21 CFR Part 11 Compliance White Paper for Chromcore Chromatography Workstation

Executive Summary: This document outlines how the Chromcore Chromatography Workstation fulfills the requirements established by the United States Food and Drug Administration (FDA) in Title 21 of the Code of Federal Regulations (CFR) Part 11. It provides both a conceptual overview of the regulation and a detailed compliance matrix demonstrating system features mapping directly to legal expectations.

1. Overview of FDA 21 CFR Part 11

FDA 21 CFR Part 11 establishes the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and fundamentally equivalent to paper records and handwritten signatures executed on paper. Released in 1997, it applies to all FDA-regulated industries (such as pharmaceuticals, medical devices, and biotech) that choose to maintain records or submit information electronically.

Key Pillars of Part 11 Compliance:

- **Data Integrity & Electronic Records (Subpart B):** Focuses on ensuring that electronic entries are authentic, cannot be altered without detection, and are accurately retrievable throughout their lifecycle. This requires closed system controls, independent audit trails, and strict system validation.
- **Electronic Signatures (Subpart C):** Ensures that electronic signatures are uniquely linked to individual users, legally binding, and secure against falsification or unauthorized copying.

Compliance is a shared responsibility. The software platform (Chromcore) provides the technical controls and safeguards, while the end-user organization must implement proper standard operating procedures (SOPs), system validation protocol, and administrative policies.

2. 21 CFR Part 11 Compliance Matrix

The following evaluation matrix outlines the specific requirements of Subpart B (Electronic Records) and Subpart C (Electronic Signatures), detailing the technical controls built directly into the Chromcore Chromatography Workstation software.

21 CFR Clause	FDA Requirement Summary	Chromcore Chromatography Workstation Implementation
§ 11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Chromcore is developed under a strict software development life cycle (SDLC). The software includes automated Installation Qualification (IQ) tools to allow users to execute automated performance verification. To maintain full validation states, BIKAI provides comprehensive Operational Qualification (OQ) and Performance Qualification (PQ) documents and protocols for manual execution.
§ 11.10(b)	The ability to generate accurate and complete copies of records in both human readable and electronic form for inspection, review, and copying by the agency.	All raw chromatographic data, meta-data, integration parameters, and calibration curves are securely stored in database. Chromcore provides reporting engines that export raw and processed data into secure, immutable PDF formats or encrypted electronic formats while maintaining layout fidelity for regulatory inspectors.
§ 11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Chromcore utilizes a secure, centralized database architecture that prevents direct OS-level deletion or modification of files. System files are indexed with unique database keys, supporting systematic backup strategies and archiving features that maintain data accessibility over long-term compliance cycles.
§ 11.10(d)	Limiting system access to authorized individuals.	The workstation provides configurable Role-Based Access Control (RBAC) to restrict system access to authorized users only. Users must log in using a unique username and password. Upon first login, users are required to change their password, which must comply with configurable complexity rules including uppercase letters, lowercase letters, numbers, and special characters. The system also supports configurable account lockout after multiple failed login attempts and automatic workstation locking after a defined period of inactivity.

21 CFR Clause	FDA Requirement Summary	Chromcore Chromatography Workstation Implementation
§ 11.10(e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.	Chromcore implements a system-generated, immutable audit trail. Any changes to injection sequences, methods, processing parameters, or user privileges are automatically timestamped using the secure system clock. The audit trail captures the User ID, Old Value, New Value, and requires a mandatory 'Reason for Change'. Previous values are never overwritten or obscured.
§ 11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The system utilizes procedural locks ensuring critical sequences are run in chronological order. For example, a sample cannot be processed against an unapproved or incomplete calibration method, and data analysis routines must strictly follow raw data acquisition steps.
§ 11.10(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Chromcore supports multi-level authority management through configurable user groups and role-based permissions. Users may be assigned to different groups, such as Operators, Analysts, Reviewers, or Administrators, with each group granted specific permissions according to their responsibilities. Access to functions such as data acquisition, data processing, method modification, result review, approval, and system administration can be restricted to authorized personnel only, helping ensure proper authority control and segregation of duties
§ 11.10(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Chromcore supports instrument communication through configured interfaces such as LAN and RS232. The workstation continuously monitors the connection and operational status of chromatographic modules including pumps, autosamplers, column ovens, and detectors. If device disconnection or communication abnormalities are

21 CFR Clause	FDA Requirement Summary	Chromcore Chromatography Workstation Implementation
		detected, the system generates error alerts and prevents uncontrolled data acquisition.
§ 11.10(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Chromcore provides complete product documentation, structured training paths, and comprehensive Help Menus. Client organizations must manage and log specific personnel training workflows within their own organizational SOP frameworks.
§ 11.50	Signed electronic records shall contain information associated with the signing that clearly indicates the printed name of the signer, the date and time when the signature was executed, and the meaning associated with the signature.	When a user electronically signs a report or data set in Chromcore, the software embeds a signature block displaying the signer's full printed name, a timestamp synced to the secure server clock, and a clear statement of intent (e.g., 'Created', 'Reviewed', or 'Approved'). This information is permanently bonded to the record.
§ 11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Chromcore links electronic reports with their associated raw data and related records. Once an electronic report has been reviewed and approved through electronic signature, the associated data records are locked and can no longer be modified
§ 11.100	Electronic signatures shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Chromcore requires each user to maintain a unique username and electronic signature credential. Duplicate usernames cannot be created within the system, ensuring that each electronic signature is uniquely attributable to a single individual.

21 CFR Clause	FDA Requirement Summary	Chromcore Chromatography Workstation Implementation
§ 11.200	(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual’s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine	Chromcore uses non-biometric electronic signatures based on unique user credentials. Each user is assigned a unique login username and password, and electronic signatures for report approval require credential verification by the authorized user. All passwords are masked during entry and are not displayed under normal operating conditions. The system supports additional security controls including automatic workstation locking after a configurable period of inactivity, configurable password expiration policies requiring periodic password changes, and automatic user account lockout after a defined number of failed password attempts.

21 CFR Clause	FDA Requirement Summary	Chromcore Chromatography Workstation Implementation
	owners.	
§ 11.300	Controls for identification codes and passwords to ensure their security, including maintaining uniqueness, periodic expiration, and protection against unauthorized use or replacement.	Chromcore supports strict password aging, minimum character configurations, historical password reuse blocks, and automatic account lockout thresholds following consecutive failed login attempts. Full auditing is performed on administrative changes to user security profiles.