VVSG 2007 Physical Security Requirements

This information is based on the requirements found at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

5.8 Physical Security for Voting Devices

The objective of the voting device physical security measures is to prevent undetected, unauthorized physical access to voting devices. It is assumed that adversaries have financial resources, technical savvy, and possibly insider presence to exploit vulnerabilities within voting devices. When in use, the physical security required for voting devices is relatively low compared to other types of moderate or high impact systems. Though voting areas should be private enough to maintain a voter's right to a secret ballot, the machines are generally not isolated. An attempt to physically open or disassemble a machine would likely not go unnoticed by poll workers. Similarly, a plot to tamper with the machines after the polls are closed would require a large conspiracy amongst poll workers, as an individual working alone would likely be noticed gaining access to machines outside of normal operating procedures. Voting devices also spend a considerable amount of time in storage or otherwise secured by means that could afford "open" though unauthorized access by well placed insiders. In that case, time and privacy are on the side of the adversary. One could not hope to stop an adversary from gaining access to the machine but one can hope to find evidence of their handiwork.

The effectiveness of all technical security safeguards is based, in part, on the assumption, either explicit or implicit, that all components have adequate physical security protection. Any unauthorized physical access must leave physical evidence that an unauthorized event has taken place.
This section outlines physical security requirements for voting devices both in use and in storage. It does not address the physical characteristics of polling places. It details countermeasures to be implemented by manufacturers in order to ensure the physical integrity of the voting devices.

5.8.1 Unauthorized physical access

5.8.1-A Unauthorized physical access requirement

Requirement:	Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Manufacturer may provide for and recommend a combination of procedures and physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation such as a system that relies on tamper evidence tape or tags coded with consecutive serial numbers. This requirement extends [VVSG2005] I.7.3.1 by requiring that any tampering with a device leave physical evidence. [VVSG2005] I.7.3.1 states that any tampering should be detectable using manufacturer-specified procedures and measures.
Source:	[VVSG2005] I.7.3.1-2
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence.

	Justification: This requirement directly aligns with this guideline.

5.8.1-B Unauthorized physical access capability requirement

Requirement:	Voting devices SHALL produce an audible and visual alarm if access to a restricted voting device component is gained during the Activated state.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with this guideline.

5.8.2 Physical port and access least functionality

5.8.2-A Physical port and access point requirement

Requirement:	The voting device SHALL only have physical ports and access points that are essential to voting operations and to voting device testing and auditing.
Applies to:	Voting device
Test Reference:	Part 3:4.3 “Verification of Design Requirements”
Discussion:	Examples of essential voting operations include voting machine upgrades and maintenance. Examples of physical ports are USB ports, floppy drives and network connections. Examples of access points are doors, panels and vents.
Source:	[VVSG2005]
Principle(s)/ Guideline(s):	*Security: Physical Security* The voting system prevents or detects attempts to tamper with voting system hardware. **Justification:** Principle Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing. **Justification:** This requirement directly aligns with this guideline.

5.8.3 Voting device boundary protection

5.8.3-A Physical port shutdown requirement

Requirement:	If a physical connection between voting device components is broken during Activated or Suspended State, the affected voting machine port SHALL be automatically disabled.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”

Discussion:	
Source:	[VVSG2005]
Principle(s)/ Guideline(s):	*Security: Physical Security* The voting system prevents or detects attempts to tamper with voting system hardware. **Justification:** Principle

5.8.3-B Physical component alarm requirement

Requirement:	The voting device SHALL produce an audible and visual alarm if a connected component is disconnected during the Activated state.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005]
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with this guideline.

5.8.3-C Physical component event log requirement

Requirement:	An event log entry that identifies the name of the affected device SHALL be generated if a voting device component is disconnected during the Activated state.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005]
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records **and other election artifacts (e.g. logs)** that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement directly aligns with this guideline.

5.8.4 Information flow

5.8.4-A Physical port restriction requirement

Requirement:	Voting devices SHALL be designed with the capability to restrict physical access to voting machine ports that accommodate removable media, with the exception of ports used to activate a voting session.
Applies to:	Voting device
Test Reference:	Part 3:4.3 “Verification of Design Requirements”
Discussion:	Floppy, CD or DVD drives and memory cards might be essential to voting operations during Pre-voting and Post-voting phases of the voting cycle such as machine upgrade, maintenance and testing. Therefore, they should be accessible only to authorized personnel. They should not be accessible to voters during

	Activated and Suspended phases of the voting cycle. It is paramount that the floppy, CD and DVD drives are not accessed without detection. The Manufacturer may provide for and recommend a combination of procedures and physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation, such as a system that relies on tamper resistant tape or tags coded with consecutive serial numbers.
Source:	[VVSG2005]
Principle(s)/ Guideline(s):	*Security: Physical Security* Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing. **Justification:** This requirement directly aligns with these guidelines.

5.8.4-B Physical port tamper evidence requirement

Requirement:	Voting devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.
Applies to:	Voting device
Test Reference:	Part 3:4.3 “Verification of Design Requirements”
Discussion:	Manufacturer may provide for and recommend a combination of procedures and physical measures that allow election officials to monitor and control access points such as a system that relies on tamper resistant tape of tags coded with consecutive serial numbers. This requirement extends [VVSG2005] I.7.3.1 by requiring that tampering with device ports or access points leave physical evidence. [VVSG2005] I.7.3.1 states that any tampering should be detectable using manufacturer-specified procedures and measures.
Source:	[VVSG2005] I.7.3.1-2
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with these guidelines.

5.8.4-C Physical port disabling capability requirement

Requirement:	Voting machines SHALL be designed such that physical ports can be manually disabled by an authorized administrator.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005]
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system authenticates administrators, users, devices and services before granting access to sensitive functions. ***Justification:*** *Security: Physical Security*

	Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing. **Justification:** This requirement directly aligns with these guidelines.

5.8.5 Door cover and panel security

5.8.5-A Door cover and panel security requirement

Requirement:	Access points such as covers and panels SHALL be secured by locks or tamper evidence or tamper resistance countermeasures SHALL be implemented so that system owners can monitor access to voting device components through these points.
Applies to:	Voting device
Test Reference:	Part 3:4.3 "Verification of Design Requirements"
Discussion:	
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing. **Justification:** This requirement directly aligns with these guidelines.

5.8.6 Secure ballot box

5.8.6-A Secure ballot box requirement

Requirement:	Ballot boxes SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing", 4.3 "Verification of Design Requirements"
Discussion:	The goal here is to ensure that poll workers or observers would easily notice if someone has tampered with the ballot box. This requirement can be achieved through locks or seals as a part of tamper evidence and tamper resistance countermeasures described by the use procedures and supplied by the manufacturer.
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with this guideline.

5.8.7 Secure physical lock and key

5.8.7-A Secure physical lock strength requirement

Requirement:	Voting devices SHALL only make use of locks installed for security purposes that have been evaluated to the listing requirements of UL 437 for door locks and locking cylinders or higher.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	See [UL03] for UL listing requirements.
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with these guidelines.

5.8.7-B Secure physical lock access requirement

Requirement:	Voting devices SHALL be designed with countermeasures that give a physical indication that unauthorized attempts have been made to access locks installed for security purposes.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with this guideline.

5.8.7-C Secure locking system key requirement

Requirement:	Manufacturers SHALL provide locking systems for securing voting devices that can make use of keys that are unique to each owner.
Applies to:	Voting device
Test Reference:	Part 3:Chapter 4: “Documentation and Design Reviews (Inspections)”
Discussion:	Voting device owners are the individuals accountable for purchasing, maintaining and/or operating the voting devices. They may work at the State level or at a local level. Election officials may want keying schemes that are more or less restrictive in accordance with their election management practices. The requirement does not mandate a unique key for each piece of voting equipment, but requires manufacturers to be able to provide unique keys for the voting equipment per the requests of election officials. System owners must establish procedures for issues such as key reproduction, use and storage.
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* The voting system prevents or detects attempts to tamper with voting system hardware. **Justification:** This requirement directly aligns with the principle itself.

5.8.8 Physical encasing lock

5.8.8-A Physical encasing lock access requirement

Requirement:	Locks installed for purposes other than security SHALL NOT, if bypassed, compromise the security of a voting device.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Locks on voting devices may be used to secure access points such as doors and panels or they may be used simply to fasten a segment of the voting device’s encasement. In the former case, testing labs must verify that the lock does indeed provide a measure of security. In the latter case, the testing lab must verify that bypassing the lock does not put the security of the system in jeopardy.
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* The voting system prevents or detects attempts to tamper with voting system hardware. **Justification:** This requirement directly aligns with the principle itself.

5.8.9 Power supply

5.8.9-A Back-up power requirement

Requirement:	Any physical security countermeasures that require power supplies SHALL have a back up power supply.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005]
Principle(s)/ Guideline(s):	*General: High Quality Construction* Handle errors actively and appropriately, recovering from failure gracefully – processing or avoiding well-known errors and/or software bugs; and avoiding single points of failure that could cause complete loss of voting capabilities. **Justification:**

5.8.9-B Power outage alarm

Requirement:	A physical security countermeasure that switches from its primary power supply to its back-up power supply SHALL give an audible and visual alarm.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	
Principle(s)/ Guideline(s):	*General: High Quality Construction* Handle errors actively and appropriately, recovering from failure gracefully – processing or avoiding well-known errors and/or software bugs; and avoiding single points of failure that could cause complete loss of voting capabilities. **Justification:**

	Security: Physical Security Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with these guidelines.