PERSONAL INFORMATION PROTECTION POLICY

AND

PROCEDURE MANUAL

TABLE OF CONTENTS

1. CONFIGURATION CONTROL

1.1 Policy Owner:	Lisanne Pienaar-De Gouveia (Deputy Information Officer)
1.2 Policy Approver:	Charles Pittaway (Information Officer)
1.3 Version:	1.1
1.4 Scope of Application:	Netcash Colleagues
1.5 Effective Date	1 June 2021
1.6 Review Cycle	365 days

2. VERSION CONTROL

Version	Author of Change	Date	Details of Change
1.0	Patrick Warne	1 June 2021	Policy Creation
1.1	Lisanne Pienaar-De Gouveia	1 January 2023	Revision and updates.

3. DEFINITIONS

3.1 **"The Company"** means Netcash (Pty) Ltd, which is a private company registered in terms of the laws of South Africa.

3.2 **"Colleague"** means a person, other than an independent contractor, who performs work or assists in conducting the business of the Company under a contract of employment with the Company, whether oral or written, express or implied, fixed, or permanent.

3.3 **"Data Subject"** means the person to whom personal information relates. It includes both an identifiable, living, natural person as well as an identifiable, existing, juristic person, therefore the Company and its stakeholders, namely: its Clients, Employees; Suppliers and any other third party that it does business with.

3.4 **"Information Officer"** means the Managing Director of the Company as contemplated in Section 1 of the Promotion of Access to Information Act.

3.5 **"Responsible Party"** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

3.6 **"Operator"** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

3.7 **"Personal Information ("PI") of an identifiable, living, natural person"**, means information including, but not limited to:

3.7.1 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;
3.7.2 information relating to the education or the medical, financial, criminal or employment history of the person;
3.7.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
3.7.4 the biometric information of the person;
3.7.5 the personal opinions, views or preferences of the person;

3.7.6 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;
3.7.7 the views or opinions of another individual about the person; and
3.7.8 the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

3.8 **"Personal Information in relation to an identifiable, existing juristic person (e.g., a company, trust, close corporation, state owned company, etc.)"** means, information including, but not limited to:

3.8.1 information relating to the ownership (Broad-Based Black Economic Empowerment credentials, amongst others) and age (year of registration) of the juristic person;
3.8.2 information relating to the financial (e.g., financial statements, how much a responsible party has paid a juristic person per financial year for services / products, amongst others) or criminal history of the juristic person;
3.8.3 any identifying number (e.g., registration number), symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the juristic person;
3.8.4 the personal opinions, views or preferences of the juristic person;
3.8.5 correspondence sent by the juristic person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
3.8.6 the views or opinions of another individual about the juristic person; and
3.8.7 the name of the juristic person if it appears with other personal information relating to the juristic person or if the disclosure of the name itself would reveal information about the juristic person."

3.9 **"Processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

3.9.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
3.9.2 dissemination by means of transmission, distribution or making available in any other form; or
3.9.3 merging, linking, as well as restriction, degradation, erasure or destruction of information;

3.10 All terminology not defined in this policy shall bear the same meaning as in the applicable legislation.

4. EXECUTIVE SUMMARY

4.1 Netcash is a registered Third-Party Payment Provider and Processor ("TPPP") and System Operator ("SO") that provides a variety of financial, risk solution and e-Commerce services on its technology platform, to its clients. Its flexible collection and payments services, includes but are not limited to debit order collection, billing, e-commerce check out options, secure-link payment options, salary payments, creditor payments, retail payments, wallet, and banking application contactless payments, amongst others.

4.2 The Company recognises its accountability to all its stakeholders and is committed to complying with the statutory, regulatory, and supervisory requirements (collectively known as "regulatory requirements"), applicable to its business, to act with due skill, care, and diligence and to uphold the highest standards of integrity and fair dealing in the conduct of its business.

4.3 Considering its strategic objectives, one of which is Good Governance and Sustainable Business Practices, the Company articulates and gives effect to its direction on governance to its colleagues through training, awareness and its library of governance policies and procedures.

4.4 The POPIA requires that organisations act responsibly when using data subjects' personal information. This policy outlines the Company's intent with regards to the implementation and maintenance of its ongoing Personal Information Protection efforts in line with the requirements of the Act. The Act states that Personal Information must be protected, it must remain up to date and valid and that Data Subjects must be able to access their personal information.

4.5 The Company has a zero tolerance for non-compliance with Data Privacy laws and regulatory requirements and prepared this policy to guide its colleagues to promote the protection of personal information and data privacy standards expected of the Company as a registered financial services provider.

5. PURPOSE

The purpose of this policy is to:

5.1 provide clear guidelines to all colleagues in response to the possible negative consequences associated with non-compliance with Data Privacy regulatory requirements, that could potentially impact the Company's reputation and increase the likelihood of regulatory scrutiny; and

5.2 ensure that colleagues understand their responsibilities for maintaining compliance with the applicable Data Privacy laws by implementing adequate and effective control measures to combat the threat of data loss and/or PI breaches through its people, systems, and processes, when dealing with Company PI and the processing of Data Subject PI.

6. APPLICABILITY

6.1 This policy shall apply to all permanent and fixed term contract appointments made within the Company.

7. DATA PRIVACY LEGAL FRAMEWORK (which incorporates amendments made from time to time)

7.1 The Constitution of the Republic of South Africa, 1996;

7.2 The Protection of Personal Information Act No. 4 of 2013 ("POPIA" or the "Act");

7.3 The Promotion of Access to Information Act No. 2 of 2000 ("PAIA");

7.4 The Electronic Communications and Transactions Act No. 25 of 2002; and

7.5 The Financial Sector Regulation Act No. 9 of 2017, as it relates to the protection of PI.

8. SCOPE AND APPLICATION

This policy applies to:

8.1 the personal information of all relevant Data Subjects with whom the Company interacts;

8.2 all types of and uses for personal information within the Company;

8.3 all Colleagues and Company partners that deal with personal information;

8.4 all Company methods, frameworks, controls and systems (both manual and digital, internal and external) that process personal information; and

8.5 all our data processing locations.

9. PROCESSING OF PERSONAL INFORMATION AND ADHERENCE TO POLICY

9.1 Processing of personal information refers to the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, including inaccessibility, erasure, or destruction of personal information.

9.2 The Company and its Colleagues shall:

- 9.2.1 collect and process personal information which is relevant to the operational needs of the Company, and not excessive;
- 9.2.2 regard personal information as strictly private and confidential and not disclose it to any other party, unless required by law or with the consent of the Data Subject;
- 9.2.3 together with its Data Subjects, keep their personal information protected and up to date;
- 9.2.4 not keep personal information in the hope that it may become useful later on;
- 9.2.5 only grant access to the data to people who requires access to it in order to perform their duties and functions;
- 9.2.6 protect the data from accidental loss or theft;
- 9.2.7 where required, always seek the Data Subject's consent;
- 9.2.8 where required, always seek the consent of a competent person in respect of a child;
- 9.2.9 only process sensitive personal information where the Company is legally able or required to do so;
- 9.2.10 when communicating with our Data Subjects, always be open and transparent, using language that is easily understandable;
- 9.2.11 be aware of possible Data Subjects requests to access and manage their personal information and how to respond to such requests;
- 9.2.12 be aware of possible compromises in the security of personal information and how to respond to such security compromises;
- 9.2.13 be aware of and respond timeously to any training and awareness programs, communications or standard operating procedures within our Company;

9.3 The Company takes responsibility to keep on record all the appropriate documentation of all processing operations.

10. RESPONSIBILITIES OF INFORMATION OFFICER

10.1 The responsibility of the Information Officer or Deputy Information Officer shall be to, in consultation with the relevant Information Owners to drive POPIA compliance within the Company by:

10.1.1 developing a compliance framework that defines standard operating procedures / practices relevant to the processing of personal information;
10.1.2 conducting the relevant impact / risk assessments;
10.1.3 ensuring that relevant processing frameworks / manuals are in place;
10.1.4 enabling Data Subject participation;
10.1.5 co-ordinating the necessary awareness training;
10.1.6 dealing with requests made by Data Subjects, channelling to the proper Information Owner;
10.1.7 working with the Regulator in relation to investigations, where applicable.

11. CONDITIONS FOR LAWFUL PROCESSING

11.1 The 8 (eight) conditions that shall apply, relevant for the lawful processing of personal information, shall be:

11.1.1 Accountability;
11.1.2 Processing limitation;
11.1.3 Purpose specification;
11.1.4 Further processing limitation;
11.1.5 Information quality;
11.1.6 Transparency (honesty and integrity);
11.1.7 Security safeguards; and,
11.1.8 Data Subject participation.

12. ADDITIONAL PROCESSING PROCEDURES REGARDING PERSONAL INFORMATION

12.1 The Company shall ensure that any further processing of personal information shall be in accordance or compatible with the purpose for which it was collected in terms of section 13 of the POPIA.

12.2 To assess whether further processing is compatible with the purpose of collection, the company shall take account:

12.2.1 the relationship between the purpose of the intended additional processing and the purpose or intention for which the information was collected;
12.2.2 the nature of the information concerned;
12.2.3 the consequences of this action for the Data Subject regarding the intention of processing additional information;
12.2.4 the manner / method in which this information was collected; and
12.2.5 any contractual rights and obligations between the parties.

13. RETENTION AND RESTRICTION OF RECORDS

13.1 The POPIA requires that records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

13.1.1 retention of the record is required or authorised by law;
13.1.2 the Responsible Party reasonably requires the record for lawful purposes related to its functions or activities;
13.1.3 retention of the record is required by a contract between the parties thereto; or
13.1.4 the Data Subject or a competent person where the Data Subject is a child has consented to the retention of the record.

13.2 Records of personal information may be retained for periods in excess of those contemplated above for historical, statistical or research purposes, and in such an event, the Company shall ensure that the appropriate safeguards are established.

13.3 The Company undertakes to, where personal information of a Data Subject is used to make a decision about the Data Subject:

13.3.1 retain the record for such period as may be required or prescribed by law or a code of conduct; or
13.3.2 if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the Data Subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

13.4 The Company shall destroy or delete or de-identify a record of personal information as soon as reasonably practicable after the Company is no longer authorised to retain the record.

13.5 The deletion of a record of personal information should be processed in a manner that prevents its reconstruction in an intelligible / understandable form.

13.6 The Company shall restrict the processing of personal information if:

13.6.1 its accuracy is contested by the Data Subject, for a period enabling the Company to verify the accuracy of the information;
13.6.2 the Company no longer requires the personal information for achieving the purpose for which it was collected or subsequently processed, but is required to maintain / retain it for purposes of proof or record keeping purposes;
13.6.3 the processing is unlawful, and the Data Subject opposes its destruction or deletion and alternatively requests the restriction of its use; or
13.6.4 the Data Subject requests that the personal data be transmitted or transferred to another automated processing system.

13.7 Personal information that has been restricted may only be processed for purposes of proof, or processed with the Data Subject's consent, or with the consent of a competent person where the Data Subject is a minor, or for the protection of the rights of any other natural or legal person, or if such processing is in the public interest.

13.8 Where personal information is restricted, the Company will inform the Data Subject prior to the termination of the restriction.

14. SECURITY SAFEGUARDS

14.1 The Company will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of personal information; and unlawful access to or processing of personal information.

14.2 The Company will take reasonable measures to:

14.2.1 identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
14.2.2 establish and maintain appropriate safeguards against the risks identified;
14.2.3 regularly verify that the safeguards are effectively implemented; and
14.2.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

14.3 The Company will have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

15. SECURITY COMPROMISES

15.1 Where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person, the Deputy Information Officer should be contacted immediately.

15.2 The Information Officer or Deputy Information Officer is required to notify the Information Regulator and the Data Subject.

15.3 The notification of a breach of confidentiality should be declared as soon as is reasonably possible upon the discovery of the compromise, by completing Form SCN1 – Security Compromise Notification, which is an annexure to this policy.

15.4 The Deputy Information Officer needs to provide sufficient information to the Data Subject which will enable the Data Subject to take protective measures against the potential consequences of the compromise.

16. RIGHTS OF DATA SUBJECTS

16.1 A data subject has the right to have his, her or its personal information processed in accordance with the stipulated conditions for the lawful processing of personal information including the right to:

16.1.1 be notified that personal information about him, her or it is being collected or his, her or its personal information has been accessed or acquired by an unauthorised person;

16.1.2 establish whether the Company holds personal information of that Data Subject and to request access to his, her or its personal information;
16.1.3 request, where necessary, the correction, destruction or deletion of his, her or its personal information;
16.1.4 object on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information;
16.1.5 object to the processing of his, her or its personal information at any time for purposes of direct marketing in terms of section 11 of the Act.
16.1.6 not have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications;
16.1.7 not be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person.
16.1.8 submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator; and
16.1.9 institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

17. ACCESS TO PERSONAL INFORMATION

17.1 A data subject, having provided adequate proof of identity, has the right to:

17.1.1 Request, free of charge, whether the Company holds personal information about the data subject; and

17.1.2 Request from the Company the record or a description of the personal information about the data subject, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information:

17.1.2.1 within a reasonable time;
17.1.2.2 at a prescribed fee, if any;
17.1.2.3 in a reasonable manner and format; and
17.1.2.4 in a form that is generally understandable.

17.2 If personal information is communicated to a data subject, the data subject must be advised of their right to request the correction of their information.

17.3 The Company may or will refuse to disclose any information requested to which the grounds for refusal of access to records applies.

18. MONITORING AND EXECUTION

18.1 All Colleagues within the Company shall be responsible for ensuring the effective administration and implementation of this policy where the processing of personal information is concerned, including the adopting of:

18.1.1 principles and guidelines;
18.1.2 frameworks;
18.1.3 standard operating procedures;
18.1.4 notifications / consents, and
18.1.5 associated documents and practices.

18.2 Colleagues who contravene the terms of this policy may be subjected to disciplinary action, in accordance with the Company Disciplinary Policy.

18.3 Inquiries relating to the processing of personal information shall be required to be directed to the Deputy Information Officer, who shall then (if required) collaborate or consult with the relevant Information Owners concerning the inquiry or query.

18.4 The Company will ensure that the Information Officer, Deputy Information Officer/s and Information Owners/Data Subjects receive the relevant training regarding the execution of their functions and obligations, in terms of the provisions of the POPIA and the PAIA.

FORM SCN1

NOTIFICATION OF A SECURITY COMPROMISE IN TERMS OF SECTION 22 OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

Note:

1. *Attach documents in support of the notification.*
2. *Complete the form in full as applicable.*
3. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*

A	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and Surname / Registered name of responsible party	Netcash (Pty) Ltd
Address:	Netcash Square,
	64 Parklands Main Road
	Parklands Code (7441)
Contact Number(s):	0861 338 338
E-mail Address:	Legal@netcash.co.za
B	**DETAILS OF THE INFORMATION OFFICER**
Full names of information officer	**Charles Pittaway**
Registration number of information officer	
Contact Number(s)	**0861 338 338**
E-mail address:	
C	**DETAILS OF SECURITY COMPROMISE**
Date of Incident:	
Date incident reported to Information Regulator	
Explanation for delay in notification to the Regulator, if applicable	
Kindly tick applicable box √	

NOTIFICATION OF SECURITY COMPROMISE

Type of Security Compromise	Loss of personal information		
	Damage to personal information		
	Unauthorised destruction of personal information		
	Unlawful access to personal information		
	Unlawful processing of personal information		
	Other		
	If other, please explain_____		
Description of Incident			
Kindly tick applicable box √			
Type of personal information compromised	**Personal information of children**		**Unique identifiers**
	Special personal information		**Other**
	If other, please explain_____		
Number of data subjects affected			

Method of notification to data subjects	**Mail to the data subject's last known physical or postal address**			
	Sent by e-mail to the data subject's last known e-mail address			
	Placed in a prominent position on the website of the responsible party			
	Published in the news media			
Does the notification provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:	**A description of the possible consequences of the security compromise**			
	A description of the measures that the responsible party intends to take or has taken to address the security compromise			
	A recommendation with regards to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise			
	If known, the identity of the unauthorised person who may have accessed or acquired the personal information			
Status of the compromise	**Confirmed:**		**Alleged:**	
D	**Description of the measures that the responsible party intends to take or has taken to address the security compromise and to protect the personal information of the data subjects from further unauthorised access or use.**			
E	**DECLARATION**			
I declare the information contained herein is true, correct, and accurate. SIGNED at_____ on this the _____day of _____20__				
_____ Signature				
Name: Charles Pittaway	Designation: Information Officer and Managing Director			