240-547-5446
info@gkaccess.com
gkaccess.com

Securing VCIN Access with GateKeeper

What is VCIN?

The Virginia Criminal Information Network (VCIN) functions as a service facility **under the management control of the Virginia Department of State Police**, providing operational support to the entire criminal justice community. The primary mission of VCIN is to provide a means of rapid communications for criminal justice agencies throughout Virginia. It is a **statewide data communications network** incorporating computerized links to regional and national law enforcement systems:

- Virginia Department of Motor Vehicles (DMV)
- National Crime Information Center (NCIC)
- National Law Enforcement Telecommunications System (NLETS) International Justice & Public Safety Network

VCIN is **available to any department or division of state government meeting the definition of a criminal justice agency** as contained in §9.1-101, Code of Virginia, any county, city, town, railroad, or college campus police department, special police departments maintained by corporations in Virginia, and to federal criminal justice agencies, subject to the approval of the Superintendent, Department of State Police.

Why VCIN Compliance Matters

VCIN compliance is critical because it safeguards the integrity, confidentiality, and lawful use of criminal justice information across Virginia's law enforcement network. The Virginia Criminal Information Network (VCIN) serves as a vital communication and data-sharing system that links local, state, and federal agencies. Compliance ensures that every user—whether an officer, dispatcher, or records clerk—handles criminal history and investigative data in accordance with the Virginia Administrative Code, Chapter 120, and the Code of Virginia § 9.1-126 et seq.

By adhering to VCIN security and operational standards, agencies protect sensitive information from unauthorized access, data breaches, or misuse. Noncompliance can lead to legal penalties, loss of VCIN access, and reputational harm to the agency. Beyond regulatory obligations, maintaining compliance enhances public trust, ensures the accuracy of criminal records, and supports fair and effective law enforcement operations throughout the Commonwealth.

Key VCIN Security Dimensions

6VAC20-120 – Regulations on Criminal History Record Information (CHRI) Use & Security (Virginia):

240-547-5446
info@gkaccess.com
gkaccess.com

Part III — Security Requirements

- **Physical Access (§130)**: Limit to authorized staff; controls, intrusion procedures, disaster protection, backups, and (for larger agencies) disaster recovery plans are recommended.
- **Telecommunications (§150)**: Direct/remote CHRI access must use dedicated lines; nondedicated transmission generally prohibited unless expressly approved; VCIN access requires VSP approval; unattended remote devices must be rendered inoperable; secure facilities/device & operator identification; protect against tampering/tapping.
- **Computer Operations (§160)**: Technical controls to prevent unauthorized access/changes; non-CJ terminals blocked; log intrusion attempts; designated system administrator; right to audit/monitor.

Key VCIN Requirements and How GateKeeper Delivers Compliance

Category	Citation (Combined)	VCIN Requirement (Summarized)	How GateKeeper Meets It (Specific)
Physical Access & Organizational Controls	**6VAC20-120-130(A–G)**	Agencies must limit CHRI access to authorized personnel; detect unauthorized access; ensure only authorized officers/employees have direct access; require those with access to protect CHRI; safeguard repositories from disasters; maintain backups/disaster recovery; and tightly control system documentation.	GateKeeper enforces **user-specific authentication** (token + PIN) so only authorized users can unlock CHRI workstations; **auto-locks** when users leave to prevent exposure; provides **audit logs** to help detect unauthorized access attempts; supports **Hub backup** to retain authentication policies; and uses **role-based admin access** so only designated admins can view/modify GateKeeper system configuration.

240-547-5446
info@gkaccess.com
gkaccess.com

Telecommunications & Remote Device Requirements	**6VAC20-120-150 (all paragraphs)**	CHRI/VCIN access over networks must use **dedicated or approved lines**; any access to VCIN requires **VSP approval**; remote devices must be **secure, attended, or made inoperable when unattended**; and telecom facilities/devices must be secured, hardware-identified, and protected from tampering, with proper operator identification.	On VCIN-connected workstations, GateKeeper ensures that **only authorized, authenticated users** can use the terminal; when a user walks away with their token, the workstation is **automatically locked (made inoperable)**; and each access is tied to a specific **operator identity** (user + token + PIN), supporting the requirement for operator identification and secure use of remote devices.
Computer Operations & Logical Security Controls	**6VAC20-120-160(A–I)**	Agencies must implement technical controls to **prevent unauthorized access** to CHRI; operate systems according to approved procedures; ensure CHRI cannot be modified or accessed from non-CJ terminals; restrict unauthorized queries/updates/destruction; detect and **log intrusion attempts**; keep security program details restricted; designate a **system administrator**; and maintain the ability to **audit and inspect** security procedures.	GateKeeper provides **MFA (token + PIN)** and **proximity-based locking** to prevent unauthorized use of CHRI workstations; Hub policies enforce **consistent authentication behavior** across the agency; access to CHRI-capable terminals is restricted to **authorized AD / CJ user accounts**; all unlock/lock events, failed PINs, and invalid token attempts are **logged** and can be exported for audits; and **Hub admin roles** designate who manages user accounts, tokens, and policies, supporting both system-administrator and audit requirements.

How GateKeeper Strengthens VCIN Compliance

1. **Automates Access Control & MFA**

240-547-5446
info@gkaccess.com
gkaccess.com

- Enforces **multi-factor authentication (MFA)** for all access to VCIN-connected workstations and systems, ensuring that only **authorized criminal justice personnel** can log in.
- Provides proximity-based authentication and authorization to workstations.
- Applies granular access by user, role, or workstation, restricting VCIN access to authorized operators.

2. **Data Protection**
   - GateKeeper automatically locks a user's workstation when they are no longer near their workstation - preventing unauthorized access/viewing of VCIN data.
   - Integrates secure password vaulting to auto-fill credentials without manual typing, minimizing password reuse, exposure, and phishing risks across VCIN-linked systems.
3. **Secure Configurations**
   - GateKeeper automates access control, MFA, and password management, reducing the risk of misconfigurations caused by human error.
   - Integrates with AD for centralized control.
   - Supports agency-defined lockout and timeout policies consistent with VCIN and CJIS standards.
4. **Network Security Against Unauthorized Access**
   - Generates comprehensive audit trails of user-specific login and logout activity to facilitate VCIN audits, internal inspections, and state reporting.
   - Continuously monitors for abnormal login activities 24/7.
5. **Physical Security**
   - Prevents shared, tailgated, or unattended workstation use, ensuring only authorized users' access to VCIN-connected systems.
   - Uses proximity tokens or smart cards linked to each user's presence to meet VCIN physical access requirements.

Benefits for VCIN Agencies

- **CJIS/VCIN-Compliant MFA:** Enforces strong, proximity-based authentication for all users accessing VCIN-connected systems in law enforcement.
- **Instant Session Lock**: Instantly secures unattended VCIN-connected workstations, preventing unauthorized access to criminal history record information.
- **Zero Password Sharing**: Ensures every VCIN system login is tied to a verified user identity, eliminating shared credentials and meeting audit requirements.
- **Complete Audit Trails**: Simplifies VCIN compliance reviews with precise, user-specific access logs.