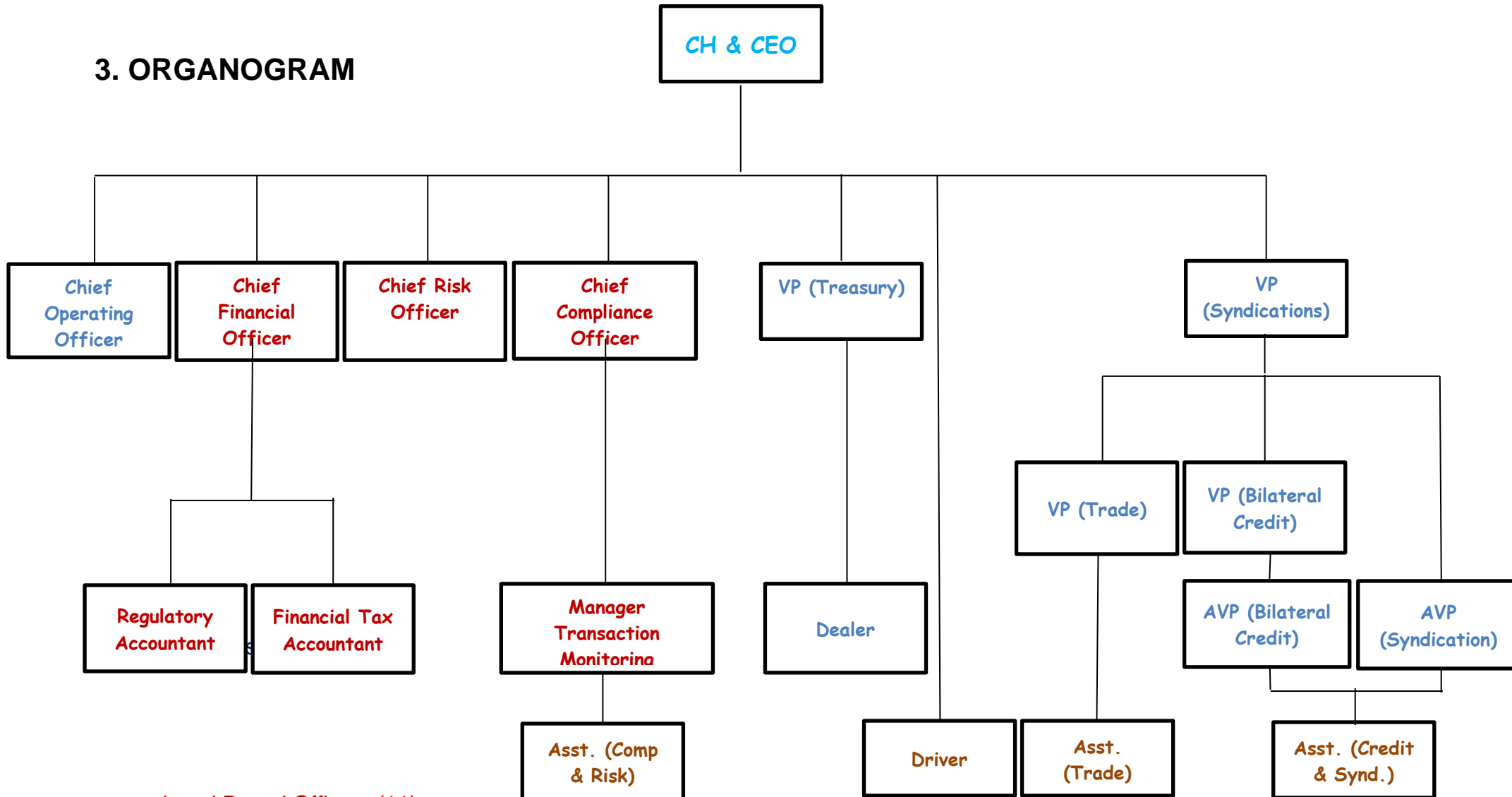
Postal: PO Box 2538
Saxonworld
2132

Tel: +27 011 778 4504

Fax: +27 011 788 6769

Email: mgrbanking.rsa@statebank.com
Website: za.statebank

3. ORGANOGRAM



- Local Based Officers (11)
- Local Based Staff (Other than Officers) (16)

ROLES AND RESPONSIBILITIES

Chief Operations Officer

He/ she must ensure compliance with the following:

- AML/CFT Policy & The Risk Management Compliance Programme
- Compliance Policy
- Human Resources Policy
- Operational Risk Management Policy
- Record Retention Policy
- IT & IT Security Policy
- Fraud Management Policy

In addition to complying with all the legislation listed in regulatory universe, the following also needs to be done:

1. Monitoring of Cash Transaction Reporting, Suspicious Transaction Reporting, Terrorist Property Reporting
2. Ensuring Day books are distributed and up to date
3. Ensuring that HBOPCUS Reporting to the South African Reserve Bank is completed and is up to date
4. Monitoring that all Nostro accounts are reconciled timeously
5. Monitoring that Samos accounts are reconciled timeously
6. Ensuring that alerts generated via AMLOCK for his/her profile, is investigated and cleared/escalated on a regular basis and within the timelines stipulated in the Transaction Monitoring Policy
7. Ensuring that the correct process is followed as per the AML/CFT policy when new accounts are opened, and existing accounts are reviewed.
8. Ensuring that the VAT is paid on a monthly basis and the VAT and Income Tax returns are filed on time to the South African Revenue Service.
9. Compilation of a mini balance sheet and profit and loss statement on a monthly basis.
10. Submission of CEO's monthly report to the Corporate Centre (IBG) Mumbai (Head Office).
11. Ensuring the payment of all the bank licenses to the various regulators.

Vice President (Treasury)

He/ she has to ensure compliance with the following:

- ALM Policy
- Forex Trading Policy
- Investment Policy
- Policy for Derivatives
- Market Risk Management Policy
- ORM Policy
- IT & IT Security Policy
- Compliance Policy
- Human Resources Policy

• In addition to complying with all the legislation listed in regulatory universe, the following also needs to be done:

1. The following needs to be monitored on a daily basis to ensure compliance:
 - - Net Overnight Open Position
 - - Aggregate Gap Limit
 - - Individual Gap Limit
 - - Liquidity Position of the branch

- - Mark to Market of securities
- - BA 325
- He/she has to ensure that the Bank is within the prescribed limits set by the regulators and has to inform management should any limits be breached.

Vice President (Syndications)

He/ she has to ensure compliance with the following:

- Credit Policy
- Human Resources Policy
- Compliance Policy
- IT & IT Security Policy

In addition to complying with all the legislation listed regulatory universe, the following also needs to be done:

1. Approvals for sanctioning of loans are achieved through the correct process
2. All KYC/AML related requirements are met.
3. Ensure that the following is submitted to the Head Office (IBG) and the Reserve Bank of India:
 - Non- performing assets (NPA) and Provision Report
 - Advanced Under Collection Account (AUCA) Return
 - New Business Data
 - Country Risk Return
 - NPA and AUCA Return
 - Specialised Mentioned Account (SMA) Return
 - Standard Assets Irregularity Return
 - Overseas Operation Return to Reserve Bank of India
 - Prudential Exposure

Chief Compliance Officer:

Responsibility will broadly include;

- i. Responsible for compliance with all applicable regulatory guidelines (both host and home country regulatory guidelines) and for implementation of compliance risk management framework and effective management of compliance risk.
- ii. Responsible for the robust compliance culture amongst all functionaries and implementation of zero tolerance of non-compliance.
- iii. Responsible for guidance under Host Country Regulations to various departments.
- iv. Responsible for any task or guidance under Host Country Regulatory prescriptions.
- v. Responsible for and would monitor compliance risk-based review of Internal Audit reports, incidents reported and other monitoring mechanisms.
- vi. Framing and implementation of branch compliance policy and coordinating and liaising with SARB, FSB and NCR for all issues relating to all core areas of compliance and reporting. He/she acts as the nodal point of contact between branch and the local regulator.
- vii. Chief Compliance officer is responsible for implementations of compliance policy of the bank.

- viii. Arranging and ensuring compliance awareness amongst the staff through training, seminars etc.
- ix. Oversee Transaction monitoring and reporting.

Chief Financial Officer

1. Setup the finance function within the bank as per the established reporting structure
2. Compiling all financial reports in consultation with the department/divisional heads.
3. Oversight of all the taxation matters such as VAT, Income Tax, Payroll taxes etc. at the bank.
4. Responsible for ensuring integrity, accuracy and completeness of financial data.
5. Overseeing the entire Bank's fiscal operating results in compliance with all accounting principles (including regulatory agencies, government policies and local laws) for ensuring & safeguarding the Bank's interests in consultation with other department heads.
6. Reviewing of all major MIS returns prepared by various department heads as well as presenting it to the Banks management in consultation with the Country Head & CEO.
7. Preparing for and ensuring completion of Annual financial statements and related returns in consultation with department heads and statutory auditors.
8. Oversee the preparation and submission of quarterly financial reports and returns to be submitted to the head Office.
9. Responsible for ensuring integrity, accuracy and timely submission of BA Returns to SARB.
10. Responsible for liaising with the external / Internal auditors regarding financial statements & reporting.
11. Oversight on the implementation of the IFRS reporting standards within the Bank
12. He/she is also responsible for the submission of the BA (Basel) returns on a monthly as well as quarterly and half yearly basis within time period stipulated by the South African Reserve Bank. He is responsible for the submission of the following returns pertaining to Market Risk:

Sn	Name of Return	Periodicity
1.	BA100	15th day return
2.	BA110	15th day return
3.	BA120	15th day return
4.	BA310	15th day return
5.	BA900	20th day return
6.	BA320	20th day return
7.	BA330	20th day return
8.	BA340	20th day return
9.	BA350	20th day return

10.	BA500	20th day return
11.	BA700	20th day return
12.	BA930	20th day return
13.	BA920	20th day return
14.	BA941	Quarterly
15.	BA942	Quarterly
16.	BA943	Quarterly
17.	BA944	Quarterly

Chief Risk Officer

He/ she has to ensure compliance with the following:

- Human Resources Policy
- Compliance Policy
- Operational Risk Management Policy 1. To oversee the Bank's Risk Policies inclusive of the Risk Appetite Statement
- 2. Holding monthly RCOM meetings.
- 3. Completing RCSA exercise.
- 4. Monitoring Near Miss & Loss events and conducting the root cause analysis monthly.
- 5. Monitoring the various limits and ratios.
- 6. Conducting Materiality Risk Assessment (Out sourced activities).

In addition to complying with all the legislation listed regulatory universe, the following also needs to be done:

7. He/she is also responsible for the submission of the BA (Basel) returns on a monthly as well as quarterly and half yearly basis within time period stipulated by the South African Reserve Bank. He is responsible for the submission of the following returns pertaining to Operational Risk:

Sn	Name of Return	Periodicity
1.	BA300	15th day return
2.	BA325	Daily
3.	BA301	Monthly

Vice President (I.T & Systems)

He/ she has to ensure compliance with the following:

- IT & IT Security Policy
- Compliance Policy
- Human Resources Policy

In addition to complying with all the legislation listed in regulatory universe, the following also needs to be done:

1. Ensuring that the software used for Sanction Screening (CITRIX) is maintained and the sanctions lists are updated daily
2. Monitoring the checking of "hits" generated via CITRIX
3. Ensuring that BCP (Business Continuity Plan) and DR (Disaster Recovery) testing/ updating is done on a yearly basis.
4. Ensuring the DR testing of SAMOS accounts as per the guidelines issued by the South African Reserve Bank.
5. Maintaining the system used for Transaction Monitoring (AMLOCK).
6. Responsible to all other I.T. related and system issues

Vice President (Bilateral Credit)

He/ she has to ensure compliance with the following:

- Credit Policy
- Compliance Policy
- Human Resources Policy
- IT & IT Security Policy

In addition to complying with all the legislation listed in the regulatory universe, the following also needs to be done:

1. He/she needs to monitor the List Excess Report and the Status List
2. Ensure that the following is submitted to the Head Office (IBG) and the Reserve Bank of India:

- Non- performing assets (NPA) and Provision Report
- Advanced Under Collection Account (AUCA) Return
- New Business Data
- Country Risk Return
- NPA and AUCA Return
- Specialised Mentioned Account (SMA) Return
- Standard Assets Irregularity Return
- Overseas Operation Return to Reserve Bank of India
- Prudential Exposure

3. NCR Form 39 (Statistical Return) is also to be submitted as per the Regulatory Reporting Calendar, this is to the National Credit Regulator.

4. He/she is also responsible for the submission of the BA (Basel) returns on a monthly as well as quarterly and half yearly basis within time period stipulated by the South African Reserve Bank. He is responsible for the submission of the following returns pertaining to Credit Risk:

Sn	Name of Return	Periodicity
1.	BA200	20th day return
2.	BA210	20th day

Vice President (Trade)

He/ she has to ensure compliance with the following:

- Compliance Policy
- Human Resources Policy
- IT & IT Security Policy

In addition to complying with all the legislation listed in the regulatory universe, the following also needs to be done:

1. He/she needs to ensure that all requirements in terms of FICA and the bank's AML/CFT policy are met in respect of all trade related activities/customers.
2. Ensure that all documents relating to Documentary Credits conform to the latest version of Uniform Customs and Practice for Documentary Credits (UCPDC).
3. Needs to ensure that import transactions do not pertain to goods on the Prohibited and Restricted Goods list issued by the South African Revenue Service.

4. State Bank of India Privacy Practices

We collect personal or other information to:

- Meet our responsibilities to customers, employees and other natural or juristic persons;
- Follow client instructions;
- Inform our clients of new services; and
- Make sure our business suits our clients' needs.

Personal information may be received from or provided to:

- Any regulatory authority (like the SARB, FIC, FSCA, NCR) and the regulators they appoint for the various financial sectors
- Comply with any regulation passed under the relevant legislation; or any legal process
- Protect and defend SBI's rights and property
- Protect public interest
- Third party service providers in order to uphold contractual obligations or service customers.

Trans border information flows

SBI may share with or receive personal information from parties as set out above, where these parties reside outside of the Republic of South Africa. All operations are required to abide by SBI's policies, procedures and guidelines, regardless of legislative requirements for data protection in these countries.

Employee personal information may be received from or provided to:

- Pension / provident funds and/or their trustees
- Medical aid funds
- Recruitment companies
- Credit bureau

Our security practices

- We are committed and obliged to implement all reasonable controls to safeguard access to our clients' and employees' personal information.
- Where third parties are required to process your personal information in relation to the purpose set out in this manual and for other legal requirements, we ensure that they are contractually bound to apply appropriate security practices

5. SAFEGUARDING CLIENTS INFORMATION

- i. It is a requirement of POPI to adequately protect the personal information the bank holds and to avoid unauthorised access and use of the personal information. SBISA will continuously review its security controls and processes to ensure that its clients' personal information is secure. The following procedures are in place in order to protect clients' personal information:
 - a) The information officer is the Chief Executive Officer, whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI. He is assisted by the Chief Compliance Officer who will function as the Deputy Information Officer.
 - b) This policy is applicable throughout SBISA and training on this policy and the POPI Act takes place as and when required.
 - c) Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;
 - d) Every employee currently employed within SBISA will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;
 - e) SBISA must secure the integrity and confidentiality of the personal information it holds. To achieve this, SBISA must have in place relevant processes, procedures and systems to prevent loss of, damage to, or unauthorised destruction of personal information; and unlawful access to or processing of personal information. This includes applying the privacy impact assessment process.
 - f) SBISA'S archived client information is stored on site which is also governed by POPI;
 - g) SBISA'S third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the protection of personal information;
 - h) SBISA will introduce an electronic document management system whereby our hard copy files are to be captured electronically for back up purposes. All files will be archived at State Bank of India disaster recovery site which will be available both electronically and in hard copy form;
 - i) All electronic files or data are backed up by the systems department who is also responsible for system security which protects third party access and physical threats. Systems department are responsible for electronic information security;

- j) A security incident management register will be kept to log any security incidents and to report on and manage said incidents this register will be maintained by VP System.
 - k) Where personal information is considered (including where amnesty for removal has been granted by the National Credit Regulator) to be no longer needed for any purpose, SBISA must ensure this information is destroyed or permanently de-identified, if reasonable to do so. Exceptions to this include, but are not limited to, instances where the personal information is required by a particular record retention law, or required for some other lawful purpose.
 - l) Consent to process client information is obtained from clients (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory/on-boarding stage of the relationship.
- ii. SBISA must not transfer personal information about a data subject to a third party who is in a different jurisdiction unless:
- a) The third-party recipient is subject to similar laws as South African legislation with regards to the processing of personal information;
 - b) The data subject consents to the transfer;
 - c) The transfer is necessary to fulfil the performance of a contract between the data subject and SBISA; or
 - d) The transfer is for the benefit of the data subject however it was not reasonably practical to obtain the consent of the data subject at the time, but it is likely that the data subject would have given consent.

6. Categories of records

Information available on request

State Bank of India has under its control or in its possession the following categories of records under the subjects described below. The categories of records are not exhaustive and are subject to amendment from time to time. A request made for access to these records will not be automatically granted, but will be evaluated in accordance with the provisions of the Act, any other legal requirements and State Bank of India's policies.

Record category	Record category description
Accounting	<ul style="list-style-type: none"> • Formal books of account and financial statements • Source documents
Company secretarial	<ul style="list-style-type: none"> • Banking • Credit provision • Financial advisory and intermediary services • Forex Investment business

	<ul style="list-style-type: none"> • Long-term, Short-term Deposits
Client records	<ul style="list-style-type: none"> • Banking and deposit-taking (includes FICA) • Deceased clients • Insolvent clients • Securities services (General)
Human resources	<ul style="list-style-type: none"> • Statutory employee records • Other employee records
Health and safety	<ul style="list-style-type: none"> • Electrical installations • Construction administration and safety • Fire equipment • Elevators
National payment systems	<ul style="list-style-type: none"> • Records obtained by 'system participants' during the course of the operation and administration of the settlement system. • Records of payment instructions generated and/or obtained. • Records obtained during the course of operation and administration of a payment or Reserve Bank settlement system.

Records automatically available

The following categories of records are automatically available for inspection. This information does not need to be requested in terms of the Act.

These categories are:

- Any promotional material for public viewing
- Posters
- Campaigns
- Product information

Requests for this information may be made through the Information Officer.

Records available under any other legislation

Details of the records that are available under other legislation are attached to this manual as Annexure2.

7. Considerations before submitting a request

Before a formal request for access is submitted by a client or third party, the following need to be considered:

Is the requestor of the information submitting the request for the exercise or protection of his/her legitimate rights?

The exercise of your rights is subject to justifiable limitations, including the reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance. This legislation may not be used for access to a record for criminal or civil proceedings or requested after the commencement of such proceedings.

Is the information that is required in record form, and under the control of State Bank of India?

This Act only applies to records that have already been created, at the date of the request, and that are under the control of State Bank of India. State Bank of India is not obliged to retrieve any records on behalf a third party that are no longer under its control, even where State Bank of India created the record.

Does the requestor of the information have a legitimate right to access the record?

A request may only be made to exercise the requestor's own right. Or where the request is made on behalf of another person, the requestor must submit proof of his/her capacity to act on behalf of the person in whose name the request is made. For example, a power of attorney must be submitted with the request where a legal representative makes the request on behalf of his/her client.

8. Request procedure

If the requestor of the information is satisfied that he/she is entitled to make a request for access to records under this Act, the procedure outlined below must be followed:

Request form

No application will be considered unless it is completed on the request form in Annexure 1 to this manual. The completed form may be submitted to the Information Officer or the Deputy Information Officer by using the details described in clause 3 above.

It should be ensured that sufficient information is provided to enable us to establish:

- The record requested;
- The proof of identity of the requestor
- The form of access required, if the request is granted; and
- The contact details of the requestor

Definition of rights

A full description of the rights which the requestor of the information seeks to protect in line with the considerations outlined in clause 5.1 above must be provided.

Payment of the prescribed fees:

There are two types of fees:

- Request fee: R50
- Access fee: This is calculated by taking into account reproduction costs, search and preparation costs, as well as postal costs.

The requestor will be notified where the Information Officer requires a deposit (calculated from the access fee) and subsequent balance of the access fee. The information Officer will release the record on full payment. Where a deposit has been taken and the request has subsequently been refused, the Information Officer will refund the deposit to the requestor.

Deposits paid by a requestor will be refunded if the request is refused.

9. Timelines for consideration of the request

- Requests will be processed within 30 days, unless the request contains considerations that are of such a nature that an extension of the 30-day time limit is needed.
- Should an extension be needed, the person requesting the information will be notified, together with reasons explaining why the extension is necessary.

10. Grounds for refusal of access to records

The main grounds on which State Bank of India could refuse access to records (as per Chapter 4 {section 33-46} of the Promotion of Access to Information Act, 2 of 2000) relate to the mandatory protection of:

- a. the privacy of a third party who is a natural person;
- b. the commercial information of a third party;
- c. certain confidential information of a third party;
- d. the safety of individuals and safety of property;
- e. records privileged from production in legal proceedings;
- f. commercial information of State Bank of India, which may include without limitation –
 - i. trade secrets;
 - ii. financial, commercial, scientific or technical information; the disclosure of which could likely harm the financial or commercial interests of State Bank of India;
 - iii. information that, if disclosed, could put State Bank of India at a disadvantage in negotiations or commercial competition; and

- iv. computer programs and related information technology software that are owned by State Bank of India and that are protected by copyright; and
- v. research information compiled by State Bank of India or a third party, if disclosure would expose the third party, the researcher or the subject matter of the research to serious disadvantage.

g. Requests for access to records that are clearly frivolous or vexatious, or that involve an unreasonable diversion of resources, will be refused.

11. Remedies available to a requestor on refusal of access

State Bank of India does not have any internal appeal procedures that may be followed after a request to access information has been refused. The decision made by the Information Officer or deputy Information Officer is final. In the event that the requestor of the information is not satisfied with the outcome of his/her request, he/she is entitled to apply to Information Regulator or a court of competent jurisdiction to take the matter further.

Any complaints can be lodged with the Information Regulator on Form 5 (complaint form), in terms of Regulation 10 which can be found on the website of the Information Regulator under the “Forms” section.

Queries and complaints can also be directed to:

The Information Regulator (South Africa)	
Email:	enquiries@infoeregulator.org.za PAIAComplaints@infoeregulator.org.za
Telephone	+27 (0)10 023 5200
Physical address	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001.
Postal address	P.O Box 31533, Braamfontein, Johannesburg, 2017
Website:	https://www.infoeregulator.org.za/contact.html

Annexure 1:



REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

A. Particulars of private body

The Head: Personal Information Officer

B. Particulars of person requesting access to the record

The particulars of the person who requests access to the record must be given below.
The address and/email address in the Republic to which the information is to be sent must be given.
Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname:

Identity number:

Postal address:

Fax number:

Telephone number:

Email address:

The capacity in which a request is made when made on behalf of another person:

C. Particulars of person on whose behalf request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full names and surname:

Identity number:

D. Particulars of record

(a) Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.

(b) If the provided space is inadequate, please continue on a separate folio and attach it to this form.

The requestor must sign all the additional folios.

1. Description of record or relevant part of the record:

2. Reference number, if available:

3. Any further particulars of record:

E. Fees

(a) A request for access to a record, other than a record containing personal information about yourself, will be processed only after a **request fee** has been paid.

(b) You will be notified of the amount required to be paid as the request fee.

(c) The **fee payable for access** to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.

(d) If you qualify for exemption of the payment of any fee, please state the reason for exemption.

Reason for exemption of payment of fees:

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 hereunder, state your disability and indicate in which form the record is required.

Description of disability	
Form in which record is required	
Mark the appropriate box with an X	
Notes	
(a) Compliance with your request in the specified form may depend on the form in which the record is available.	
(b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.	
(c) The fees payable for access to the record, if any, will be determined partly by the form in which access is requested.	

1. If the record is in written or printed form:			
	Copy of record*		Inspection of record
2. If record consists of visual images (This includes photographs, slides, video recordings, computer-generated images, sketches, etc):			
	View of images		Copy of images*
			Transcription of the images
3. If record consists of recorded words or information that can be reproduced in sound:			
	Listen to the soundtrack (audio cassette)		Transcription of the soundtrack* (written or printed document)
4. If record is held on computer or in an electronic or machine-readable form:			
	Printed copy of record*		Printed copy of information derived from the record*
*If you are requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.			YES
			NO

G. Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

-
2. Explain why the record requested is required for the exercise or protection of the aforementioned right:
-

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved or denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decisions regarding your request for access to the record?

Signed at _____ on _____

Signature of requestor/person on whose behalf
request is made

Annexure 2:

LEGISLATIVE DISCLOSURE REQUIREMENTS

SECTION 51 (1) (d)

LEGISLATION	PROVISION	SECTOR/INDUSTRY/DATA SUBJECT	SUMMARY OF PROVISION	PERSONS RESPONSIBLE FOR DISCLOSURE
Administration of Estates Act 66 of 1965	Section 28(5)	Banking	Banks must keep information of a cheque account or savings account that has been opened by an executive in the name of the estate and all information relating to vouchers in relation to the cheque or savings account.	The Master or any surety of the executor have the same rights to this information
Compensation for Occupational Injuries and Diseases Act 130 of 1993	Section 1	Banking	An employer must register with the Commissioner and furnish the Commissioner with prescribed particulars of its business	Employer
	Section 18	Banking	Employer to register with Director General and to furnish him with particulars	Employer
	Section 32A	Banking	Any inspector furnished with inspection authority in writing by the Board may conduct an investigation to determine compliance with the Act.	Inspector or the manager
	Section 40	Banking	An employee or employer shall at the request of the Director General furnish such further particulars regarding the accident and injuries concerned as the Director	Director General

			General may require	
	Section 81	Banking	Employer must maintain a register or record of the earnings and prescribed particulars of all employees and shall produce such records on demand to an authorized person for inspection. Such records shall be maintained for a period of at least 4 years after the date of the last entry in that record.	Employer
	Section 82	Banking	Employer must furnish a return to the commissioner reflecting: amount of earning up to the maximum paid by him, and any further information as is necessary	Employer
Constitution of the Republic of SA Act 108 of 1996	Section 32	Banking	Everyone has the right to access any information held by another person and that is required for the exercise or protection of any rights.	Public
Inspection of Financials Institutions Act 18 of 1998	Section 4	Banking	In clearing out an inspection of the affairs of an institution under section 3 an inspector may, at any time without prior notice enter and search any premises occupied by the institution and require the production of any document relating to the affairs of that institution. Open any strong room, safe or other container in which he or she suspects any document of	Inspector

			<p>the institution is kept. Examine and make extracts from the copies of any document of the institution or against the issue of a receipt remove such document temporarily for that purposes. Against the issue of a receipt, seize any document of the institution which in his or her opinion may afford evidence of an offence or irregularity.</p>	
Unemployment Insurance Act 63 Of 2001	Section 56	Insurance / Bank	(1) Every employer must, as soon as it commences activities as an employer provide information regarding its employees to the commissioner.	Unemployment Insurance Commissioner