System Security Plan (SSP) for closed out projects

Purpose:

The purpose of a system security plan (SSP) is to outline the management, operational, and technical safeguards or countermeasures prescribed for an information system involved with controlled unclassified information (CUI) when the project has been closed out.

Instructions:

The Principal Investigator (PI), or designee, shall submit the SSP immediately after the close of the project or work.

Once all sections of the SSP, including the Minimum Security Controls table are completed, the PI(s) should date and sign the document, and submit to Cyber Security at cui@security.gatech.edu for review.

Contents

System Security Plan (SSP) for closed out projects

SSP Revision Number	

Project Summary

Please complete the information below.

People Soft Fund Number	
Primary Sponsor	
Project Title	
Principal Investigator	
Campus Unit / Laboratory / Center	

Disposition of CUI

An explanation of what data (CUI) was involved in the project and the disposition of this data at the end of these activities

System Environment

For all CUI retained after the close of the work, detail all:

- Physical location(s)
- Storage location(s) to include all applicable media and cloud services.
- If a cloud service has been used, what steps have been taken to ensure the data is not being synced to systems where it is no longer needed?

Minimal Security Controls

Describe how your storage environment(s) meet the basic and derived security requirements.

Control Number	Control Name	Control Description	Description of how control is met.	Control Met? (Y/N)	Central Service Used? (Y/N)
3.8 MEDIA PROTECTION					
Basic Security Requirements					
3.8.1	Media Access	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.			
3.8.3	Media Sanitization	Sanitize or destroy information system media containing CUI before disposal or release for reuse.			
Derived Security Requirements					
3.8.8	Media Use	Prohibit the use of portable storage devices when such devices have no identifiable owner.			
3.8.9	Information System Backup	Protect the confidentiality of backup CUI at storage locations.			

Approvals

Approved By: ____ Approval Date: __________
Insert Approver Title

Approved By: ____ Approval Date: __________
Insert Approver Title

Approved By: ____ Approval Date: __________
Insert Approver Title

This is a Georgia Institute of Technology internal document. Unauthorized disclosure of this document outside the Institute for any purpose is strictly forbidden.