Data Protection Policy

This document outlines the policies and procedures
all staff are required to adhere to when dealing with data.

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

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 disciplinary action and/or termination and/or prosecution.

Procedures

When a CRS employee requires access to client data the following procedures 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.

Document Review Outline (Admin Use Only)

Author	**Review Team**	**Date**
Mat P	Ian, Mat	Dec 2019
Nicol M	Nicol	July 2021