CITY OF LYNCHBURG

Electoral Board

Computer Systems Security Program

Approved by the Electoral Board
September 1, 2021

____
John W. Cobbs, Secretary

August 30, 2021

Purpose: This document establishes the specific requirements applicable to the security of computer systems in use in the City of Lynchburg to conform to the requirements and recommendations of *Virginia Department of Elections Minimum Security Standards and Voter Registration System Security*, *COV VSM Standard SEC2005-01.1* (Voting Systems Security Standard), *COV VSM Policy SEC2005-01* (Voting Systems Security Policy), *COV VSM Self-Assessment Guide SEC2005-01.1* (Voting System Security Self-Assessment Guide), *COV VSM Guideline SEC2005-01.1* (Voting Systems Security Guidelines), and the Virginia Help America Vote Act (HAVA) State Plan dated July 31, 2003 as amended on July 19, 2005.

These procedures and policies apply to all personnel who may come into contact with the Computer Systems in use in the City of Lynchburg General Registrar's Office, including all employees, volunteers, vendors, and emergency personnel.

Any aspect of Computer Systems security not addressed by this document shall be governed by the references stated above.

General Responsibilities:

Electoral Board - In accordance with the *Code of Virginia, §24.2-109*, the Electoral Board "…shall perform the duties assigned by this title including, but not limited to, the preparation of ballots, the administration of absentee ballot provisions, the conduct of the election, and the ascertaining of the results of the election."

General Registrar, Deputy Registrar, Assistant Registrar – In accordance with the *Code of Virginia §24.2-114*, the General, Deputy, and Assistant Registrar(s) shall "Carry out such other duties as prescribed by the Electoral Board."

Officers of Election – In accordance with the *Code of Virginia, §24.2-611*, Officers of Election are sworn to "…perform the duties of this election according to the law and the best of my ability…" and "…studiously endeavor to prevent fraud, deceit, and abuse in conducting this election."

City Police/Sheriff –Coordinate with the Electoral Board to provide physical security and traffic control as required by exigent circumstances.

TABLE OF CONTENTS

I. Administrative Security Safeguards

A. *Security Risk Assessment*

Security Risks	Risk Impact
Tampering Loss/Theft Vandalism Improper Operations	Financial Loss Public Embarrassment Loss of Public Confidence Degraded Capability to Conduct Elections Breach of data in the Voter Registration System Breach of data in City of Lynchburg's Payroll/Personnel System
Specific Site/Operation	**Risk Evaluated and Managed**
Desktop Computers (4) General Use Laptops (3)	Physical Security Environmental Security Access Security Disaster Planning Operational Procedures and Guidelines

In order to ensure proper safeguarding of voting systems from evaluated risks:

1. All computers are to be operated only:
   - For their intended purposes
   - In accordance with approved procedures
   - With permission of the General Registrar or Electoral Board
   - All files with sensitive information are to be stored on the encrypted network drive and not on the disk drive of the computers.
2. In the event of an emergency, all computers should be safeguarded from risk using whatever means necessary and available at the time of the emergency.
3. In the event of an emergency and replacement devices are needed, the General Registrar's Office will coordinate with the City of Lynchburg IT Department to coordinate purchase of suitable equipment.
4. The Security Risk Assessment will be reviewed and documented annually, not later than 90 days before each November general election.

B. *Security Awareness and Training*

All staff in the office shall undergo background checks before assuming duties. Any and all access shall be granted at the discretion of the Electoral Board or General Registrar. All staff shall undergo security training and sign the *Oath of Confidentiality* before granted access to the Voter Registration Information System. The General Registrar or responsible party must notify ELECT (during working hours) within 4 hours of termination if voluntary, and 1 hour if involuntary, if the user has access to the Voter Registration Information System. The City of Lynchburg IT Department shall also be notified of the date and time network access should be revoked upon termination, and any changes to this date or time should be reported immediately. Any issued keys, badges, IDs, smart cards, or additional locality-provided property or resources shall be returned by the parting employee upon separation from the City of Lynchburg General Registrar's Office.

1. *Training*

Training Requirements	Standards
Basic/Refresher Training	• Prior to assumption of basic duties • Annually • May be combined with Election Official Training for all personnel • As required due to changes
Position Specific Training	• Prior to assumption of duties
Training Records	• Date/time of training • Written/signed acknowledgements
Training Review	• Updated as required • Annually (no later than 60 days before each November general election)

Dates of policy training and individuals trained will be recorded using the *Appendix A Computer Systems Security Training Record*.

Responsibility to adhere to the *Code of Virginia*, State Board of Elections policy and standards, and local Electoral Board procedures, is accepted when duties are assumed and approved by Electoral Board Members, the General Registrar, Deputy Registrar, and Assistant Registrars. Documentation of this acceptance is made upon signing the Constitutional Oath form and Oath of Confidentiality.

2. Disciplinary System

   See *Appendix G Disciplinary System for Employee Misconduct*. The City of Lynchburg Human Resources Department shall provide assistance to supervisors, managers, and employees in developing approaches to problems which first and foremost serve the City's interest and also the overall policy objective.

C. *Security Incident Handling*

Security is everyone's responsibility. Everyone is responsible for reporting and containing security incidents, to the best of their abilities based on the guidelines in this section, as soon as possible upon discovery of an incident.

1. *What Qualifies as an Information Technology Security Incident*

   An information technology security incident is an indication of attempted or successful unauthorized entry to a system, an information attack on a system or network, or a disclosure of sensitive information contained in an information system. Information technology security incidents include:

   - Attempted entry (failed or successful) to gain unauthorized access to a system or data; e.g., unauthorized scans and probes.
   - Unexplained disruption or denial of service.
   - Unauthorized use of a system for the processing or storage of data.
   - Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent (e.g., malicious logic such as virus, worm or a Trojan horse).
   - Poor security practices, such as exposure of passwords, etc.
   - A disclosure of sensitive information contained in a system.

2. *Incident Response*

   See *Appendix B Information Technology Security Incident Response Guidelines*

3. *Reporting Threats, Risk or Vulnerabilities*

Type of Incident	Reporting
Damage, Theft, Loss	All incidents require immediate action to minimize the effect. In the case of active theft, vandalism, fire, flooding, or other disaster, appropriate emergency services are to be notified. All incidents are to be reported immediately to the General Registrar who will direct further action to be taken appropriate to the incident. The General Registrar will report the incident to the Electoral Board members and the City of Lynchburg IT Department. For non-emergency incidents, the General Registrar will complete *Appendix B Computer Systems Incident Investigation and Analysis Report* and submit it to the Electoral Board members within 72 hours of notification of the incident.
Unauthorized access, intrusion into or alteration of hardware, firmware or software	
Unlawful or unauthorized use of system components	
Unlawful or unauthorized access to, disclosure, use or manipulation of sensitive or confidential data or private information	
Interruption of chain of custody, control or accountability	
Programming or function errors, or system failures that could affect or compromise the voter registrations system	
Gaps, lapses or inconsistencies in the implementation and enforcement of security mechanisms	

D. *Security Monitoring and Review Control*

Security monitoring and review will be conducted by the General Registrar and Electoral Board using state security standards, and documented on *Appendix C Computer Systems Security Review*. The review will assess compliance with security policy, standards, and procedures, verify consistent application of sound operational practices, maintain individual accountability, and support security incident analysis annually. The results will be sent to the Electoral Board and reviewed by August 1st.

Partial reviews of specific items designated by the Electoral Board will be conducted when changes occur and as part of incident after action reporting (see *Appendix B Computer Systems Incident Investigation and Analysis Report*).

E. *Security Contingency Planning*

1. *Security Chain of Command*
   The Electoral Board and General Registrar are the ultimate authorities regarding Computer Systems Security and will be consulted by staff and officers of election on all matters that pertain to the safety and integrity of the equipment. In the event that no member of the Electoral Board or the General Registrar can be contacted in a time reasonable to ensure safety and integrity of equipment, the senior Assistant Registrar present (or senior Election Official in a precinct) may act to stabilize the situation until the General Registrar and Electoral Board can be notified.

2. *Security Contingency Planning*
   The *Security Contingency Plan* shall be reviewed, tested, and documented annually. The annual testing may be by tabletop discussion, and is most effective when combined with annual security training for Officers of Election.

Situation	Actions & Responsibility
Short-Term Loss of Power	Each desktop computer should be connected to power through a short-term uninterruptible power supply, and on-board software utilized to facilitate an orderly shutdown of the computer system in the event of a longer-term power loss.
Long-Term Loss of Power	A generator will be utilized to maintain electricity in the event of a long-term loss of power.
Severe Weather	1. Call City Emergency Management in case of structural damage 2. Take steps to protect equipment 3. Call the City IT Department
Loss of Environmental Control	1. Call City Emergency Management 2. Take steps to protect equipment 3. Call the City IT Department
Loss of Physical Security Control	1. Call police 2. Call ELECT 3. Call the City IT Department
Physical Loss of Equipment – Theft	1. Call police 2. Call ELECT 3. Call the City IT Department
Physical Loss of Equipment – Disaster	1. Call Emergency Management 2. Take steps to protect remaining equipment 3. Call ELECT 4. Call the City IT Department

F. *Security Access Management*

Only the Electoral Board or General Registrar may approve access to computer systems and only personnel granted access to computers by the Electoral Board may have access to the computers. Permission to access the computers and support equipment will be documented in writing using *Appendix D Computer Systems Security Access List.* The *Computer Systems Security Access List* will provide a roster of authorized personnel by name. It will be maintained and updated by the General Registrar as personnel changes warrant. The Security Access List will be reviewed annually by the Electoral Board at least 60 days before each November general election. Anyone granted access to voting systems will be given security training based upon the Computer Systems Security Program Manual.

Security Access List General Guidelines

Position	Reason	Access Granted
Electoral Board Members	Ultimate responsibility for safeguarding the security of the voter registration systems.	Access as required for completion of reviews and investigations as designated by this document to include all General Registrar secure spaces.
General Registrar	Maintains day-to-day security of the computer systems and responsible for programming and testing of the voting systems for elections at the direction of the Electoral Board. Authorized Escort.	Access as required for completion of reviews and investigations designated by this document and to program, test, and conduct elections as directed by the Electoral Board.
Assistant Registrars	Assists the General Registrar as directed. On a case-by-case basis, may be a designated Authorized Escort.	Access as required for completion of duties assigned by the General Registrar.
IT Support	Install and test new programs, applications, computers and other devices. Maintain equipment.	Access as required for completion of duties assigned by the General Registrar.
All Other Employees, Temporary Hires, and Volunteer Election Officials	Performs duties as assigned by the General Registrar.	On a case-by-case basis, access as required for completion of assigned duties as determined by the General Registrar.

II. Physical Security

A. *Physical Access Control*

1. The computers utilized by the General Registrar's office are located behind the counter in the main office, Suite A of the Kemper Street Station. Physical security is provided by key access and a motion sensitive, monitored alarm system. Access is restricted to those individuals on the Access List, and City personnel and vendors with escort.

2. All visitors, vendors, and maintenance personnel must have written authorization from the Electoral Board or General Registrar to go behind the counter. They must present positive identification prior to admittance, enter their information legibly on the log, and must be accompanied by an individual designated as an Authorized Escort.

3. A record will be maintained of all individuals who have been granted access behind the counter, and this entry log will be reviewed by the Electoral Board quarterly or as appropriate. These will be scanned and stored on the network drive, and physical copies stored in accordance with locality record retention policies.

4. Individuals granted access to computer system and Voter Registration Information System are subject to successfully passing a background check prior to assumption of duties. Background checks of all staff shall be completed annually.

5. Information & Information System User Responsibilities:

    a. Accountable for keeping passwords confidential. Passwords must adhere to CIS standards of at least 15 characters in length.
    b. Accountable for activities performed under their user account and keeping personally identifying information (PII) confidential.
    c. Accountable for keeping any issued keys, badges, ID's, smart cards, etc. secure and not allowing others to borrow them.
    d. Responsible to report any suspicious activity.
    e. Required to return all locality provided property or resources on last working day before leaving.
    f. Responsible and accountable to comply with these responsibilities; any violation may result in administrative and/or disciplinary action, and potentially legal action.

6. In the event of an emergency or crisis that threatens the physical security of computers, the General Registrar, members of the Electoral Board, and the State Department of Elections are to be notified immediately.
7. All modifications and repairs to physical security system elements (e.g., walls, doors, locks, alarm systems, etc.) must be documented in the Configuration Management Database (CMDB) (see Section III.B. Configuration Management). Maintenance

8. In the event of discovery of an Information Technology Security Incident, see *Appendix B Information Technology Security Incident Response Guidelines*

B. *Environmental Control*

Each desktop computer should be connected to power through a short-term uninterruptible power supply, and on-board software utilized to facilitate an orderly shutdown of the computer system in the event of a longer-term power loss.

In the event of a longer-term power loss during regular business hours, the City of Lynchburg General Registrar’s office has a generator to restore power to facilitate the regular order of business until power can be restored to the area at large.

The department will submit an annual request to the City of Lynchburg Building Manager for inspection of power and network cabling for fraying or other wear, such as damage from water or pest infestation. The generator and UPS systems should also be inspected at this time for proper function. Testing of the generator should be scheduled ahead of time in order to minimize the impact upon daily business. Documentation of this inspection will be kept via closed work order submitted through the locality. General maintenance is completed through the City of Lynchburg Building Manager office.

In the event of large-scale disaster and access to the building is restricted or the structure is damaged, operations can be continued with temporary or replacement devices at the City of Lynchburg Public Library or the IT Building. The General Registrar should contact the IT Department to arrange this in the event of disaster.

III. Technical Safeguards

A. *Technical Access Control*

1. The computers utilized by the City of Lynchburg General Registrar's Office are hardwired into network. They cannot be accessed remotely except through IT installed and managed software. The computer systems are password protected and the City has a password management policy in effect. Connection to the network is managed via NAC protection (Network Access Control) and managed by the City of Lynchburg IT Department, effective November 2021.

2. All elections personnel have access to the voting systems with specific passwords, and to voter registration information systems with Multi-Factor Authentication (MFA). All password access to voting systems is terminated when an individual's employment is terminated or when the personnel no longer needs access. MFA setup for the voter registration information system is done directly with IT or General Registrar involvement.

B. *Configuration Management*

The City of Lynchburg General Registrar's office utilizes computer systems and programs managed by the City of Lynchburg IT personnel. Systems are monitored, and system scans and program updates are run regularly. Systems are either certified by the Commonwealth or are grandfathered in and align with the City of Lynchburg's Information Technology Security Policies. The General Registrar's Office will ensure that any programs that do not currently align with Department of Elections Minimum Security Standards meet or exceed state safety specifications or have a plan to come into compliance.

C. *Testing*

1. Symantec Endpoint Protection computer scan logs are captured and reported to the City IT Department automatically from the City's Symantec server, and any alerts are addressed with the General Registrar's Office.
2. Any irregularities or system security incidents are logged and investigated, and the locality will work with ELECT to reestablish system integrity in the event of critical failure.

D. *Network Security*

Information & Information System users are responsible to:

i. Use the computer systems for their intended purposes in accordance with approved procedures and with permission of the General Registrar or the Electoral Board.
ii. Be accountable for keeping passwords and sensitive information confidential.
iii. Be accountable for activities performed under their user account.
iv. Be accountable for not saving sensitive files onto the physical drive of the office computers to minimize risk of compromise of system integrity.
v. Be responsible and accountable to comply; any violation may result in administrative and/or disciplinary action, or legal action.
vi. Be responsible to report any suspicious activity.

IV. Audit and Accountability Policy

Computer systems are owned and maintained by the City of Lynchburg IT Department.

The City of Lynchburg IT Department monitors several major server systems with a rolling data limit of 90 days maximum. The City hopes to fund an event management/logging system upgrade (which will depend heavily upon federal and/or state grant availability) to accommodate up to 6 months of event log storage for all critical Lynchburg-managed server systems. Local logs and events for the City-supported administrative PCs in the General Registrar’s office are stored locally on the endpoints and can be reviewed by the elections office personnel as needed.

Any alerts from the computer systems are addressed with the General Registrar.

Appendix A – Computer Systems Security Training Records

<table>
<tr><th colspan="3">Initial Basic Training Record</th></tr>
<tr><td colspan="3"><b>By my signature I hereby acknowledge that I have received and understand the Basic Voting Systems Security Training, and that I understand my role in the safeguarding of the City of Lynchburg Registrar’s Office Computer Systems.</b></td></tr>
<tr><th>Date/Time</th><th>Name (Print)</th><th>Signature</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

Appendix A – Computer Systems Security Training Records

Refresher Training Record

By my signature I hereby acknowledge that I have received and understand the Voting Systems Security Refresher Training, and that I understand my role in the safeguarding of the City of Lynchburg Registrar’s Office Computer Systems.

Date/Time	Name (Print)	Signature

Appendix A – Computer Systems Security Training Records

Position Specific Training Record

By my signature I hereby acknowledge that I have received and understand the Voting Systems Security Training as it applies to my specific position, and that I understand my role in the safeguarding of the City of Lynchburg Registrar’s Office Computer Systems.

Date/Time	Name (Print)	Position	Signature

Appendix B – Information Technology Security Incident Response Guidelines

Email Phishing, Malware, or Ransomware

- If you receive a suspicious email, contact the City IT Help Desk at 401-HELP.
- If you opened a malicious file or clicked a malicious link, unplug and/or disconnect the device from the network as this will prevent it from spreading
- Do the Following:
    1. Take a screen shot of the email.
    2. Contact ***City of Lynchburg IT at 401-HELP***
    3. Contact the ***Virginia Fusion Center at 804-674-2196***
    4. If you have a VERIS account call the VERIS Helpdesk to immediately have your account disabled.
    5. If the email claims to be form a foreign nation or people claiming to represent foreign nations contact the Virginia Fusion Center
    6. DO NOT FORWARD THE EMAIL TO anyone else

If the Security Incident may have impacted access to VERIS, report the incident to ELECT:

NORMAL BUSINESS HOURS:

- Weekdays - 7AM – 6PM ET
    - All issues should be reported to the ELECT Systems Support team via telephone: 833-716-0001.
    - If unable to make contact or no callback is received within 15 minutes, please use the alternate contact listed below.
- NON-BUSINESS HOURS:
    - Weekends, Holidays and Weekdays - 6PM – 7AM ET Urgent/Major issues should be immediately reported to the ELECT Systems Support team via telephone: 804-593-2268. If unable to make contact or no callback is received within 15 minutes, please use the alternate contact listed below.
- ALTERNATE CONTACT:
    - Please contact the Virginia Fusion Center (VFC) via telephone at: 804-674-2196 or via email at vfc@vsp.virginia.gov.

City of Lynchburg IT Desk
434-401-HELP (4357)

VA Department of Elections general number
800-552-9745

US Department of State
OFM-Info@state.gov
202-895-3500

Appendix C – Computer Systems Incident Investigation & Analysis Report

(Use the reverse of the form for expanding comment areas)

Date ____________ Time ____________ Person Reporting ____________________

Type of Incident: ____

____

1. Who discovered the problem, and how was the problem found?

2. Who was notified?

3. What actions were taken to safeguard the integrity of the computer systems?

4. Were computer systems returned to normal operation? ☐ Yes ☐ No (Explain why not)

5. What follow up actions are recommended?

6. Have all follow up actions been completed? ☐ Yes ☐ No (Explain why not)

7. What lessons have been learned from this incident?

8. What steps are being taken to prevent this type of incident from recurring?

Completed by ____________________ ____________________ ____________________
Print Signature Date

Review:
General Registrar

____________________ ____________________
Signature Date

Electoral Board

Chairman ____________________ ____________________
Signature Date

Vice Chairman ____________________ ____________________
Signature Date

Secretary ____________________ ____________________
Signature Date

Appendix D – Computer Systems Security Review

(Use the reverse of the form for expanding comment areas)

Date		Reviewer	
1. What is the purpose for this review (i.e., annual, software change, etc.)			
2. What references were used?			
3. What specific items were audited?			
4. What problems were noted?			
5. What actions, if any, are required to correct deficiencies?			
6. What changes, if any, need to be made to training?			

Completed by ____________________ ____________________ ____________________
Print Signature Date

Review:
General Registrar

____________________ ____________________
Signature Date

Electoral Board

Chairman ____________________ ____________________
Signature Date

Vice Chairman ____________________ ____________________
Signature Date

Secretary ____________________ ____________________
Signature Date

Appendix E – Computer Systems Security Access List

Date	Name, Title and Organization	Type of ID Reviewed	System to which Access Granted	Authorized by	Authorized Escort

Appendix F – Computer Systems Security Training Plan

Basic and Refresher Training

I Responsibility

Security and integrity of computer systems is a shared responsibility among all personnel, contractors, and volunteers

Must consistently implement security safeguards, abide by security standards, and maintain associated documentation

Must report security issues and incidents

Must take action to safeguard voting systems in emergencies

II Review & Monitoring

Elections personnel can and will be reviewed and monitored

III Legal Requirements

Protecting Voting Systems

IV Components

Identification of computer systems, programming, system information, voter information, votes, results or other data about which there are restrictions as to their use, disclosure, distribution or duplication, as well as privacy and confidentiality expectations required of personnel

V Potential Threats, Risks, Vulnerabilities

VI Written Instructions for Security

VII Written Instructions for Operations

Appendix G – Computer Systems Security Policy Statement for the Public

The City of Lynchburg Electoral Board considers the safeguarding of the voter registration computer systems as paramount to keeping the public trust in the election process. In order to preserve that integrity, the Computer Systems Security Program has been implemented and in general terms consist of the following:

- Comprehensive Risk Assessment and Mitigation Planning
- Documented Security Awareness and Training for all Registrar Office staff members, including Electoral Board Members, General Registrar, Deputy Registrar, Assistant Registrar(s), Officers of Election, Voting Machine Technicians, and any other employees, vendors, and volunteers who perform tasks associated with the voting systems.
- Policy and Procedure Monitoring and Review
- Physical Access and Environmental Control and Monitoring
- Technical Access Control, Configuration Management, Testing and Security

Appendix H – Disciplinary System for Employee Misconduct

The City of Lynchburg Electoral Board will make use of the City of Lynchburg Human Resources policy for employee misconduct as it relates to the computer systems security program. An updated policy can be found at Employment Policies & Procedures | City of Lynchburg, Virginia (https://www.lynchburgva.gov/employment-policies-procedures)