GOVERNANCE POLICY FOR DATA PRIVACY AND SECURITY

| | |
|---|---|
| ADOPTED | BY THE BOARD OF DIRECTORS |
| COMMENCEMENT | 28 MAY 2021 |
| VERSION LEGACY | V0.1/20210528 |
| LAST VERSION DATE | 28 MAY 2021 |
| INFORMATION OFFICER | ELAINE O GORMAN |
| APPLICATION | CONTRACTORS, MANAGEMENT EMPLOYEES, PERMANENT EMPLOYEES, SERVICE PROVIDERS, AND TEMPORARY EMPLOYEES |
| SUMMARY | ACCESS CONTROL.<br>BUSINESS CONTINUITY.<br>CHANGE MANAGEMENT.<br>COMPLIANCE WITH LAWS.<br>DATA AND INFORMATION PROTECTION.<br>INFORMATION TECHNOLOGY.<br>RECORD KEEPING.<br>REPORTING.<br>RISK AUDIT AND MANAGEMENT.<br>ROLES AND RESPONSIBILITIES.<br>SYSTEMS AND PROCESSES.<br>TELECONFERINCING: GOOGLE/SKYPE/TEAMS/ZOOM. |
| HEADLINE OBJECTIVES | TO CREATE ONGOING DAY-TO-DAY AND LONG-TERM ORGANISATIONAL AWARENESS, MINDFULNESS, AND SENSITIVITY RE PREVALENT DATA PRIVACY RISKS AFFECTING THE BUSINESS.<br>TO DESCRIBE THE GOVERNANCE ARRANGEMENTS, AWARENESS PROGRAMMES, FRAMEWORKS, POLICIES, PROCEDURES, AND STRATEGIES APPLICABLE TO ALL STAFF, TEMPORARY STAFF, AND CONTRACTORS TO THE FIRM, AS APPEAR FROM THE TABLE OF CONTENTS BELOW |

ramsaywebber

# GOVERNANCE POLICY FOR DATA PRIVACY AND SECURITY

## CONTENTS

## 1. CONTEXT

Why is there a need for data protection laws and policies?

- In a free trade and opportunity context: incorrect processing of personal information compromises equal opportunity and fair trade;
- In an international criminal context, the following criminal endeavours benefit from our non-adherence to protection requirements: identity theft, phishing scams, sex and slavery trades, theft,
- In a moral context: people are often required to make disclosure of information which may cause reputational harm and emotional distress if disclosed which exposes them to unfair and immoral abuse;
- In an organisational context: we must be responsible corporate citizens which means we must comply with laws, but we must also observe a moral and ethical duty to protect those whom we serve and those who serve us.
- In a prospective context: the rate of technological advancement means that personal information may be used in future for purposes which are not yet anticipated.

In the firm's course of supplying services clients are requested to hand over information which they would not ordinarily hand over, therefore they are owed a duty of care to safeguard any information the disclosure of which might expose hi/ or her to harm.

It is in this fundamental context that this policy is drafted: treat all information as confidential because often we are not aware of how it might be abused.

## 2. VERSION CONTROL

Considering the relative novelty of the legislative framework and the regulations' draft status, this policy document will undergo numerous changes as the strategies and objective are implemented. All version changes will be shown once in each preceding version by underlining inserted wording and striking deleted wording (changes to version 1 will be shown in version 2, but will not appear in version 3 for example, which will only emphasis changes to version 2).

## 3. TYPES OF PERSONAL DATA COLLECTED BY THE FIRM

- Data, evidence, information, or material.
- Concerning business partners, clients, customers, employees, members of the public and their children, directors, employees, and next of kin.
- Like their:
    - age;
    - assignment;
    - bank accounts;

- beliefs;
- birth;
- biometric information;
- credit card information;
- culture;
- colour;
- conscience;
- correspondence sent by him/her that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- criminal history;
- disability;
- driver's license details;
- education history;
- email address;
- employment history;
- ethnic or social origin;
- financial history and standing;
- gender;
- language;
- marital status;
- medical history;
- name;
- nationality;
- passport number;
- physical or mental health;
- physical address (location information);
- personal opinions, views or preferences;
- pregnancy;

- race;
- religion;
- sex;
- sexual orientation;
- telephone numbers;
- views or opinions of another individual about the person;
- well-being; and
- work address.

4. THE HOW

4.1. Consultations (whether in person or by electronic media) in the form of hand-written notes or recordings.

4.2. Copies of paper given by:

(a) Clients, relating to:

(i) Themselves.

(ii) Children.

(iii) Other adults and children.

(iv) Their shareholders/members (where client is a company/cc/club).

(b) Other people, relating to:

(i) Themselves.

(ii) Children.

(iii) Other adults and children.

(iv) Their shareholders/members (where client is a company/cc/club).

4.3. Emails received from clients and other people relating to those listed above.

4.4. External devices received from clients (like CD's, USB's, and hard-drives).

4.5. On-line access to folders (like DropBox and WeShare).

5. EXECUCTIVE SUMMARY

5.1. Before doing anything with data no matter how it is received ask yourself:

(a) What class does the information fall into (see classification Schedule 1).

(b) Who is the data subject? To whom does the information relate?

(c) How did I get the information?

(i) From the data subject.

(ii) From the data subject's authorised representative or guardian?

(iii) From the Deeds Office (Windeed/Searchworks) or the Court or the Master or the Companies and Intellectual Property Commission?

(iv) From another public record that is not subscribed for like the internet.

(v) From a client who is not the data subject and is not an authorised representative of the data subject?

(vi) From a member of the public who is not the data subject and is not an authorised representative of the data subject?

(vii) From an auditor or accountant serving a person (juristic or natural) related to the data subject (of which s/he is a shareholder or director).

(d) If it is CLASS 1, it **may not** be dealt with **at all** (it **may not** be printed, or saved, or sent, or shared, or typed into another document or device, or typed into a web-browser, or spoken aloud, or copied, or pasted, or written down) unless with the information officer's written permission. This information relates to children, bank account information, and information that if disclosed could cause physical harm to a person.

(e) If it is CLASS 2, it may not be it **may not** be dealt with **at all** (it **may not** be printed, or saved, or sent, or typed into another document or device, or typed into a web-browser, or spoken aloud, or copied, or pasted, or written down) unless with the data subject's express prior written consent detailing the specific processing activity contemplated.

(f) If it is CLASS 3, it may not be it **may not** be:

(i) sent, or shared with any person other than another authorised user (being a person who is working on the same matter for the same client who is the data subject) unless:

(aa) With the data subject's express prior written or verbal consent detailing the specific processing activity contemplated.

(aa) Then only to the extent necessary.

(ii) reproduced unless necessary.

(g) If it is CLASS 4, it may not be it **may not** be:

(i) sent, or shared with any person other than another authorised user (being a person who is working on the same matter for the same client who is the data subject) unless:

(aa) It is necessary to carry out the client's instructions (and the client is the data subject).

(aa) Then only to the extent necessary.

(ii) reproduced unless necessary.

5.2. You may generally only use the information for the purpose for which it was disclosed.

5.3. If you do share the information, you must be careful not to be selective in a way that undermines the data subject. You may not change any personal information supplied or represent it out of context.

## 6. ACCESS RESTRICTIONS

6.1. Objective: restrict access to personal information on a need-to-know basis.

6.2. Strategy:

(a) The information officer is mandated to engage with Custom-Cut, the firm's independent IT supplier to ensure that all access to electronic files is restricted to pre-defined users who require access and that all other users are denied access.

(b) A system will be implemented (by subsequent version):

(i) in which all files called from archives, outsourced to MetroFile, will be recorded; and

(ii) preventing files from being called from archives without the information officer's prior consent after s/he has verified the reason for the file being requested and the need for the person doing so to access the information likely to be retained therein.

6.3. Rules: files may only be accessed by authorised users who are authorised on the firm's practice management software.

## 7. BACKGROUND CHECKS

7.1. Objective: undertake a due diligence in relation to all persons employed by the firm who are not members of a recognised professional body.

7.2. Strategy: the information officer will ensure that criminal records, credit status, and qualifications verifications are obtained before the firm hires staff or contractors (whether permanent or temporary) who are not members of professional bodies which conduct these checks as preconditions to admission.

## 8. BACKUP AND RESTORATION PROCESSES

8.1. Objective: ensure that there are regular back-ups of systems and data.

8.2. Daily back-up processes will be done from the server to a hard-drive device which will be stored under lock and key in a location known only to the information officer and the managing director.

8.3. Strategy:

(a) The information officer is mandated to engage with Custom-Cut, the firm's independent IT supplier to ensure that all access to electronic files is restricted to pre-defined users.

(b) The security of the back-up should be verified by the board as soon as possible after the implementation of this policy version 1/20210521.

## 9. BUSINESS IMPACT ASSESSMENTS

9.1. Objective: conduct a BIA in conjunction with a business risk assessment to:

(a) identify which processes are business critical and the impact on the business should the processes become dysfunctional or available;

(b) deal with inabilities to perform business processes;

(c) identify how quickly the process must be made available to avoid duplicitous risk (particularly default risks under POPI and other applicable data privacy laws);

(d) determine what technology or planning is needed for functional recovery.

9.2. Strategy: the board, including the information officer, will carry out a high level BIA in conjunction with the IT services provider and international best practice and will develop an appropriate BIA for implementation.

## 10. BUSINESS CONTINUITY MANAGEMENT

10.1. Objective:

(a) Identify business continuity and privacy risks.

(b) Discover and then implement business recovery, crisis management, contingency planning disaster recovery, and emergency management incident management.

(c) Involve internal structures and external parties in planning, revision, and execution.

(d) Detail how prioritised activities will be resumed in predetermined timeframes.

(e) Ensure that BCP or DR tests and exercises are carried out in specific scenarios.

(f) Ensure that reports containing the outcomes of test or exercises are placed on file and disclosed to management and where necessary, audited or verified independently.

(g) Identify remedial actions to deal with failures or gaps highlighted in the test and exercises.

10.2. Strategy:

(a) Carry out a risk assessment of all the firm's departments in an all-inclusive way to identify potential risks.

(b) Update risk assessments on a quarterly basis in conjunction with paragraph 14 below.

(c) Develop plans to mitigate or eliminate the risks.

(d) Engage IT suppliers on capable separate hot, warm, standby, and/or data replication DR and BC facilities with business appropriate recovery times from point of invocation to recover mission critical activities.

(e) Ongoing BCM status monitoring.

10.3. The firm's management and the information officer do not possess the required internal competencies to conduct these activities, therefore budgets will be obtained for the exercise and a plan developed as soon as possible thereafter whether in a phased or outright basis.

## 11. COMPLAINTS

11.1. Objective: implement a formal process to deal with external complaints.

11.2. Strategy:

(a) All staff are required to forward all complaints concerning any of the items of this policy to the information officer.

(b) Once the information officer receives the compliant s/he will appoint a committee of 2 directors to investigate the complaint provided they are from internal departments other than those from which the complaint emanates or in relation to which it emanates.

(c) The complaints outcome will be investigated immediately, and a report presented to the information officer and the board.

(d) The board will publish the findings of the report subject to insurance restriction undertakings.

11.3. Rules: all complaints must be passed to the information officer for investigation as part of the reporting protocols below.

## 12. DATA GENERAL

12.1. Objective: ensure general data access, collection, disclosure, security, storage, and usage.

12.2. This general item is a catch-all process control for all aspects of the handling of personal information which is not covered under separate header.

12.3. Requirements:

(a) All information recorded must be correct, complete, reliable, and updated.

(b) Only information that is relevant to a matter or required to service clients and which the client consents to being recorded, may be collected, and recorded on the system.

(c) No information obtained and which is not recorded may be disclosed to anyone. This obligation is inherent in an attorney and client relationship; however, it is restated here to remove any doubt. All client information must be kept in the strictest of confidence even though there may be reason to suspect that it is not confidential, proprietary, or sensitive.

(d) Information concerning children may only be retained on a separate file under lock and key in the information officer's care before being deleted.

(e) No personal information of any kind may be disclosed other than with the department head's consent or the consent of a member of the board of directors.

(f) All client mandates must be updated to make it clear the way in which personal information will be collected and the purposes for which it will be used.

(g) Under no circumstances may any personal information be used other than to supply services to or at the client's request or direction. Information may not for example be used in any mailing lists.

(h) Each department will have separate access controls to information. In due course each need to know department member will have restricted access to information pertaining to clients in matter dealt with per department.

(i) All paper files drawn from archives must be done through reception, which will keep a record of all files drawn and the details of the person drawing the file.

(j) No files may be drawn from archives without client permission.

12.4. Strategy: external services providers will be engaged by the information officer on:

(a) Disaster recovery.

(b) Electronic user access control and restrictions.

(c) Change management subject to the procurement guideline below.

(d) Cloud storage risk assessments and jurisdictional protocols up to the standards applicable in local laws and internationally recognised best practice.

## 13. INFORMATION CLASSIFICATION SCHEME

13.1. Objective: ensure that information is classified as to risk, sensitivity, children, financial and banking, and ease of transmission and encryption so that restrictions and security levels are based on classification.

13.2. Strategy: as part of the risk assessment to be carried out with a focus on information technology and the handling of personal information, the board will develop a risk-based classification system for implementation.

## 14. DETECTION, RESPONSE, AND RECOVERY TO/FROM CYBER EVENTS

14.1. Objective: ensure that:

(a) Prevalent (in multiplicities of occurrence) cyber events are notified to the board by the information officer and via the IT service providers.

(b) Non-prevalent but high-risk cyber events are noted for monitoring and mention in the risk assessments.

(c) Implement appropriate recovery procedures in line with the BCM and BIA in consultation with the firm's IT providers.

(d) Include SIEM and CSIRT.

14.2. Strategy: the information officer will engage with the firm's IT service providers and report to the board with a view to seeking external specialised advice on prevalent cyber risks because the firm does not possess the required in-house competencies.

## 15. CHANGE MANAGEMENT PROCESSES

15.1. Objective: ensure that all changes to business systems and processes are managed in accordance with the risk assessments and the procurement policy so data privacy is secured.

15.2. Strategy: the information officer will prepare a list of service providers and the board will consider the firm's procurement policies and contractor terms of appointment.

## 16. CLEAN/CLEAR DESK POLICY

16.1. Objective: ensure that all records (represented physically) are stored under lock and key when they are not being accessed by authorised users.

16.2. Rules applicable to all staff:

(a) All documents recording personal information must be held in a file opened under the client name.

(b) All files must be replaced in the department's filing cabinets immediately after use, no files may be kept in staff offices after they have been worked on.

(c) All filing cabinets must be locked after hours and remain accessible under lock and key only by authorised users.

16.3. Strategy: management will investigate updated filing systems to increase security protocols in line with the BCM, BIA, and risk assessments.

## 17. CLOUD ENVIRONMENT

17.1. Objective: ensure that data storage locations are identified and applicable laws are met in jurisdiction.

17.2. Strategy: the information officer will consult with the firm's IT service providers and report to the board on storage locations and rack servers in cloud.

## 18. COMPLIANCE WITH LAWS AND REGULATIONS AFFECTING INFORMATION SECURITY

18.1. Objective: ensure that the firm complies with POPI.

18.2. Strategy:

(a) A training session and work-shop with all staff will be scheduled as soon as possible to discuss the applicable laws and their rationale.

(b) The work-shop will be used to inclusively gather information from all staff on their perceptions of data security processes and potential shortcomings for input within the risk planning objectives and strategies.

(c) Law practitioners are knowledgeable on POPI will assist all other unqualified (legally) staff.

(d) Regular updates to this policy will be sent to staff and contractors and all new staff and contractors (whether permanent or temporary/fixed-term will undergo induction training and pre-appointment checks and will be subject to heightened access restrictions for probationary periods and subject – like all staff – to appropriate need-to-know restrictions).

## 19. CONFIGURATION OF SYSTEMS AND NETWORKS

19.1. Objective: ensure that all the firm's systems and networks are configured in a consistent, accurate manner and application of approved good-practice security settings.

19.2. Strategy:

(a) The information officer will consult with the IT service providers and report to the board on their compliance with international best-practices.

(b) The firm's IT service providers will be required to give ongoing assurances on best practice adherences appropriate to the business and its risk planning and mitigation.

## 20. CONTRACTORS INCLUDING COUNSEL

20.1. Objective: obtain assurances and request compliance with the firm's policies.

20.2. Strategy:

(a) Update all terms and conditions to include assurances on privacy and information security responsibilities of contractors and subcontractors.

(b) Evaluation BCP or DR capabilities of suppliers and third parties on an ongoing basis.

(c) Postulate pre-appointment requirements for subcontractors and assessment of their compliance with this policy.

20.3. The firm's major service providers are advocates who are required by law to adhere to strict confidentiality, however, advocates should be required to give specific assurances.

20.4. Strategy: the board will formulate assurance notices to counsel for countersignature, taking account of risk strategies.

## 21. CONTROLS FOR ELECTRIC AND PHYSICAL DATA REPRESENTATIONS

21.1. Objective: control the way information is represented and stored.

21.2. Rules:

(a) Where data is obtained electronically it should be moved to a secure access restricted folder.

(b) All printed data must be held in file therefore subject to the information classification.

21.3. Strategy: controls will be updated in accordance with the risk analysis and classification guidelines to be adopted under this policy.

## 22. CONSEQUENCES FOR VIOLATING THIS POLICY

22.1. Objective: adopt clear policies on policy breaches.

22.2. Strategy: after adopting the risk policy and consulting with all staff by work-shop and then carrying out the necessary training, the board will develop and offense grading system which will be implemented in a phased approach while all staff practice new processes and controls.

22.3. Rules: unlawful disclosures of client and staff confidential information however remains an offense.

## 23. CRYPTOGRAPHIC SOLUTIONS

23.1. Objective: ensure that information under a separate highly sensitive classification of information under the information classification protocol is encrypted in accordance with international best practice.

23.2. Strategy:

(a) Complete the information classification protocol as soon as possible under paragraph 13.

(b) Develop a cryptographic representation system in consultation with experts.

23.3. Considerations:

(a) If possible, it is best not to share any information over electronic media (email, telephone, WhatsApp, short messaging, teleconferencing facilities).

(b) Be mindful that many of the electronic means of communication are not always secure, are often capable of being recorded, and are open to abuse.

(c) Where dealing with highly sensitive information and information of any kind concerning children, it is best not to use names but rather cryptic abbreviations when sharing the information.

## 24. CYBER RISK MANAGEMENT FRAMEWORK

24.1. Objective: develop a cyber risk management framework to identify and manage cyber threats and vulnerabilities and implement mitigating controls.

24.2. Strategy:

(a) The information officer will consult with the firm's IT services provider in conjunction with the consultations under the aforegoing paragraphs and as part of assessing cyber risks on an ongoing basis.

(b) Develop a cyber risk management framework in conjunction with the risk assessment and IT consulting outcomes.

## 25. DISASTER RECOVERY PLAN

25.1. Objective: develop a DRP that is supported by alternative processing facilities and tested regularly using simulations of the live environment.

25.2. Strategy:

(a) The information officer will consult with the firm's IT services provider in conjunction with the consultations under the aforegoing paragraphs and as part of assessing cyber risks on an ongoing basis.

(b) Develop a cyber risk management framework in conjunction with the risk assessment and IT consulting outcomes.

## 26. DISPOSAL OF EQUIPMENT AND INFORMATION

26.1. Objective: to implement rules for the disposal of electronic and physical data when it is no longer needed in accordance with the ISO 27001 standard.

26.2. Strategy: the board will consult with its service providers on the most secure means of disposal/destruction of information the ISO 27001 context.

26.3. Rules:

(a) All files containing personal financial information must be shredded before being disposed of.

(b) No electronic media devices like CD's, USB's, or Hard-drives may be disposed of, instead they must be handed to the information officer to be disposed of in consultation with the firm's service providers.

(c) All files called from archives which are older than 7 years and which do not contain original documents should be marked for destruction and handed to the information officer.

## 27. EMAIL AND INTERNET USAGE GUIDELINES

27.1. Objective: to define and implement guidelines to limit risk.

27.2. Rules:

(a) Staff may not access any websites other than strictly required to fulfil their work obligations.

(b) If any websites are accessed where there is a warning of any description, the staff member must immediately notify the information officer therefore so IT may be engaged on monitoring server access through external networks.

(c) All emails containing personal information should be printed and filed electronically and then deleted permanently from the system.

(d) Employees are urged to never open links on an email and if there are suspicious emails:

(i) They must be forwarded to the information officer before any attachments are opened, or before responding thereto; and

(ii) Their purported authors should be contacted to verify authenticity and purpose.

27.3. Strategy: implement additional guidelines to address any risks identified in formulating the business continuity, impact, and risk assessments.

28. EMPLOYEES AND RECORDS

28.1. Objective:

(a) Require all staff to undergo an initial and then regular privacy training course(s) supplied by a reputable expert service provider.

(b) Enforce an induction program for all new employees and temporary/fixed term staff in terms whereof this policy is summarised.

(c) Ensure that all temporary staff and service providers are subject to strict access restrictions.

(d) Ensure that all staff are subject to data access restrictions per department and that all staff within each department are subject to data restrictions per matter and data classification.

(e) Implement rules and guidelines for the storage and processing of employee information including personal information, medical history, employment contract terms and conditions, updates to deal with privacy and information security responsibilities of staff.

28.2. Rules:

(a) No person may be employed by the firm until a background check has been done which should include a criminal record check in cases where the person is not part of a professional body like the Law Society.

(b) On a bi-annual basis the firm will carry out a training session at a time convenient where the firm's IT service providers will give an address on the latest cyber and IT risks impacting the business.

28.3. Strategy: additional rules will be implemented in accordance with the business continuity, impact, and risk assessment.

29. ENCRYPTION

29.1. Objective: like paragraph 23, but with the addition of automated data encryption and rules for the transmission of personally identifiable information over the Internet.

29.2. Strategy: engage with the firm's IT suppliers and develop rules in accordance with the business continuity, impact, and risk assessments.

30. EXTERNAL AUDIT

30.1. Objective: ensure that there are regular back-ups of systems and data.

30.2. Strategy: engage with the firm's IT suppliers and develop rules in accordance with the business continuity, impact, and risk assessments.

31. FAILOVER CAPABILITIES

31.1. Objective:

(a) ensure that there are regular back-ups of systems and data.

(b) deal with utility and communication outages (for example water tanks, generators, backup data and voice links).

31.2. Strategy: engage with the firm's IT suppliers and other external advisors including the landlord, and develop rules in accordance with the business continuity, impact, and risk assessments.

## 32. HANDLING OF CLIENT/CUSTOMER INFORMATION

32.1. Objective: ensure that strict rules are placed and adhered to on the handling of client personal information.

32.2. Rules:

(a) all client information should be deemed to be personal information and treated in all respects (gathering, storage, sharing, deleting, disposal, uploading, keeping etc.) with the utmost confidence in the same manner as an employee would treat his/her own sensitive information.

(b) Refer to paragraphs 16 (clear desk), 21 (controls for data representations), 22 (cryptographic alternatives re highly sensitive data and data concerning children), 26 (data disposal/destruction), 27 (email and internet usage).

32.3. Strategy: Update the rules in line with the business continuity, impact, and risk assessment.

## 33. IDENTITY AND ACCESS MANAGEMENT

33.1. Objective: provide effective user administration, segregation of duties as well as identification, authentication, and authorisation mechanisms to ensure that access to information and systems is restricted to authorised individuals (including third parties).

33.2. Strategy:

(a) Consult with the firm's IT suppliers on access restrictions.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

## 34. INCIDENT REPORTING AND MANAGEMENT PROCESSES

34.1. Objective: develop rules pertaining to the reporting of data privacy incidents and their management.

34.2. Rules:

(a) the following incidents must be reported immediately to the information officer by email and telephone call and to the head of department:

(i) Accessing a suspicious website.

(ii) Opening a suspicious link or attachment.

(iii) Having any media containing personal data stolen or losing/being unable to immediately find any such media (in which case full details of the likely information and the owner's identity must be confirmed and all surrounding circumstances detailed: what, where, who, when, and how).

(iv) Experiencing any suspicious email activity (for example, someone emailing in response to an email which was never sent).

(b) once reported the information officer will consult with the IT service provider, the South African police services, the board, the relevant employee, and potentially the relevant information possessor (person to whom the data belongs) insofar as required to limit risk.

34.3. Strategy:

(a) Consult with the firm's IT suppliers.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

35. INDEPENDENT SECURITY AUDITS, USING A REPEATABLE AND CONSISTENT APPROACH

35.1. Objective: implement appropriate risk-based approaches.

35.2. Strategy:

(a) Consult with the firm's IT suppliers and potentially an independent security provider.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

36. INDUSTRY CODES OF CONDUCT

36.1. Objective: adhere to all industry codes.

36.2. Rules: all industry codes are incorporated herein by reference and will be expressly included by summary in training and subsequent versions.

37. INTERNAL AUDIT

37.1. Objective: ensure that there is an internal audit on data privacy risks.

37.2. Strategy: develop an internal audit process in line with the business continuity, impact, and risk assessment outcomes and international best practice.

38. LAPTOPS AND OTHER MOBILE DEVICES

38.1. Objective: identity, assess, and mitigate or eliminate data privacy risks associated with mobile devices (laptops, cell-phones, tablets, other hardware containing personal information).

38.2. Rules:

(a) All mobile devices must be password secured and accessible only by the user.

(b) Users may not share their passwords with anyone, nor may the firm's service providers share such information.

(c) When not in use laptops must be locked away and cell-phones should be kept out of reach

(d) While in transit laptops must be stowed in the car's boot.

(e) If a mobile devices is stolen or is accessed by any person other than the user or the firm's service providers under direction of the user, a report must be filed forthwith the information officer under paragraph 34.

38.3. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

39. **MALWARE PROTECTION AND HANDLING CAPABILITIES**

39.1. Objective: implement appropriate solutions including anti-virus software and behavioural analysis.

39.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

40. **NETWORK**

40.1. Objective:

(a) Ensure that there are regular back-ups of systems and data.

(b) Continuously monitor designated systems and networks and record security events including the identification of and response to information security/privacy incidents as well as recovery and post implementation reviews for current and predicted levels of traffic and alternative facilities support.

(c) Create a network diagram showing network entry points, firewalls, servers, switches, and routers.

40.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

41. **PRIVACY BY DESIGN**

41.1. Objective:

(a) Ensure that all stakeholders consider what personal information they capture, manage and store, and how best to secure the information. It makes common, logical sense that this information is sensitive, and should not be exposed, however it is best to treat all information as personal information and then treat that information as one would treat one's own personal confidential information.

(b) Consider privacy implications in all our processes and systems and build security and privacy concepts into the day-to-day operation of our organisations.

41.2. Strategy:

(a) Implementation of this policy.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

## 42. PROCESSING OF PERSONAL INFORMATION

42.1. Objective: develop rules aimed at ensuring that personal information and special personal information (each dealt with separately per classification generally and vis-à-vis each category of personal information) is:

(a) Properly classified to determine risk levels, encryption, access restriction, sharing restrictions, processing restrictions, breach reporting requirements, breach holder notification procedures, and any other enhanced processing rules/guidelines/systems/procedures.

(b) Only accessible and processed by authorised users in accordance with its proper classification and in accordance with this policy.

42.2. Rules:

(a) All information must be regarded as being highly confidential and personal information, even if it might not seem that way.

(b) No information may be processed (collected, stored, printed, uploaded, used, shared, converted, destroyed, or dealt with in any way) other than to serve the owner of that information per his/her/its instruction (tacit or express and considering aspects of guardianship and ostensible authority).

42.3. Strategy: develop additional rules in line with the business continuity, impact, and risk assessment outcomes.

## 43. PROCUREMENT

43.1. Objective: ensure that all hardware and software is obtained from reputable suppliers

43.2. Strategy: develop an approved list, subject to a security evaluation and recorded in an inventory.

43.3. Rules: no new service providers or correspondents may be appointed unless they have given the firm assurances that they will adhere to the firm's privacy policy herein.

## 44. PROHIBITIONS ON THE USE OF PORTABLE STORAGE MEDIA

44.1. Objective: prohibit the use of portable storage media like CDs, USB devices, or external hard drives) and allow the use of encrypted media only.

44.2. Rules: personal information may not be moved onto any portable storage media unless it is encrypted.

## 45. PROTECTION OF IT FACILITIES AND SERVICES

45.1. Objective: ensure that systems are protected against against damage, loss of power, natural hazards, and unauthorised physical access.

45.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

46. PROTECTION OF ELECTRONIC COMMUNICATION SYSTEMS

46.1. Objective: implement security protocols and measures to protect systems like e-mail, instant messaging, and VoIP and configuring security settings, performing capacity planning, and hardening supporting infrastructure.

46.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

47. PROTECTION OF INTERNAL NETWORK FROM EXTERNAL NETWORK

47.1. Objective: implement security protocols and measures to protect the systems from the internet for example by using firewalls.

47.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

48. RECORDS OF EVENT AND INCIDENTS

48.1. Objective: ensure that record is kept of all reported incidents.

48.2. Rules: a record of all events and incidents will be kept by the information officer in a centralised manner accessible only to directors and which will be reviewed monthly.

49. RECOVERY AND POST IMPLEMENTATION REVIEWS

49.1. Objective: ensure that there are regular back-ups of systems and data.

(a) Monitoring by and reporting to executive management of:

(i) Compliance requirements;

(ii) Current cyberthreats through threat intelligence and modelling to determine the organisation's vulnerability to such threats.

(iii) Information risks;

(iv) Security- and privacy-related incidents/breaches;

(v) Security condition of the organisation;

(b) Penetration tests and remediate vulnerabilities detected (IT and systems).

(c) Risk assessments for critical information infrastructure, sites, and systems using a structured methodology.

(d) Training programs.

49.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

## 50. REMOTE WORKING CONTROLS

50.1. Objective: ensure that information remains secure including guidelines for laptops and other portable computing devices when transported off-site.

50.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

50.3. Rules: refer to overlapping items at paragraphs 34 and 38.

## 51. RISK ASSESSMENTS

51.1. Objective: undertake risk assessments, prepare reports, and develop risk-based strategies to pass, mitigate, or eliminate risks and encourage ongoing and internal and sense of responsibility.

51.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

## 52. SECURITY BREACH RESPONSE PLAN

52.1. Objective: ensure that appropriate security breach response plans are developed and practiced.

52.2. Rules: as and when security breaches are notified to the information officer hereunder, an ad hoc meeting of the board will be convened with attendance of the IT service providers (if the information officers feels their attendance is prudent) and a response plan agreed and implemented under applicable corporate governance rules.

52.3. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes and international best practice.

53. SEGREGATION OF KEY NETWORK AREAS

53.1. Objective: consider the cost and benefits of network dematerialised zones, wireless and critical systems, and the segregation of areas/computer systems for access control purposes.

53.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

54. SYSTEM DEVELOPMENT METHODOLOGY

54.1. Objective:

(a) Develop systems methodologies that involve isolating development, testing and production environments, applying security throughout the development process and performing quality assurance.

(b) Continuous monitoring and assessment.

54.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

55. TELECOMMUNICATION CONTROLS

55.1. Objective: develop appropriate controls for all telecommunications in consultation with external service providers to ensure information remains secure.

55.2. Strategy:

(a) Consult with the firm's IT and VOIP suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

56. THIRD PARTY ASSURANCES

56.1. Objective: ensure that all third-party service providers, including advocates, will at all times adhere to POPI and applicable parts of this policy on the implementation of controls to protect data to which they have access.

56.2. Strategy: develop rules in line with the business continuity, impact, and risk assessment outcomes and due regard for the rules applicable beyond POPI in the attorney-client-advocate relationship.

57. VALIDATION OF INFORMATION

57.1. Objective: ensure that all data entered, processed by, and output from business applications and verification that it has not been subject to unauthorised change.

57.2. Strategy: develop rules in line with the business continuity, impact, and risk assessment outcomes.

58. **PHYSICAL SECURITY**

58.1. Objective: ensure that there are adequate physical security measures in place for all systems and media recording personal data.

58.2. Strategy: develop rules in line with the business continuity, impact, and risk assessment outcomes.

59. **COMPUTER AND NETWORK SECURITY**

59.1. Objective: ensure that appropriate risk-centric computer and network security is put in place.

59.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

60. **SECURE COMMUNICATIONS**

60.1. Objective: ensure that all communications are secure.

60.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes.

61. **SECURITY IN CONTRACTING OUT ACTIVITIES OR FUNCTIONS**

61.1. Objective: ensure that all contract outsourcing is subject to strict access control and security.

61.2. Strategy: develop rules in line with the business continuity, impact, and risk assessment outcomes.

61.3. Rules: adhere to the procurement guidelines, access restrictions, third-party assurances, induction programs, and training.

62. **RETENTION AND DISPOSAL OF INFORMATION**

62.1. Objective: develop rules for the retention and disposal of information.

62.2. Strategy: develop rules in line with the business continuity, impact, and risk assessment outcomes.

63. **MONITORING ACCESS AND USAGE OF PRIVATE INFORMATION**

63.1. Objective: determine appropriate monitoring functions.

63.2. Strategy:

(a) Consult with the firm's IT suppliers to develop additional rules.

(b) Develop rules in line with the business continuity, impact, and risk assessment outcomes while remaining sensitive to the privacy of staff in their own affairs whether evident in organisations systems and equipment or otherwise.

(c) Periodic analysis to inform ICMCI's management of the state of implementation of internal policies with impact on the processing of personal data;

(d) Internal audit;

(e) Monthly checks on the state of implementation of internal policies.

(f) Periodic analysis will include the following:

(i) Continuously adjusting Company internal policies and procedures so as to ensure a high degree of compliance with the requirements of the Regulation;

(ii) The results of the internal audit missions organized at ICMCI level;

(iii) Results of monthly checks on the state of implementation of internal policies;

(iv) Actions to be taken to promote improved implementation of internal policies.

(g) The internal audit will be organized as follows:

(i) it will be organized by people who have no responsibilities in the areas that are audited;

(ii) it will cover all policies and procedures with impact on Personal Data Processing activities implemented at Company level at least once a year;

(iii) include the corrective measures to be taken and the documentation to be drawn up to remedy the deficiencies noted in the implementation of internal policies to ensure continued compliance with the requirements of the Regulation at all times;

(iv) monitoring the findings of internal audit missions to verify that the proposed corrective actions are successful / generate the expected outcome.

(h) Monthly checks on the state of implementation of internal policies will include:

(i) Monitoring the implementation of policies and procedures;

(ii) Review the results of the audit missions already drawn up;

(iii) Monitoring the implementation of corrective measures;

(i) Preparing reports for ICMCI's management containing the results of the verifications undertaken.

(j) Monitoring the progress of internal policies implementation with impact on personal data processing activities at Company level requires internal audit reports to be conducted at least every 12 months or whenever necessary.

64. <u>INVESTIGATING SECURITY INCIDENTS</u>

64.1. Objective: ensure protocols for investigating security incidents.

64.2. Rules:

(a) The information officer will have discretion on how incidents relating to all information classes except class 1 will be investigated and will report to the board on the outcomes thereof.

(b) The board and the information officer will develop investigation protocols on an ongoing basis using each investigation as a template.

(c) Any incidents concerning information class 1 breaches will immediately be referred to the full board which will appoint an independent third party to investigate the incident without delay and report back to the board.

65. ROLES AND RESPONSIBILITIES

65.1. Objective: set out in this policy, by schedule or otherwise of a protocol/schematic representation of roles and responsibilities for managing data privacy and information security. Assigned ownership and responsibility for information and systems to designated individuals who have the required skills, tools, and authority. Information officer. Define role and responsibilities of a designated information officer and those of directors, top management, personnel dealing with personal information, vendors, contractors, suppliers.

65.2. Rules:

(a) As a professional body, all staff are required to assume full and unfettered responsibility for the safekeep and lawful processing of personal information and the firm will ensure that novel cyber or specialised cyber criminal risks are drawn to the firm's attention and policies, rules, and strategies are implemented herein.

(b) The firm's information officer will serve as the focal point for all data privacy compliance and risk and will be the custodian of this policy.

65.3. Strategy: develop rules in line with the business continuity, impact, and risk assessment outcomes and international best practice on internal checks and balances and officer background checks.

65.4. The information officer:

(a) The information officer will:

(i) Work with the firm's IT suppliers in carrying out his/her duties.

(ii) Follow-up on the compliance with the POPI.

(iii) Advise the board on POPI and data protection matters and be responsible for coordinating governance within the data governance filed together with individual business areas and support functions (see below).

(b) As part hereof, the information officer will ensure that personal data processing records are maintained, that agreement templates, group routines etc., are updated for use by the firm and that a central training program is available within the firm.

65.5. Contact Persons:

(a) A contact person must be appointed for each business unit and group support function.

(b) The contact person is the point of contact for the information officer and individuals in privacy matters relating to the individual business unit or support function.

(c) The contact person will report to the information officer on a regular basis (as further agreed between the information officer and the contact person) and must immediately notify the information officer of any processing activities in violation of POPI, local legislation or governing documents.

65.6. Compliance:

(a) The firm has a separate compliance function, which operates independently of the firm's other operations.

(b) The compliance function ensures compliance with applicable rules and regulations, including those within the privacy field.

65.7. Confidential internal audit:

(a) The firm will establish an internal audit function that is separate and independent from the firm's other activities.

(b) The internal audit function may perform audits within the privacy field as deemed appropriate from time to time.

## SCHEDULE 1 – INFORMATION CLASSIFICATION

| |
|---|
| Class 1 |
| • Bank account information.<br>• Children.<br>• Inside information in a public exchange. |
| Class 2 |
| All information that cannot be obtained from public record. |
| Class 3 |
| All information that cannot be obtained from public record by paying for it. |
| Class 4 |
| Information obtained from public record. |