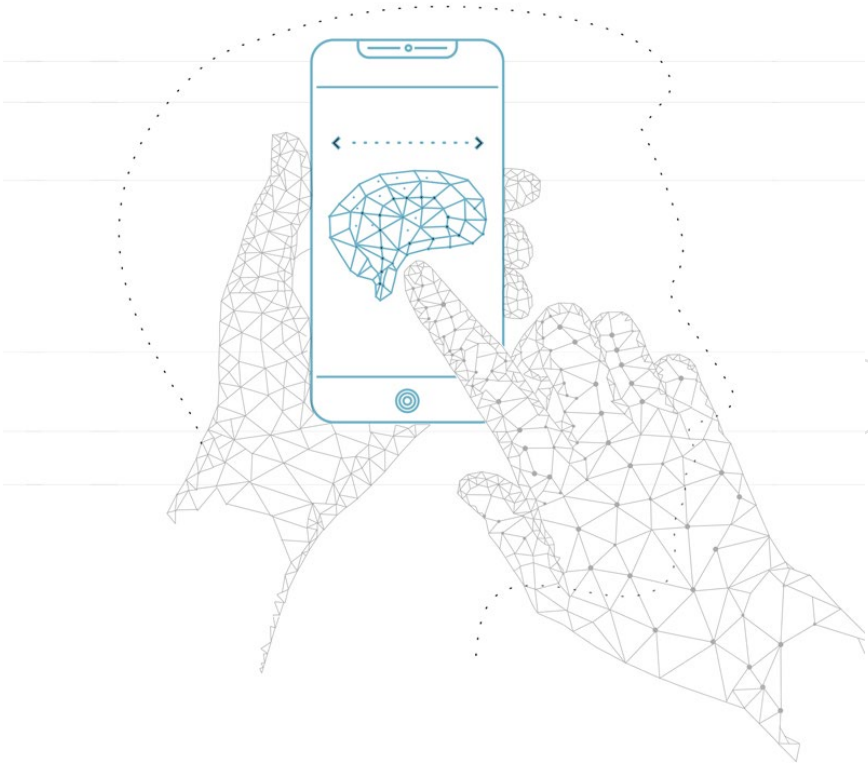
Supplier Compliance

General Data Protection Regulation (GDPR)
and
Protection of Personal Information Act (POPIA)

21/07/2021



CRS Technologies (RF) (Pty) Ltd - 2000/009010/07
+27 11 259 4700 (t) • +27 11 259 4750 (f) • info@crs.co.za • crs.co.za
Centric House, Mellis Court, Mellis Road, Rivonia, 2128 • PO Box 2712, Rivonia, Gauteng, 2128
Director: M. Moodle

engage
Unlocking human potential

Overview

This document outlines the compliance required by suppliers to CRS Technologies. The sections below require information and acceptance of responsibility for;

- Supplier data code of conduct;
- Supplier data protection security;
- Supplier confidential information policy.

All members who have access to the CRS environment must accept all three sections.

Members of SUPPLIER

Suppliers need to complete the table below outlining all members who have access to the CRS environment and what they have access to.

Name	Surname	Contact No.	Email	ID No	Address
Mathew	Payne	000000	example@crs.co.za	0000000000	1 Mellis Road Rivonia
Access to the following. **1. Environment = Yes** **2. Servers = Yes** **3. Data = Yes** **4. Full Permissions = Yes**					

Supplier Code of Conduct

SUPPLIER Data Code of Conduct Alignment with POPIA

1. Each SUPPLIER member is required to comply with the code of conduct insofar as those sections of the code are relevant and applicable to the services provided by that member.

2. This code applies to internet services offered by SUPPLIER's members. In cases where a division of a company applied for SUPPLIER membership the code only applies to the services and products offered by that division.

B. Freedom of expression

3. SUPPLIER members must respect the constitutional right to freedom of speech and expression.

C. Privacy and confidentiality

4. SUPPLIER members must respect the constitutional right of internet users to personal privacy and privacy of communications.
5. SUPPLIER members must respect the confidentiality of customers' personal information and electronic communications. SUPPLIER members must only gather or retain customer information as permitted by law, and must not sell or distribute such information to any other party without the written consent of the customer, except where required to do so by law.

D. Consumer Protection and Provision of Information to Customers

6. SUPPLIER members must provide the following information on their websites: registered name, email address and telephone numbers and physical address.
7. SUPPLIER members must inform their customers that member of SUPPLIER must uphold and abide by this code of conduct. Members' websites must include a reference to SUPPLIER membership, a prominent copy of SUPPLIER's logo and a link to the section of the SUPPLIER website that contains the code of conduct, complaints and disciplinary procedure and the take-down procedure.
8. SUPPLIER members must have policies for acceptable or fair use for their internet access services. This policy must be made available to customers prior to the commencement of any such service agreement and at any time thereafter, on request.
9. Policies for acceptable or fair use must include:
    - A requirement that the customer will not knowingly create, store or disseminate any illegal content;
    - A commitment by the customer to lawful conduct in the use of the services, including copyright and intellectual property rights; and
    - An undertaking by the customer not to send or promote the sending of spam.
10. In their dealings with consumers, other businesses, each other and SUPPLIER, SUPPLIER members must act fairly, reasonably, professionally and in good faith. In particular, pricing and other material information about services must be clearly and accurately conveyed to customers and potential customers.
11. SUPPLIER members may only offer service levels which are reasonably within their technical and practical abilities.

12. SUPPLIER members must comply with all compulsory advertising standards and regulations.

E. Terms and Conditions

13. SUPPLIER members must make available to customers (and potential customers) any applicable terms and conditions prior to the commencement of any contract. Terms and conditions must include all information and terms relevant to the relationship with the recipient of the service.
14. Terms and conditions must give an SUPPLIER member the right to remove any content hosted by that member which it considers illegal or for which it has received a take-down notice.
15. Terms and conditions must give the SUPPLIER member the right to suspend or terminate the service of any customer that does not comply with the terms and conditions, acceptable or fair use policies, or any other contractual obligations.

F. Unsolicited Communications (Spam)

16. SUPPLIER members must not send or promote the sending of unsolicited electronic communications and must take reasonable measures to ensure that their networks are not used by others for this purpose.
17. SUPPLIER members must provide a facility for dealing with complaints regarding unsolicited electronic communications originating from their networks and must react expeditiously to complaints received.

G. Cyber Crime

18. SUPPLIER members must take all reasonable measures to prevent unauthorised access to, interception of or interference with any data on that member's network and under its control.

H. Protection of Minors and Vulnerable Persons

19. SUPPLIER members must take reasonable steps to ensure that they do not offer any paid services to minors without written permission from a parent or guardian.
20. SUPPLIER members must provide Internet access customers with information about procedures and software applications which can be used to assist in the control and monitoring of minors' access to Internet content. This requirement does not apply to corporate customers where no minors have Internet access.
21. SUPPLIER members must have processes in place to respond to directives issued by a court in terms of any applicable legislation, including but not limited to:
    - The Protection from Harassment Act (No. 17 of 2011); and
    - The Maintenance Act (No. 99 of 1998).

22. SUPPLIER members must have processes in place to ensure that they comply with the requirements set out for ISPs (internet service providers) in the Films and Publications Act (No. 65 of 1996) as amended.

I. Lawful Conduct

23. SUPPLIER members must always conduct themselves lawfully and must co-operate with law enforcement authorities within the applicable legal framework.
24. SUPPLIER members must respect intellectual property rights and not knowingly infringe such rights.
25. SUPPLIER members must uphold and abide by this code of conduct and adhere to the associated complaints and disciplinary procedures.

J. Unlawful Content and Activity

26. There is no general obligation on any SUPPLIER member to monitor services provided to customers, but a member is obliged to take appropriate action where it becomes aware of any unlawful content or conduct.
27. SUPPLIER members must not knowingly host or provide links to unlawful content, except when required to do so by law.
28. If a SUPPLIER member becomes aware of conduct or content which has been determined to be illegal, it must suspend or terminate the relevant customer's service and report the conduct or content to the relevant law enforcement authority. The SUPPLIER member must report such cases and any action taken to SUPPLIER within a reasonable period of time.
29. SUPPLIER members must establish a notification and take-down procedure for unlawful content and activity in accordance with SUPPLIER's take-down notification procedure, and respond expeditiously to such notifications.
30. SUPPLIER members must submit a report to SUPPLIER on the steps taken in response to a take-down notice within a reasonable period of time after such a notice is lodged.
31. SUPPLIER members must keep a record of all take-down notices received and any materials taken down for a period of at least three years unless possession of such materials is illegal.

K. Voluntary Codes of Best Practice

32. SUPPLIER publishes a number of voluntary codes of practice and best practice documents. SUPPLIER's members are not obliged to comply with these additional codes. If a member has indicated that they are voluntarily complying with any additional codes, then they are required to do so as an extension of this code of conduct.

L. Compliance with the Code of Conduct

33. SUPPLIER members must receive and investigate complaints made in accordance with this code of conduct and any additional codes of practice or best practices a member has voluntarily complied with, unless such complaints are frivolous, unreasonable, vexatious or in bad faith.
34. SUPPLIER members must make all reasonable efforts to resolve complaints in accordance with the complaints procedure.
35. SUPPLIER members must co-operate with SUPPLIER in accordance with the complaints and disciplinary procedure and comply with any decisions taken by SUPPLIER with respect to the code of conduct and complaints and disciplinary procedure.
36. SUPPLIER members must submit an annual statement to SUPPLIER confirming their compliance with the code of conduct.
37. SUPPLIER members accept that SUPPLIER has an obligation to audit member compliance on an annual basis and perform regular compliance spot checks, and must co-operate with SUPPLIER during such audits or spot checks.
38. SUPPLIER may investigate the conduct and compliance with the code of conduct by members on its own initiative and may, if appropriate, institute disciplinary proceedings as set out in the code of conduct complaints and disciplinary procedure.

M. Alterations

39. SUPPLIER reserves the right to make alterations to this code of conduct from time to time. Such amendments are binding on all SUPPLIER members. The current code of conduct will be maintained on the SUPPLIER's website.

CRS Data Protection Policy

Policy

Our policy is and always will be that clients own their data. No employee will be allowed to access client data without adhering to the procedures set out in this document.

Non-adherence to this policy may lead to disciplinarily action and/or termination and/or prosecution.

Procedures

When a SUPPLIERS employee requires access to the CRS environment the following procedure will be followed:

A system request **MUST** be logged in support.crs.co.za. The system request number must be used as a reference on all communication. The subject line must contain “SRxxxx:” followed by the subject.

Accusation

- Employee is appointed to the data, takes ownership and accepts responsibility.
- Send a written request to the client and carbon copy (Cc) the following:
    - Direct manager
    - Client services
    - Senior management
    - Technical support
- Client must confirm in writing that access has been granted to the appointed individual.
  Request drive from technical support.

Transportation

- CRS approved memory stick or external HDD is collected from technical support.
    - Drive is formatted and renamed to client.
    - Antivirus is run on device.
    - Encryption is applied as required.
- Only approved files are copied to the drive.
    - Files are compressed with passwords.
    - The client must sign off the copy.
- File encryption must be enabled.

Termination

Refer to the CRS Confidential Information Policy.

The CRS Way

We ensure that we deal with client data in a professional manner. Security of the data is our top priority.

SUPPLIER Confidential Information Policy

Policy

‘Confidential Information’ refers to any information or document that a business or individual does not wish to make public. It can include anything that has been acquired by or made

available to an individual or other legal entity in the course of the relationship between the parties.

It may include, but is not limited to, any information or documents about a business's organisational structure, activities, operating procedures, products and services, intellectual property, trade secrets and know how, finances, plans, transactions and policies, all employee records, pay runs and client data.

We treat all information as confidential.

Procedures

Client Data Termination/Implementation Completion

- Client sign-off required.
- On completion of client installation or termination, the following actions are required by staff:
    - *Developers only*: push final changes to developer branch for master release.
    - All confidential communication, from client-related to confidential, must be permanently deleted or moved to a secure encryption location.
    - All database backups and archived information must be permanently deleted.
    - Off-site backups to be removed and recycled.
    - *Developer only*: developer environment cleaned of client data, super admin remains.
    - Production environment is cleaned and all backups removed.
    - Live systems and databases are checked for confidential information.
    - Removal confirmation letters from all staff are required before certificate will be issued.
    - Issue client certificate.

Client Database Backups

This process is for dealing with client data received from the client for analysis or advanced stage debugging.

- Client sign-off required.
- On completion of action task the following actions are taken by staff:
    - Delete client database version from:
        - Development
        - Quality Assurance

        - Production
    - *Developer only*: Delete local instance.
    - Delete all communication related to the transfer of the database.
    - Delete the SFTP client database backup.
    - Live systems and databases are checked for confidential information and removed.
    - Issue client certificate.

Client On-Premise

- Client access sign-off is required.
- Remote access details.
- VPN details.
- Monitoring details (Team Viewer).
- No employees will be modified or viewed.
- Access to employee pay items are restricted and no access unless client accesses the employee.
- If you require access to an employee the client should create a test employee.
- No screen captures allowed, unless client taken and emailed.
- No screen recorders are allowed, unless client stipulated.
- No USB devices are allowed, unless client backup required for analysis in writing signed off by the client.

Client Emails with Confidential Files

- All files or emails containing the following information must be removed and permanently deleted;
    - Passwords (StoreVault is required)
    - RDP details (remote connection manager is required)
    - VPN details
    - Backups
    - Import or CSV files
- If files cannot be deleted, they will need to be stored on the CRS file server, and will be scheduled for compression and encryption. These files are password-protected and require administrator access.
- Issue client certificate.

The CRS Way

CRS Technologies employees are always required to adhere to these policies and procedures when dealing with client and company data.

All employees who have/had access to client data will be required to sign off the client certificate on completion or termination of the project and/or employment.

SUPPLIER Member	Signature	Date

Document Review Outline (Admin Use Only)

Author	**Review Team**	**Date**
Nicol M	Nicol	July 2021
Mat P	Ian, Mat	Dec 2021