# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## MP: Media Protection

### MP-1: Media Protection Policy And Procedures

The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency].

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for media protection controls as the system is entirely within the AWS Cloud boundary.

##### CivicActions

CivicActions has developed, documented and disseminated to personnel a media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls. This information is maintained in CivicActions Media Protection (MP) Policy and Procedure document that can be found in the CivicActions Github repository at <https://github.com/CivicActions/compliance-docs>.

### MP-2: Media Access

The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for media protection controls as the system is entirely within the AWS Cloud boundary.

### MP-6: Media Sanitization

The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for media protection controls as the system is entirely within the AWS Cloud boundary.

### MP-7: Media Use

The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for media protection controls as the system is entirely within the AWS Cloud boundary.