DEPARTMENT OF CORRECTIONS

Information Technology Services

Title:	**Removable Media Policy**	**DOC Policy: 60.3.2**
Effective:	**8/5/22**	**Supersedes: Renumbered from 60.1.8 dated 9/6/19**
Applicability:	**All employees, volunteers, and contract services providers**	
Directives Cross-Reference:	**Information Security Incident Management—60.6.3**	
Attachments:	**None**	

I. PURPOSE

The purpose of this policy is to establish acceptable use procedures, standards, and restrictions for the use of removable media connected to any Department of Corrections (DOC) computing device that the department hosts or maintains.

II. DEFINITIONS

A. Data: Information in raw or unorganized form that refers to or represents conditions, ideas, or objects.

B. Data-At-Rest: Inactive data not actively moving from computing device to computing device or network to network.

C. Data-In-Transit: Data is actively moving from one location to another such as across the Internet or through a private network.

D. Decryption: The process of transforming data that has been rendered unreadable through encryption back to its original form.

E. Department Computing Devices: All electronic information devices, interconnections, and technical information of the department. Examples of systems include, but are not limited to:

1. Computers, printers, copiers, recorders, transmitters, data telecommunications connections and any similar connected devices.
2. All portable devices such as cell phones, smart phones, tablets, MP3 players, and any other devices as defined by the department
3. Networking devices includes routers, switches, VPN concentrators, or any device interconnecting networks.

4. Large scale information systems which provide services to the department such as logon access, file servers, data warehousing, web access, web hosting, mail, and instant message services.
5. Applications such as Corrections Information System (CIS), Integrated Supervision Information Systems (ISIS), CIS (DOC 400), or any other systems accessed by or through these systems or systems devices. Methods include, but are not limited to, the internet, Internet Service Providers (ISP) and DOC hosted connections.

F. Encryption: The use of a mathematical process to transform information to make it unreadable for unauthorized users.

G. Information: Information is data or knowledge that is transmitted, analyzed, edited, or reproduced in department systems by electronic, printed, written, verbal or media transmission means. Examples include, but are not limited to:

1. Documents, reports, statistics, files, records, compiled or stored on DOC computing devices or applications.
2. E-mails or messaging system conversations and their attachments.
3. Audio and video files.
4. Images, graphics, pictures, and photographs.
5. Programs (such as CIS (DOC 400), ISIS, WebLEDS, etc.), software, and macros.
6. Text and data

H. Removable Media: Any storage device that can be portable, accessible, connected to any computing device with the ability to process the contents held on that media. Examples include but are not limited to:

1. USB-based memory sticks.
2. Removable memory cards in any format (Secure Digital, Multimedia, Compact Flash).
3. Portable audio/media players that internally or externally supports data storage.
4. Cell phone handsets, smartphones with internal or hard drive-based memory.
5. Digital cameras with internal or external memory support.
6. Removable memory-based media such as writable or re-writable DVDs, CDs, or floppy disks.

I. Personal Identification Number (PIN): A sequence or pattern of characters (letters, numbers, special symbols) used to validate access to a device or application.

III. Policy

A. Removable Media Acquisition

1. All removable media used on any DOC computing device must be purchased through the department's acquisition process.

2. Once purchased and received, the media must be registered by the Information Security Office or local Technology Support Analyst (TSA) and scanned for possible embedded malware.
3. Once scanned, the local TSA must email the serial number of the thumb drive to the ITS Security office email: dlitssecurity@doc.state.or.us
4. All removable media recipients must complete a CD 1489, Employee Property Tracking Form and return it to the responsible business unit for placement in the user's working personnel file. If the employee has a CD 1489 on file, they are required to provide updates to it as necessary.

B. Removable Media and Data Security

1. Department employees must ensure security of all assigned removable media. When not in use, all portable and removable media must be reasonably secure and protected from theft, tampering, or destruction.
2. Information stored on any removable media must be protected at the highest level of data classification requirements.
3. Any form of password (text, Personal Identification Number, etc.) used for encrypting removable media must comply with current department standards and be known only to the authorized user.
4. Passwords housed on removable media must be encrypted except when in use and must comply with current department standards and be based on the asset and data classification level of the system where the password is used.
5. Level 4 data as defined in the DOC Records Retention and Information Security Classification Schedule shall not be stored on removable media.
6. Department-owned removable media shall not be removed from department premises or property, except for department business.
7. Department-owned removable media shall not be connected to personally owned devices under any circumstances.
8. Personally owned removable media shall not be connected to any department computing device, under any circumstance.
9. All DOC-owned removable media requires an annual inventory to ensure proper control and maintenance.

C. Third-Party owned Removable Media Connecting to Department Computing Devices

1. Third-party (non-departmental staff) removable media shall not be connected to the department's network without explicit consent of the Department Chief Information Officer, Information Security Officer (ISO), or a designated representative.
2. Media must be scanned by the department ISO, TSA, or designated representative before connecting to any department computing device.

3. Before exiting any department facility, third-party removable media must be reviewed by the ISO, TSA, or designee to ensure no data has been removed from department computing devices or network resources without authorization.

D. Information Security Incident Management

1. When department-owned removable media is lost or the owner becomes aware that it may be stolen, they must report the incident to their functional unit manager, their site TSA, and the Information Security office via email immediately.
2. Once reported, a security investigation should be initiated in accordance with DOC policy 60.6.3, Information Security Incident Response.

E. Removable Media Disposal

1. When department-owned removable media is no longer needed, it must be returned to either the functional unit manager or local TSA.
2. Once returned, staff must fila an updated CD 1489, Employee Property Tracking Form annotating the return of the removable media.
3. Technical Support staff must sanitize all returned removable media prior to reissue.
4. Technical Support staff will sanitize then ship all removable media to the Information Security team for removal from inventory.

IV. IMPLEMENTATION

This policy will be adopted immediately without further modification.

Certified: _signature on file_____
Julie Vaughn, DOC Rules Coordinator

Approved: _signature on file_____
Heidi Steward, Acting Director