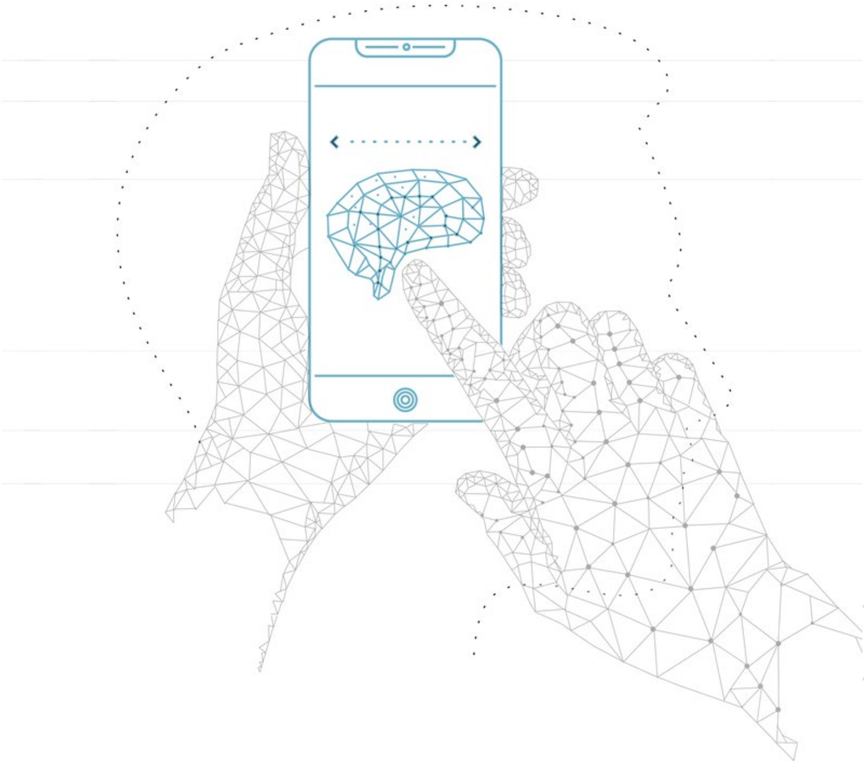
CRS Security & Password Policy

CRS Requirements and Standards

Last Updated: 20/07/2021



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 requirements and processes support agents at CRS are required to follow.

Terms and Conditions

This document outlines the policies and procedures that all employees of CRS Technologies (Pty) Ltd and affiliated companies, including CRS Human Capital (Pty) Ltd, CRS Recruitment Outsourcing Solutions (Pty) Ltd, CRS Konsult (Pty) Ltd, CRS Outsourcing (Pty) Ltd, Centric Solutions (Pty) Ltd and Adfinserv (Pty) Ltd must adhere to.

Document Information

Author	Mathew Payne
Amendment	Nicol Myburgh
Date Amended	20-07-2021
Definition	Draft
Version	1.00.3
Review Date	01-09-2021

CRS Application Data

All CRS applications adhere to the following data policies:

Data in Transit

All data is transferred over SSL with valid RapidSSL certificates.

Data at Rest

All passwords are encrypted in the database SHA256. Only the hash is stored.

FTP

All data is transferred over SFTP. All files are compressed and encrypted.

API

All sensitive data is encrypted during transit using a SQL symmetric key.

Password Policy

The CRS application adheres to the following password policies:

Password Expiry Interval

Number of days a user can use his/her password before the system forces a password change.

Inactive Days before Profile Disabled

If a user did not log on to the system for a selected number of days his/her user status will be changed to inactive.

Number of Passwords to Remember

Prevent a user from using the same password for a selected number of times when doing password changes.

Minimum Password Length

Password length cannot be less than the entered number of characters.

Number of Adjacent Characters

Prevent passwords from containing more than the entered number of adjacent characters.

Number of Repeating Characters

Prevent passwords from containing more than the entered number of same characters.

Maximum Logon Attempts

Number of invalid password attempts before the user status is changed to inactive.

Force Alpha and Numeric Password

Password must consist of both alpha and numeric characters.

Password Storage

All CRS application passwords are stored in Microsoft SQL. The following steps have been taken to ensure they are not visible to anyone:

Data Encryption At Rest

CRS uses bit locker to encrypt the drive which stores the database.

Password Encryption

The physical password in the SQL table is also encrypted using SHA256 HASH. The password is not stored, only the hash is stored.

Client Keys and Passwords

All CRS client keys or passwords and/or critical information is stored in the CRS Azure key vault, with limited access and multifactor authentication.