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)

COMPRSA Security Policy

Overview
The System Security Plan identifies the development, test and deployment environment of COMPRSA behind secure firewalls - that was designed, built and implemented as a secure system. These systems are incorporated into the teams' plans and will increase confidence that COMPRSA meets with security expectations.
This Security Policy provides an overview of the security of the COMPRSA systems and describes the controls currently in place.

System Category
All software development done by COMPRSA requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse or unauthorized access to or modification of information.

Coverage Areas
Employee Conducts and responsibilities – NDA, security policy training, illegal activities, confidential information, Safe use of Internet and email, Use of authorized software and tools, Protection of userid/password, Transport and storage of data storage – security and encryption, Violations and penalties, Password Policy, Security Awareness

Objectives
COMPRSA objectives for a secure system include:

- Data is complete: no data is lost
- Data is accurate: no data is/becomes corrupted
- Data is accessible: authorized users can access data as and where required
- No unauthorized access: only authorized users access data

System Environment
COMPRSA has high speed data lines provided by Telkom SA and Internet Solutions – Dimension Data.
Each data line is routed into the internal network of COMPRSA via secure hardware firewalls and in addition the internal computer network is NATTED for the network to maintain the public IP addresses separately from the private IP addresses.

Computer and systems usage
Computers, computer files, software, email, voice mail (or any electronic means of communication) and all other information and contents furnished to employees of COMPRSA are the exclusive property of COMPRSA.
The systems are made available to the employees according to their needs to accomplish the requirements for their position and is intended solely for COMPRSA business. COMPRSA will honor the policy noted below but reserves the right to change this policy at any time as may be required.

- The systems are provided by COMPRSA to assist in the conduct of business within the company. The use of these systems for private purposes is strictly prohibited.

- The hardware is the company's property. Therefore all messages composed, sent or received on the systems are and remain the property of COMPRSA. They are not the private property of any employee.
- The email system may not be used to solicit for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.
- No software may be installed on any computer or on the company network without prior approval from a principal.
- The company's policy prohibiting harassment, in its entirety, applies to the use of COMPRSA's systems. This includes accessing the Internet to view, download, store, print or communicate inappropriate or offensive materials. No one may use the systems in a manner that may be construed by others as harassment or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by federal, state or local law. COMPRSA reserves and will exercise the right to review, audit, intercept access and disclose all messages created, received or sent over COMPRSA's email system for any purpose. The contents of email properly obtained for legitimate purposes may be disclosed within the company without the permission of the employee.
- The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.
- COMPRSA strongly discourages the storage of large numbers of email messages, either sent or received. Retention of messages requires large amounts of storage space on the network server and personal hard drives which can slow the performance of both network and individual personal computers. All COMPRSA personnel should audit their stored email messages monthly, deleting those that no longer require action or are not necessary to an ongoing project.
- The company purchases and licenses the use of various computer software packages for business purposes and does not own the copyright to these packages or their related documentation.
- COMPRSA prohibits the illegal duplication of software and its related documentation. Unauthorized software not owned by the company is prohibited and will be removed from the systems and destroyed.
- Any COMPRSA employee who discovers a violation of this policy shall notify a management.
- Any COMPRSA employee who violates this policy or uses the systems for improper purposes shall be subject to disciplinary action, up to and including discharge from the company.

A. Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by company management, employees are prohibited from engaging in, or attempting to engage in:
   1. Monitoring or intercepting the files or electronic communications of other employees or third parties;
   2. Hacking or obtaining access to systems or accounts they are not authorized to use;
   3. Using other people's log- ins or passwords;
   4. Breaching, testing or monitoring computer or network security measures.

B. No email or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

C. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

D. Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner or as otherwise permitted by applicable law.

E. No personal email accounts or any email accounts not assigned by COMPRSA

COMPRSA email servers can be used to send communications to clients, vendors, etc.
All COMPRSA related messages must be sent from a COMPRSA email account.

Anti-Virus policy
AVAST AntiVirus is installed on all workstations and servers and may not be removed or tampered with by employees.

Access to work area and secured area (ex. server room)
Physical access to the data center is not allowed unless authorized.

Access controls measures are defined to the area containing system hardware, data, cables, electrical power, back-up media and any other elements required by the system to operate.

Physical access to the COMPRSA premises are monitored by camera and the entire complex has security guards on 24/7/365 duty.

COMPRSA has also engaged the services of an armed response company and the premises is well equipped with sensors, beams and movement detectors – directly linked to the armed response company.

The premises have a fire safety instruction procedure with fire extinguishers placed on the outside and the inside the office building.

Laptop and safe-guard of confidential information
All laptops are using encryption software.

Information Sensitivity
COMPRSA will adhere to all confidentiality agreements between the parties - information that requires protection from unauthorized disclosure.

COMPRSA will ensure data integrity - information that must be protected from unauthorized, unanticipated or unintentional modification.

In consideration for the furnishing of confidential information, COMPRSA irrevocably undertake to ensure that confidential information will be kept and safeguarded as strictly private and confidential and will not in any manner whatsoever - in whole or in part - be used by me or any representatives of COMPRSA - other than in connection with our intended working relationship.

Management Controls
Each COMPRSA employee has signed a NDA.
COMPRSA has a management-level approach to controlling security for the internal and external systems. This includes risk assessment processes, risk reviews and the behavioral expectations of all individuals who work within the system.

Personnel Security
As the greatest harm to systems comes from users' actions, users are assigned the least amount of privilege required to function.

- COMPRSA has divided critical functions among different individuals
- COMPRSA has developed a process for requesting, establishing, issuing and closing user accounts
- COMPRSA has defined termination procedures
- COMPRSA has ensured that mechanisms are in place for holding users responsible for their actions
- COMPRSA performs background screenings appropriate for the position to which users are assigned
- COMPRSA restricts user access to the minimum necessary to perform the job
- COMPRSA regularly review all positions for sensitivity level

Hardware and Software Maintenance Controls
COMPRSA has ensured that controls are in place to monitor and prohibit the unauthorized installation of hardware components or software.

COMPRSA has the following restrictions in place:

- Restrictions/controls on those who perform hardware and software maintenance activities
- Procedures for performance of emergency repair and maintenance
- Procedures for items serviced through on-site and off-site maintenance
- Procedures for controlling remote maintenance services

Data Integrity/Validation Controls
COMPRSA has adopted data integrity tools to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets their expectations. All workstation and servers have been installed with virus detection and elimination software.

Security Awareness and Training
Security training is a mandatory requirement for all system users prior to system access and also on a periodic basis for continued access.
COMPRSA provides system-specific training in the form of workshops, classroom, focus groups, role-based training and on-the job training.

Incident Response Capability
COMPRSA has created procedures for incident reporting and has ensured that the incident reporting chain is known to all users.
The plan includes descriptions for the following:

- Procedures for reporting incidents handled either by system personnel or externally
- Procedures for recognizing and handling incidents
- Identity of persons who receive and respond to alerts/advisories
- Identify the preventative measures in place, such as intrusion detection tools, automated audit logs and penetration testing

Identification and Authentication
COMPRSA user access is controlled via the Active Directory and user authentication control mechanisms, such as password, token and biometrics are enforced. Passwords are recycled and changed on a monthly basis via the system administrator and COMPRSA adheres to the standard industry-wide password policy as indicated below:

- Allow storage of passwords using reversible encryption for all users in the domain
- Allowable character set
- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Number of generations of expired passwords disallowed for use
- Passwords must meet complexity requirements of installed password filter
- There are procedures for handling password compromise
- There are procedures for password changes (after expiration and forgotten/lost)
- There are procedures for training users and the materials covered
- User must logon to change password

Ongoing Security Management
There is no public access to COMPRSA servers or workstations.

COMPRSA regularly determine if security standards are in place and adhered to, if they fulfill the requirements during operation and if they should be altered after changes have taken place.