Principle 12
Physical Security
The voting system prevents or detects attempts to tamper with voting system hardware.

Requirements for Principle 12
Principle 12 Physical Security The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.1-A – Unauthorized physical access
12.1-B – Unauthorized physical access alarm
12.1-C – Disconnecting a physical device
12.1-D – Logging of physical connections and disconnections
12.1-E – Logging door cover and panel status
12.1-F – Secure containers
12.1-G – Secure physical locks
12.1-H – Secure locking system key
12.1-I – Backup power for power-reliant countermeasures

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

12.2-A – Physical port and access least functionality
12.2-B – Physical port auto-disable
12.2-C - Physical port restriction
12.2-D – Disabling ports
12.2-E – Logging enabled and disabled ports
12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.1-A – Unauthorized physical access
Any unauthorized physical access must leave physical evidence that an unauthorized event has taken place.

**Discussion**
Access points such as covers and panels need to be secured by locks or other mechanisms that leave physical evidence in case of tampering or unauthorized access. Manufacturers can 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 evident tape, seals, or tags coded with consecutive serial numbers. Other systems might use seals incorporating radio frequency identification devices with physically unclonable functions or other technology in the future.

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.

Prior VVSG Source: VVSG 1.0 7.3.1

12.1-B – Unauthorized physical access alarm
Voting devices must produce an alarm if access to a restricted voting device component is detected during the activated state.

**Discussion**
This alarm is meant to call attention to election workers in the polling place.

12.1-C – Disconnecting a physical device
The voting device must produce an alarm if a connected component is physically disconnected during the Activated state.

**Discussion**
Examples of connected components include printers, removable storage devices, and mechanisms used for networking. If a token is necessary for normal operation, such as a memory card or other device granting a voter access to the voting system, it is not necessary to trigger the alarm.

12.1-D – Logging of physical connections and disconnections
The voting system must log when a voting device or component is connected or disconnected during the Activated state.
**Discussion**
Logging of the devices is vital for determining cause and providing incident information if a physical security event occurs.

Related requirement: Aligns with 15.1, Detection and Monitoring

**12.1-E – Logging door cover and panel status**
The voting system must log the status (for example, open, closed) of physical access points, such as covers and panels, upon boot of the system.

**Discussion**
This ensures system owners can monitor access to voting device components whenever they are being used on election day. The status of the open physical access points can be externally monitored and communicated to the voting device itself.

Related requirement: Aligns with 15.1, Detection and Monitoring

**12.1-F – Secure containers**
Unauthorized physical access to a container holding voting system records must result in physical evidence that an unauthorized event has taken place.

**Discussion**
The goal is to ensure that election workers or observers would easily notice if someone has tampered with the container. 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.

Additionally, to support the auditable principle, containers which hold either paper or electronic voting system records needed for audits need to be secure against physical access.

**12.1-G – Secure physical locks**
Locks installed in voting devices for security purposes must be:

1. evaluated and meet or exceed requirements of UL 437 for door locks and locking cylinders.
2. designed with countermeasures that give a physical indication that unauthorized attempts have been made to defeat the lock and gain access to the voting device.

**Discussion**
See [UL03] for UL listing requirements.

External source: UL 437
12.1-H – Secure locking system key

The voting system must support locking systems for securing voting devices that are flexible enough to support different keying schemes, including a scheme that can make use of keys that are unique to each owner.

Discussion

The use of a single key used to unlock thousands of precinct-based voting devices makes for a challenging security situation, as copies of this single key design are distributed to a large number of individuals. This creates a situation in which the key can be easily lost or stolen, and subsequently copied. At the same time, this situation does make key management significantly easier for election officials. To alleviate this situation, election officials might want keying schemes that are more or less restrictive in accordance with their election management practices and needs. This system can make use of replicable locks or cylinders, mechanisms which allow for rekeying of locks, or other technologies. 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 if requested by election officials. System owners need to establish procedures for issues such as key reproduction, use, and storage.

12.1-I – Backup power for power-reliant countermeasures

Any physical security countermeasure that requires power must have a backup power supply. In addition, switching from primary power supply to backup power supply:

1. produces an alarm, and
2. generates an event log entry.

Discussion

This ensures that the countermeasure isn’t disabled or intentionally circumvented by a power failure.

Switching to the backup power supply triggers an alarm that alerts an election worker to the issue so that any problem can be further diagnosed and eventually resolved. The alarm can be visible and audible.

The log entry information is security relevant, especially once a security incident has occurred, and would be useful when determining cause. Alternatively, the voting system should log when there is a switch from backup power to the primary power supply.

Applies to: Voting Device, EMS
Prior VVSG Source: VVSG 2007 5.8.9-A, VVSG 2007 5.8.9-B
Related requirement: Aligns with 15.1, Detection and Monitoring

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.
12.2-A – Physical port and access least functionality
The voting device must only have physical ports and access points that are essential to voting operations, testing, and auditing.

Discussion
Examples of ports are USB and RJ45 physical network interfaces. Examples of access points are doors, panels, and vents. Voting operations include voting device upgrades and maintenance.

Prior VVSG Source: VVSG 2007 5.6.3-C

12.2-B – Physical port auto-disable
If a physical connection between voting device components is broken during an activated or suspended state, the affected voting device port must be automatically disabled.

Discussion
Automatically disabling will require an election worker’s attention to re-enable and re-attach any network or power cabling. Under ideal circumstances, the specific election worker performing maintenance is uniquely identified within the logs, but this is not required.

12.2-C - Physical port restriction
Voting systems must restrict physical access to voting machine ports that accommodate removable media, with the exception of ports used to activate a voting session.

Discussion
Although voting systems can have ports dedicated to voting operations outside of election day activities, those ports need not be exposed while balloting is in progress. Removable media (such as Floppy, CD or DVD drives, thumb 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, all removable media 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 essential that any removable drives, whether or not they are used by the system, are not accessed without detection.

Related requirements: Aligns with 14.2, System Integrity

12.2-D – Disabling ports
Voting devices must allow authorized administrators to be able to put physical ports into a disabled state.

Discussion
Logically disabling ports prevents unused ports from being used as a staging point for an attack on the voting system.
12.2-E – Logging enabled and disabled ports

An event log entry that identifies the name of the affected device must be generated when physical ports are enabled or disabled.

**Discussion**

Whether a port is disabled or not is security relevant, especially once a security incident has occurred, and this information would be useful when determining cause. 12.2-D applies to physical restrictions, whereas 12.2-F discusses logical disabling of ports.

Applies to: Voting Device, EMS
Related requirements: Aligns with 9.3, Access Control and 15.1, Detection and Monitoring