



**Georgia Institute
of Technology**

Georgia Tech System Security Plan Exception Temporary GT SSP Exception

Overview

This System Security Plan (SSP) Exception has been developed and will be used to protect all systems storing and processing CUI and thus requiring compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204.7012 *Safe Guarding Defense Information and Cyber Incident Reporting*.

Purpose

This document outlines the management, operational, and technical safeguards or countermeasures approved by the Institute for meeting the requirements for an information system or storage location/device involved with CUI. Deviations will be documented and will require the approval of the Primary Investigator (PI).

This document serves as a temporary addendum to an established SSP in times that PI or researchers are forced to adjust their operations from the established SSP.

Instructions

The Principal Investigator, or designee, shall submit the temporary SSP exception form for approval.

The Controls

The SSP NIST 800-171 Controls Form lists each control, the control family, the control text and the approved solution for each of the 110 controls. These approved solutions are offered as centrally supported services. In situations where the approved solution is not possible or appropriate for your system, the compliance team will work with you to identify an approved mitigation. All mitigations will be filed as a supplemental SSP to the standard SSP. Both will require the signature of the Principal Investigator. If utilizing an approved central solution, no action is needed.

Contents

Overview.....	1
Purpose.....	1
Instructions.....	1
The Controls.....	1
Project Summary.....	4
Project Information.....	4
Description of research/work/project.....	5
Description of CUI.....	5
Systems Inventory.....	6
NIST 800-171 Controls Form.....	7
Plans of Action and Milestones (POA&Ms).....	Error! Bookmark not defined.
Barriers to Compliance.....	Error! Bookmark not defined.
Approvals.....	10

Project Summary

Please complete the information below.

Project Information

Prime Award Number			
Document ID			
Primary Sponsor			
Project Title			
Principal Investigator			
Name/Role of Users Working On This Project	<i>Full Name</i>	<i>Role</i>	<i>Login Accounts Used</i>
Physical Location(s)			
Project IT Contact			
Contracting Officer			

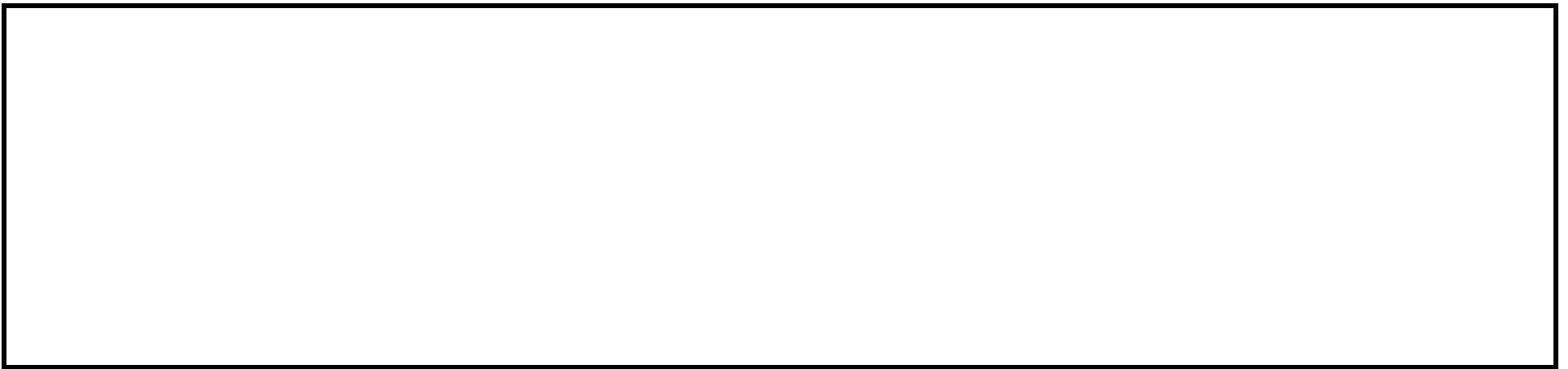
Description of research/work/project

Please describe the nature of the research being done, as well as some of the details at a high level, that will present a picture of how data is processed in this project.

A large, empty rectangular box with a black border, intended for the user to provide a detailed description of their research, work, or project.

Description of CUI

What CUI is involved in the project and how it will be handled? Make sure you address; CUI that is delivered to you from external sources, CUI you generate, and CUI you deliver to external sources.

A large, empty rectangular box with a black border, intended for the user to describe the types of Controlled Unclassified Information (CUI) involved in their project and how it will be managed.

NIST 800-171 Controls Form

For all deviations from the SSP, either the standard solution should be attested or a mitigation specific to this addendum should be entered

NIST 800-171 Control Number	Control Family	Control Text	Standard Solution	Exception-Specific Solutions and Mitigations
3.1.12	Access Control	Monitor and control remote access sessions.	GT VPN ¹	
3.1.13	Access Control	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	GT VPN	
3.1.14	Access Control	Route remote access via managed access control points.	GT VPN	
3.1.15	Access Control	Authorize remote execution of privileged commands and remote access to security-relevant information.	Central Endpoint Management	
3.5.3	Identification and Authentication	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	GT 2FA ² LastPass ³ Thycotic Secret Server ⁴	
3.5.4	Identification and Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	GT 2FA	
3.8.1	Media Protection	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	Cable lock Door Keys ⁵ Encryption ⁶	
3.8.2	Media Protection	Limit access to CUI on information system media to authorized users.	Central Endpoint Management SSP Document	

¹ Georgia Tech uses Cisco [AnyConnect VPN](#) which offers a [2FA option](#). All employees and students are required to use the 2FA option.

² GT 2FA (Georgia Tech Two-Factor Authentication) secures access to services where required.

³ Georgia Tech offers [LastPass](#) to provide additional security when using privileged accounts accessed with Two-Factor Authentication.

⁴ Georgia Tech offers [Thycotic's Secret Server](#) which uses Two-Factor Authentication to secure access to the password vault.

⁵ Physical keys require the use of a key management and tracking system. This should be reviewed on a periodic basis.

⁶Please see Georgia Tech encryption standard: <https://security.gatech.edu/encryption-best-practices>. BitLocker (Windows), LUKS (Linux), FileVault (Mac)

3.8.5	Media Protection	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	CUI is encrypted during transport	
3.8.6	Media Protection	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Cable Lock Door Keys Encryption	
3.8.7	Media Protection	Control the use of removable media on information system components.	Either no removable media devices are used or only labeled removable media devices are used	
3.8.8	Media Protection	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Either no portable storage devices are used or only labeled storage devices are used	
3.8.9	Media Protection	Protect the confidentiality of backup CUI at storage locations.	Dropbox ⁷ Office 365 ⁸ Box ⁹	
3.10.1	Physical Protection	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Cable Lock Door Keys Encryption	
3.10.2	Physical Protection	Protect and monitor the physical facility and support infrastructure for those information systems.	Cable lock Door Keys Encryption	
3.10.5	Physical Protection	Control and manage physical access devices.	Cable lock Door Keys Encryption	
3.10.6	Physical Protection	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	Cable lock Door Keys Encryption	
3.13.7	System and Communications Protection	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.	GT VPN	

⁷ [Georgia Tech Dropbox Enterprise](#) – please note that only Georgia Tech Box Accounts are compliant, and CUI must be encrypted first before it is stored in Dropbox.

⁸ This is for the instance associated with Georgia Tech’s Office 365 offering. Personal Office 365 accounts are noncompliant with established Georgia Tech Policies

⁹ [Georgia Tech Box Account](#) – please note that only Georgia Tech Box Accounts are compliant.

3.13.12	System and Communications Protection	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	BlueJeans ¹⁰ Skype for Business ¹¹ WebEx ¹² Microsoft Teams ¹³	
3.13.14	System and Communications Protection	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	BlueJeans Skype for Business WebEx Microsoft Teams	

Disclaimer: We understand that you may be using computers not listed in the SSP to perform remote work for projects requiring an SSP. Please be sure to save your data in approved cloud storage services.

The SSP Exception Form document temporarily allows use of GT-Owned and Personal Devices to maintain research continuity as campus reacts to COVID-19. Any data that is stored, processed, or transmitted must be removed from the devices temporarily allowed, and PI will need to sign an attestation form of destruction when they are back to normal function.

Physically protecting systems while offsite when complying with NIST 800-171 is required. All systems whether in or out-of-scope should be secured using one of the following when not in use:

- Non-public secure area (*preferably behind lock and key*)
- Cable lock
- Full Disk Encryption

If you have additional questions on the options above, please visit: <https://cui.gatech.edu/digital-media-protection/>

¹⁰ [Georgia Tech BlueJeans Collaboration](#)

¹¹ Skype for Business is available through Office 365

¹² [Georgia Tech WebEx Collaboration](#)

¹³ Microsoft Teams is available through Office 365

Approvals

I acknowledge that I will manage CUI associated with this project in accordance with this SSP Exception.

Principal Investigator (printed):	_____
Principal Investigator (signature):	_____
Approval Date:	_____

Approved CISO or Designee (printed)	_____
Approved CISO or designee (signature)	_____
Approval Date	_____

Approved VP Research or Designee (printed)	_____
Approved VP Research or Designee (signature)	_____
Approval Date	_____

SSP Exception is valid through _____.

END OF DOCUMENT