

VESTAL FIRE DISTRICT

Key and Access Control Policy

Adopted: September 23, 2026

Revised

Policy #:	208.00
Policy:	Key and Access Control Policy
Effective Date:	September 23, 2026
Authority:	
Cross-reference:	

1. Purpose

The purpose of this policy is to establish uniform procedures and responsibilities for the issuance, control, use, accountability, and return of all physical and electronic access credentials used to access Vestal Fire District property, facilities, and secured areas.

This policy is intended to protect district personnel, property, equipment, information systems, and operational readiness through proper access control and security practices.

2. Scope

This policy applies to all members, employees, officers, commissioners, contractors, vendors, and any other individuals authorized to access Vestal Fire District property.

The Vestal Fire District currently maintains:

- Four (4) fire stations
- One (1) district office
- One (1) Fire Training Site

Access methods covered under this policy include, but are not limited to:

- Physical keys
 - Electronic key fobs
 - Mobile credential access through approved applications
 - Any future district-issued access credentials or systems
-

3. Policy Statement

Access to Vestal Fire District facilities shall be limited to authorized individuals with a legitimate operational or administrative need. All access credentials remain the property of the Vestal Fire District and are issued solely for official district business.

Members and personnel entrusted with access credentials are responsible for maintaining the security, accountability, and proper use of those credentials at all times.

4. Authority and Administration

The Commissioner directly overseeing the Physical Security Director shall maintain overall administrative oversight of the district physical security program.

The Physical Security Director shall have primary responsibility for the administration, oversight, issuance, tracking, auditing, and revocation of all district access credentials.

The Physical Security Director may designate authorized personnel to assist with the administration of this policy.

No access credential shall be issued without authorization from the Physical Security Director or designee.

5. Access Levels and Credential Issuance

A. Mobile Access Credentials

General district members may be granted mobile application-based access credentials for approved district facilities as determined appropriate by district administration.

B. Electronic Key Fobs

Electronic key fobs may be issued to personnel based upon operational need, assignment, rank, or administrative necessity.

C. Physical Keys to District Station

Physical exterior door keys shall generally be limited to:

- Physical Security Director
- Department Chief
- Station Chiefs

D. Physical Keys to District Office

Physical exterior door keys shall generally be limited to:

- Physical Security Director
- Fire Commissioner Chair
- One designee (Commissioner or Staff Member) of the Fire Commissioner Chair

Additional physical keys for interior areas within district buildings shall be the responsibility of the respective Station Chief for their assigned station or the appropriate Commissioner for the district office.

An exterior access key shall be maintained at the district office for temporary sign-out when operationally necessary. Any sign-out or issuance of the exterior access key must receive prior approval from the Physical Security Director or the Commissioner overseeing the Physical Security Director. Appropriate accountability records shall be maintained for any temporary key issuance.

6. Prohibited Conduct

No member or authorized individual shall:

- Loan, share, duplicate, transfer, or provide any access credential to another person
- Permit any unauthorized individual to use their assigned credential
- Allow another authorized member to use their assigned credential in place of obtaining proper authorization or credentials
- Duplicate or attempt to duplicate any district key, fob, or access credential without written authorization
- Circumvent, disable, tamper with, or interfere with any district security or access control system
- Use district access credentials for non-district or unauthorized purposes

Each issued access credential is assigned to a specific individual and shall remain under that individual's control at all times.

7. Lost, Stolen, or Compromised Credentials

Any lost, stolen, compromised, damaged, or unaccounted-for access credential shall be immediately reported to:

- The member's chain of command; and
- The Physical Security Director or designee

This requirement applies to:

- Physical keys
- Electronic key fobs
- Mobile device access credentials

Personnel shall provide all available information regarding the loss or compromise so that appropriate corrective action may be taken, including credential deactivation, reprogramming, lock replacement, or access auditing.

Failure to promptly report compromised credentials may result in disciplinary action.

8. Credential Accountability

The Physical Security Director or designee shall maintain records of all issued credentials, including:

- Credential type
- Credential number or identifier, if applicable
- Assigned individual
- Date issued
- Access level granted

The district may conduct periodic audits of issued credentials and access permissions.

Personnel shall cooperate with all accountability checks and audits.

9. Return of District Property

All district-issued access credentials shall be returned immediately upon:

- Resignation
- Retirement
- Suspension
- Termination
- Leave of absence when directed
- Removal from position requiring access
- Request by district administration

The Vestal Fire District reserves the right to revoke or modify access privileges at any time.

Failure to return district property may result in disciplinary action and/or legal action.

10. Mobile Device Security

Members utilizing mobile application-based access credentials shall maintain reasonable security measures on their devices, including:

- Device passcodes or biometric security
- Updated software when practical
- Prompt reporting of lost or stolen devices

Members shall not intentionally store or share access credentials in an insecure manner.

The district reserves the right to revoke mobile access credentials from any device deemed insecure or compromised.

11. Access Monitoring and Privacy Notice

The Vestal Fire District reserves the right to monitor, log, review, and audit facility access activity for security, operational, investigative, and administrative purposes.

Use of district-issued or district-authorized access credentials constitutes acknowledgment that access activity may be recorded and reviewed.

12. Visitors and Contractors

Vendors, contractors, and governmental entities shall access district facilities only when authorized.

Visitors and non-members shall access district facilities only when authorized and when appropriate supervision or an escort is provided.

Temporary access credentials may be issued when operationally necessary and shall be returned immediately upon completion of authorized activities.

Temporary access credentials may also be signed out through the district office. District staff shall be responsible for documenting and issuing the temporary credential to the authorized vendor, contractor, or visitor, and for maintaining appropriate accountability records regarding the issuance and return of the credential.

13. Emergencies and Temporary Access

Nothing in this policy shall prohibit members from taking reasonable actions necessary to protect life, safety, or district property during emergencies.

Temporary emergency access assignments may be authorized by district administration or the Physical Security Director when operationally necessary.

14. Violations

Violations of this policy may result in one or more of the following, as applicable:

- Revocation of access privileges
- Disciplinary action
- Financial responsibility for replacement costs
- Referral for criminal investigation or prosecution when applicable

Disciplinary action shall be consistent with applicable district rules, bylaws, policies, and laws.

15. Policy Review

This policy shall be periodically reviewed and updated as necessary by district administration and the Physical Security Director to ensure continued effectiveness and compliance with operational and security needs.

16. Acknowledgment

All personnel issued district access credentials may be required to acknowledge receipt and understanding of this policy in writing.

Appendix A – Definitions

Access Credential

Any physical or electronic method used to gain entry to district property or systems, including keys, fobs, mobile applications, cards, codes, or similar devices.

Compromised Credential

Any credential believed to be lost, stolen, duplicated, improperly accessed, shared, or otherwise no longer secure.

Physical Security Director

The individual designated by the Vestal Fire District to oversee facility security and access control systems.

Designee

An individual authorized by the Physical Security Director to perform functions under this policy.

By Order of the Board of Fire Commissioners
Vestal Fire District
Date approved: September 23, 2026