COMPRSA
Web-based Business Solutions

Registration Number
CK2000/064940/23
VAT Number
4840196317

1 Leadwood Crescent, Fairview
Port Elizabeth, South Africa
www.comprsa.com
johan@comprsa.com
+27 83 338 6418 (m)
+27 41 368 2299 (o)

Business Continuity Plan (BCP)

Emergency Contact Persons

Our company's emergency contact persons are:

- Johan Swart, 27833386418, johan@comprsa.com
- Dewald Steenkamp, 27724313689, dewald@comprsa.com
- Jahn Roux, 27825537452, jahn@comprsa.com
- Nico de Jongh, 27718873000, nico@comprsa.com

These names will be updated in the event of a material change, and our Executive Representative will review them within 17 business days of the end of each quarter.

I. Company Policy

Our company's policy is to respond to a business disruption by safeguarding employees' lives and company property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the company's intellectual property and in the event that we determine we are unable to continue our business, we will assure customers prompt action in the shortest possible time.

A. Business Disruptions

Our plan anticipates two kinds of business disruptions, internal and external. Internal business disruptions affect only our company's ability to communicate and do business, such as a fire in our building. External business disruptions prevent the operation of the developers to execute their daily tasks for our clients. Our response to an external business disruption relies more heavily on other organizations and systems.

B. Approval and Execution Authority

Johan Swart is responsible for approving the plan and for conducting the required annual review. Dewald, Nico and Jahn have the authority to execute this BCP.

C. Plan Location and Access

Our company will maintain copies of its BCP plan and the annual reviews and the changes that have been made to it for inspection. An electronic copy of our plan is located on backup server in the documents folder.

II. Business Description

Our company conducts business in software development.
We do not hold customer funds.
Our company does not service retail customers.

III. Office Locations

Our Company has offices located King's Court, Suite 3, Buffelsfontein Road, Port Elizabeth, South Africa.
Its main telephone number is 2741 3682299. Our employees may travel to that office by means of foot, car, train, bus.

IV. Alternative Physical Location(s) of Employees

In the event of a business disruption, we will move our staff from affected offices to the closest of our unaffected office locations at 32 Overdale Avenue, Lovemore Heights, Port Elizabeth, South Africa.

V. Data Back-Up and Recovery (Hard Copy and Electronic)

Our company maintains its primary backup records and its electronic records at 32 Overdale Avenue, Lovemore Heights, Port Elizabeth, South Africa. Mario Steenkamp, 27833976984 is responsible for the maintenance of these backups.

Our company backs up its paper records by copying and taking them to our back-up site.

The company backs up its electronic records daily by transfer to a removable drive in the backup server and keeps a copy at 32 Overdale Avenue, Lovemore Heights, Port Elizabeth, South Africa.

In the event of an internal or external business disruption that causes the loss of our paper records, we will physically recover them from our back-up site. If our primary site is inoperable, we will continue operations from our back-up site or an alternate location. For the loss of electronic records, we will either physically recover the storage media or electronically recover data from our back-up site, or, if our primary site is inoperable, continue operations from our back-up site or an alternate location.

VI. Financial and Operational Assessments

A. Operational Risk

In the event of a business disruption, we will immediately identify what means will permit us to communicate with our customers, employees, critical business constituents, critical banks, critical counter-parties, and regulators. Although the effects of a business disruption will determine the means of alternative communication, the communications options we will employ will include our website www.comprsa.com, our telephone 27413682299 or our email johan@comprsa.com. In addition, we will retrieve our key activity records as described in the section above, data back-up and recovery (hard copy and electronic).

B. Financial and Credit Risk

In the event of a business disruption, we will determine the value and liquidity of our investments and other assets to evaluate our ability to continue to fund our operations and remain in capital compliance. If we determine that we may be unable to meet our obligations to those counter-parties or otherwise continue to fund our operations, we will request additional financing from our bank or other credit sources to fulfill our obligations to our customers and clients. If we cannot remedy a capital deficiency, we will file appropriate notices with our regulators and immediately take appropriate steps.

VII. Mission Critical Systems

Our company's "mission critical systems" are those that ensure prompt and accurate processing of data from and to our servers, including the maintenance of customer accounts and access to customer accounts.

We have primary responsibility for establishing and maintaining our business relationships with our customers and have sole responsibility for our mission critical functions of software development.

Recovery-time objectives provide concrete goals to plan for and test against. They are not, however, hard and fast deadlines that must be met in every emergency situation and various external factors surrounding a disruption, such as time of day, scope of disruption and status of critical infrastructure — particularly telecommunications — can affect actual recovery times.

VIII. Alternate Communications Between the Company and Customers and Employees

A. Customers

We now communicate with our customers using the telephone, email, our web site, fax, mail and in person visits at our company or at the other's location. In the event of a business disruption, we will assess which means of communication are still available to us and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. For example, if we have communicated with a party by email but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the mail.

B. Employees

We now communicate with our employees using the telephone, email and in person. In the event of a business disruption, we will assess which means of communication are still available to us and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. We will also employ a call tree so that senior management can reach all employees quickly during a business disruption. The call tree includes all staff home and office phone numbers.

IX. Critical Business Constituents, Banks and Counter-Parties

A. Business constituents

We have contacted our critical business constituents (businesses with which we have an ongoing commercial relationship in support of our operating activities, such as vendors providing us critical services) and determined the extent to which we can continue our business relationship with them in light of the internal or external business disruption. We will quickly establish alternative arrangements if a business constituent can no longer provide the needed goods or services when we need them because of a business disruption to them or our company.

B. Banks

We have contacted our banks to determine if they can continue to provide the financing that we will need in light of the internal or external business disruption. The bank maintaining our operating account is:
First National Bank - Corporate Banking

C. Counter-Parties

We have contacted our critical counter-parties, such as other broker-dealers or institutional customers, to determine if we will be able to carry out our transactions with them in light of the internal or external business disruption.

X. Updates and Annual Review

Our company will update this plan whenever we have a material change to our operations, structure, business or location. In addition, our company will review this BCP annually to modify it for any changes in our operations, structure, business, or location.

COMPRSA developed and periodically updates information and thus created:

(i) a documented contingency planning policy that addresses purpose, scope, roles, responsibilities and compliance

(ii) procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

(iii) designated officials within the organization to review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

(iv) conducts capacity planning so that necessary capacity for information processing, telecommunications and environmental support exists during crisis situations.

(v) trains personnel in their roles and responsibilities with respect to the system and provides training annually.

(vi) incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(vii) reviews the contingency plan for the information system once per year and revises the plan to address system/organizational changes or

problems encountered during plan implementation, execution, or testing.

(viii) alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.

(ix) primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization’s availability requirements.

(x) conducts backups of user-level and system-level information (including system state information) contained in the information system monthly and protects backup information at the storage location.

(xi) tests backup information quarterly to ensure media reliability and information integrity.