QuanWay Insurance Brokers cc
Authorised Financial Service Provider
FSP 14751
Telephone 087 8022 635
Fax 086 5756 265
e-mail wayne@quanway.com
Website www.quanway.com

Data Breach and Security Incident Management Policy

Insurance Innovated Evolved

QuanWay Insurance Brokers cc

Authorised Financial Service Provider
FSP 14751
Telephone 087 8022 635
Fax 086 5756 265
e-mail wayne@quanway.com
Website www.quanway.com

V1

V1

1. DEFINITIONS

1.1. “**Breach**” means any data security breach whether the incident is confirmed or suspected;

1.2. “**Consultants**” means all third parties and service providers appointed by the Company who has access to and collects, holds, processes and shares data for or on behalf of the Company;

1.3. “**Company**” means Quanway Insurance Brokers

1.4. “**Data**” means all private data, confidential data and secret/restricted data;

1.5. “**Data subject**” means the person to whom personal information relates;

1.6. “**Employees**” means all permanent and fixed term employees of the Company;

1.7. “**Incident**” means any event or action which may compromise the confidentiality, integrity or availability of the Company’s systems or data, which caused or has the potential to cause loss or damage to the Company. An incident includes but is not limited to:

1.7.1. theft or loss of Personal data;

1.7.2. theft or loss of equipment which contains Company data, irrespective of whether the equipment is owned by the Company. For the purpose of this clause 1.4, equipment means any physical object that contains or stores data and/or personal information which includes but is not limited to Laptops, USB’s, iPads, Tablets, Cell phones and paper records.

1.7.3. failure of Company systems and/or equipment;

1.7.4. unauthorised use of, access to or modification of Company data or systems;

1.7.5. unauthorised disclosure of personal information; and

1.7.6. unauthorised access or attempted unauthorised access to Company systems and/or personal information.

1.8. "**Personal Information**" and "**Personal Data**" as defined in "POPI" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

1.8.1 information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

1.8.2 information relating to the education or the medical, financial, criminal, or employment history of the person;

1.8.3 any identifying number, symbol, e-mail address, physical address, telephone number location information, online identifier or other particular assignment to the person,

1.8.4 the biometric information of the person;

1.8.5 the personal opinions, views or preferences of the person;

1.8.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence;

1.8.7 the views or opinions of another individual about the person; and

1.8.8 the name of the person if it appears with other personal information relating to the person, or the disclosure of the name itself would reveal information about the person.

1.9. "**POPI**" means the Protection of Personal Information Act, 4 of 2013; and

1.10. "**Regulato**r" means the Information Regulator established in terms of section 39 of POPI.

2. PURPOSE AND SCOPE

2.1. The Company collects, holds, processes, and shares data (which includes personal information), and the purpose of this policy is to:

2.1.1. protect the Company's data; and

2.1.2. ensure that a consistent and effective approach is in place to identify, contain and manage information, security incidents and data security breaches in all areas of the Company's business

2.2. This policy applies to all:

2.2.1. business processes;

2.2.2. data and information systems and components; and

2.2.3. employees and consultants appointed by the Company.

3. DATA DISCLOSURE

3.1. The Company's data is comprised of the following information:

3.1.1. Private data:

Private data is defined as corporate information that is required to be kept within the Company. Private data cannot be distributed outside of the workplace and includes but Is not limited to work phone directories, organisational charts and company policies.

The disclosure of private data by staff to any individual that is not employed or appointed by the Company is prohibited.

All information not otherwise classified will be assumed to be Private data.

3.1.2. Confidential data:

Confidential data is defined as personal or corporate information that may be considered potentially damaging if released, and is only accessible to specific groups (e.g. payroll, HR, etc.).

Confidential data includes, but is not limited to, Identity Numbers, contact information, tax forms and accounting data. The Company prioritises the protection of personal information. Employees may only share confidential data within the authorised scope of their employment and in accordance with POPI.

3.1.3. Secret/Restricted data:

Secret/Restricted data is defined as sensitive data which, if disclosed without authorisation, would be harmful to the Company, its employees and/or consultants.

Access to Secret/Restricted data is limited to authorised personnel and third parties as required. Secret/restricted data includes, but is not limited to audit reports, legal documentation and business strategy details. Employees can only disclose Secret/restricted data within the authorised scope of their employment.

3.2. The Company will collect relevant personal information in order to:

3.2.1. provide the services required by the Company's clients;

3.2.2. amend its services and develop new services in line with requirements of the Company's clients;

3.2.3. meet its reporting and other legal obligations in terms of legislation and any regulatory requirement to which the Company is subject.

3.3. Information obtained from clients will be treated as confidential, and will be stored securely. Access to the information will be restricted to authorised staff only, and it will not be disclosed to persons outside of the Company without the express consent of the client, unless the Company is obliged by law to make the disclosure. Information will not be used for marketing purposes without the client's prior consent or where there is a legitimate common purpose.

3.4. Information will only be kept for the period required by law, and the Company's financial and other reporting requirements.

3.5. The Company is required to disclose information held in respect of clients under the following circumstances:

3.5.1. when required by law or a court order;

3.5.2. when disclosure is in the public interest;

3.5.5. when disclosure is necessary to protect the Company's rights or interests; or

3.5.4. where disclosure is done for a legitimate purpose.

4. REPORTING

4.1. The responsibility to report any data breach or information security incident, whether confirmed or suspected, vests with the employees, consultants and any other individual who accesses, uses or manages the data of the Company.

4.2. Data breaches and/or information security incidents needs to be reported immediately to:

Chief Operations Officer:
Wayne Duval

and

Group Legal and Risk Officer:
Kush Pillay

5. CONTAINMENT AND RECOVERY

5.1. Any data breach or information security incident reported will be investigated by the Chief Operations Officer and Group Legal and Risk Officer who will:

5.1.1. contain the breach;

5.1.2 assess the potential adverse consequences;

5.1.3. limit the scope and impact of the breach; and

5.1.4. determine a suitable cause of action to ensure a resolution to the incident.

5.2. Should any personal information be disclosed without authorisation, whether or not the disclosure was intentional, the following process will be followed:

5.2.1. the recipient will be advised that the information cannot be distributed or discussed with anyone else, and the implications of the failure to do so will be explained to the recipient;

5.2.2. the recipient will be advised to destroy or delete the information, and written confirmation will be requested as confirmation that the information has been destroyed or deleted as required; and

5.2.3. where required, the data subject(s) will be informed of the unauthorised disclosure in order to take any steps available to protect themselves.

6. RISK ASSESSMENT

6.1. The Chief Operations Officer and Group Legal and Risk Officer will immediately, alternatively as soon as may be reasonably possible, investigate any breach or incident reported and assess the risk associated with it taking into account:

6.1.1. the type of data involved;

6.1.2 the data's sensitivity;

6.1.3. the data protection currently utilised, such as encryptions;

6.1.4. what happened to the data, whether it was lost, stolen or damaged;

6.1.5. whether the data can be utilised for illegal means;

6.1.6. the data subject(s) affected by the incident or breach, the number of individuals involved and the potential effects on the data subject(s);

6.1.7. the wider consequence of the breach, if any; and

6.1.8. manner in which losses can be recovered and the damage caused limited.

7. NOTIFICATION

7.1. The Chief Operations Officer, or the employee nominated by the Chief Operations Officer is responsible for all notifications required in terms of this policy, which

includes any notification to the Regulator, as required in terms of POPI, data subject(s) and/or third parties.

7.2 In the event that the severity of the breach or incident requires notification to the data subject(s), the data subject(s) will be informed as soon as may be reasonably possible in order to mitigate any damage or possible damage that may occur to the data subject(s). Notifications to data subjects will include:

7.2.1. a description of the breach or incident;

7.2.2. the manner in which the breach or incident occurred;

7.2.3 when the breach occurred;

7.2.4 the data involved in the breach or incident;

7.2.5 recommendation on how to mitigate any further damage or loss;

7.2.6 the action taken by the Company to mitigate the risks; and

7.2.7 the contact information of the Information Officer.

7.3 The Company will maintain a record of all data breaches and information security incidents, regardless of whether any further notification was required.

8. EVALUATION AND RESPONSE

8.1. Upon containment of any breach or incident, the Chief Operations Officer will review the causes of the breach, the effectiveness of the response(s) and whether any system changes or policy or procedures amendments should be implemented.

8.2. The existing controls will be reviewed to determine adequacy and corrective action will be implemented to minimise the risk of similar incidents.

8.3. The review will consider:

8.3.1. the manner in which personal data is collected and stored;

8.3.2. the potential risks existing within existing security measures;

8.3.3. the security of transmissions; and

8.3.4. staff awareness;

9. COMPLIANCE

9.1. Ownership of this policy falls to the Executive Committee and Information Officer within the Company.

9.2. In accordance with POPI, the requirements as set out in section 55 will be attended to by the Information Officer:

Information Officer
Chief Operations Officer
Name of IO
Email address of IO

9.3. Violations of this policy and allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

9.3.1. disciplinary action;

9.3.2. termination of employment; and

9.3.3. legal action according to applicable laws and contractual agreements.

10. POLICY REVIEW

This policy will be reviewed on an annual basis.

V