# 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].

**Status:** Complete

**Summary:** Fully inherited from AWS (FedRAMP).

##### AWS

This Media Protection control associated with hardware components within AWS is generally either partially or fully inherited from the AWS physical infrastructure, while the customer organization is responsible for any part of the control that is applicable to customer-controlled equipment and facilities, and the customer’s configurable portion of the AWS logical infrastructure, including the Operating systems on Amazon EC2 instances and the customer’s applications.

For the U.S. East, U.S. West, and GovCloud regions, this control is inherited from pre-existing Agency Authority to Operate (ATO) or JAB provisional Authority to Operate under the Federal Risk and Authorization Management Program (FedRAMP).

Refer to the AWS FedRAMP SSP artifacts, including the Control Implementation Summary and Customer Responsibility Matrix, available from the AWS Compliance Team. http://aws.amazon.com/compliance/fedramp/

##### 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>.

##### Project

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog. Media protection policy and procedures are fully inherited from AWS Cloud.

### 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].

**Status:** Complete

**Summary:** Fully inherited from AWS (FedRAMP).

##### AWS

This Media Protection control associated with hardware components within AWS is generally either partially or fully inherited from the AWS physical infrastructure, while the customer organization is responsible for any part of the control that is applicable to customer-controlled equipment and facilities, and the customer’s configurable portion of the AWS logical infrastructure, including the Operating systems on Amazon EC2 instances and the customer’s applications.

For the U.S. East, U.S. West, and GovCloud regions, this control is inherited from pre-existing Agency Authority to Operate (ATO) or JAB provisional Authority to Operate under the Federal Risk and Authorization Management Program (FedRAMP).

Refer to the AWS FedRAMP SSP artifacts, including the Control Implementation Summary and Customer Responsibility Matrix, available from the AWS Compliance Team. http://aws.amazon.com/compliance/fedramp/

### 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.

**Status:** Complete

**Summary:** Fully inherited from AWS (FedRAMP).

##### AWS

This Media Protection control associated with hardware components within AWS is generally either partially or fully inherited from the AWS physical infrastructure, while the customer organization is responsible for any part of the control that is applicable to customer-controlled equipment and facilities, and the customer’s configurable portion of the AWS logical infrastructure, including the Operating systems on Amazon EC2 instances and the customer’s applications.

For the U.S. East, U.S. West, and GovCloud regions, this control is inherited from pre-existing Agency Authority to Operate (ATO) or JAB provisional Authority to Operate under the Federal Risk and Authorization Management Program (FedRAMP).

Refer to the AWS FedRAMP SSP artifacts, including the Control Implementation Summary and Customer Responsibility Matrix, available from the AWS Compliance Team. http://aws.amazon.com/compliance/fedramp/

### 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].

**Status:** Complete

**Summary:** Fully inherited from AWS (FedRAMP).

##### AWS

This Media Protection control associated with hardware components within AWS is generally either partially or fully inherited from the AWS physical infrastructure, while the customer organization is responsible for any part of the control that is applicable to customer-controlled equipment and facilities, and the customer’s configurable portion of the AWS logical infrastructure, including the Operating systems on Amazon EC2 instances and the customer’s applications.

For the U.S. East, U.S. West, and GovCloud regions, this control is inherited from pre-existing Agency Authority to Operate (ATO) or JAB provisional Authority to Operate under the Federal Risk and Authorization Management Program (FedRAMP).

Refer to the AWS FedRAMP SSP artifacts, including the Control Implementation Summary and Customer Responsibility Matrix, available from the AWS Compliance Team. http://aws.amazon.com/compliance/fedramp/