



## Purpose

This document provides the Voter Photo ID software application (Software Application) users with requirements to secure the data of the Voter Photo ID software application while offsite.

## Scope

This policy shall apply to any Voter Photo ID software user and device that processes voter photo ID cards outside of a secure location (Registrar's Office).

## Background

The offline version of the Software Application stores the voter data collected directly on the computer of the user processing the voter photo ID card. This data includes the first and last name, date of birth, last four digits of the applicant's social security number (SSN4), signature, and photo. The first and last name, date of birth, and SSN4 data elements are encrypted and all data elements are saved in a secure location on the user's device.

Once the user logs into the Software Application while online, any data stored on the device while offline will automatically be transmitted to the Department of Elections' database (for automatic processing), then completely removed from the device.

This local storage of sensitive data on a portable device, outside of a secure office location, requires that users of offline functionality procure and install an additional layer of encryption. See the [Vendor Solutions](#) for recommended software options and contact information.

## Offsite Recommendations

Whenever possible, users should run the Software Application over a secure, online network connection. The following options for offsite use of the Software Application are listed in order of preference based on providing the highest level of security:

1. online by connecting with VPN to your local network
2. online with a static IP address on a wireless card
3. offline

## Security Requirements

When using the Software Application offline and offsite:

1. A second layer of encryption is required to protect data in the event the first layer of encryption is compromised.
2. Physical security of the device is required, such as a cable lock, to secure the device to a larger, heavier object, to prevent theft of the device itself.



## Vendor Solutions

Either **Symantec Drive Encryption** or **McAfee Total Protection** is required to be installed and operational on any machine pre-designated to process voter photo ID applications in the offline mode. Users can procure these software solutions through SHI International Corporation.

SHI International Corp.	Title	Name	Email Address
290 Davidson Ave	Account Executive	Erik Schroeder	erik_schroeder@SHI.com
Somerset NJ 08873	Account Manager	Patrick Jaron	Pat_Jaron@SHI.com
888-235-3871			

## Definitions

**Encryption** - The transformation of information into a form that is impossible to read unless you have a specific piece of information, which is usually referred to as the “key.” The purpose is to keep information private from those who are not intended to have access to it. To encrypt is essentially about making information confusing and hiding the meaning of it.

**Sensitive Data** - The classification of data defined by COV that is required to be protected by applicable law or statute, or which, if disclosed to the public could expose the Commonwealth to legal or financial obligations; and specifically (i) more than four digits of a social security number or other unique identifier other than voter identification number; (ii) day and month of birth; or (iii) the residence address of voters qualified for protection under § 24.2-418 of the Code of Virginia.

## Authoritative References

- Virginia Administrative Code / 1VAC20-20-20. Electronic Transmission of Records Containing Sensitive Personal Information; Encryption or Redaction Required
- Code of Virginia Title 2.2. Chapter 38 – Government Data Collection and Dissemination Practices Act
- Code of Virginia § 18.2-186.6. Breach of personal information notification
- Code of Virginia § 24.2-103. Powers and duties of local Elections Boards and General Registrars
- VITA CSRM IT System and Communications Encryption Policy v1.0; revised 07/01/2014
- ITRM SEC501-08; 04/03/2014 / AC-3 Access Enforcement, related controls SC-8, SC-9, SC-13
- COV ITRM Guideline SEC507-00: Information Technology Data Protection Guideline

## Revision History

2014-08-29 – Initial policy created.