# Clayton State University

## Clayton State System Security Plan

CSU SSP

### Overview

This Standard System Security Plan (SSP) has been developed and will be used to protect all systems storing and processing CUI.

### Purpose

This document outlines the management, operational, and technical safeguards or countermeasures approved by the university 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 ISO and CIO or its designee.

# SSP Controls

For all deviations, or items where there is no approved central solution, marked "To be determined as appropriate per project" an approved mitigation should be entered.

| NIST 800-171 Control Number | Control Family | Control Text | Standard Solution | Mitigation |
|---|---|---|---|---|
| 3.1.1 | Access Control | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | Technology Infrastructure team | |
| 3.1.2 | Access Control | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | Technology Infrastructure team | |
| 3.1.3 | Access Control | Control the flow of CUI in accordance with approved authorizations. | Technology Infrastructure team | |
| 3.1.4 | Access Control | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | Technology Infrastructure team | |
| 3.1.5 | Access Control | Employ the principle of least privilege, including for specific security functions and privileged accounts. | Technology Infrastructure team | |
| 3.1.6 | Access Control | Use non-privileged accounts or roles when accessing nonsecurity functions. | Technology Infrastructure team | |
| 3.1.7 | Access Control | Prevent non-privileged users from executing privileged functions and audit the execution of such functions. | Technology Infrastructure team | |
| 3.1.8 | Access Control | Limit unsuccessful logon attempts. | Technology Infrastructure team | |
| 3.1.9 | Access Control | Provide privacy and security notices consistent with applicable CUI rules. | Technology Infrastructure team | |
| 3.1.10 | Access Control | Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity. | Technology Infrastructure team | |

| | | | | |
|---|---|---|---|---|
| 3.1.11 | Access Control | Terminate (automatically) a user session after a defined condition. | Technology Infrastructure team | |

| | | | | |
|---|---|---|---|---|
| 3.1.12 | Access Control | Monitor and control remote access sessions. | CSU VPN | |
| 3.1.13 | Access Control | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | CSU VPN | |
| 3.1.14 | Access Control | Route remote access via managed access control points. | CSU VPN | |
| 3.1.15 | Access Control | Authorize remote execution of privileged commands and remote access to securityrelevant information. | Technology Infrastructure team | |
| 3.1.16 | Access Control | Authorize wireless access prior to allowing such connections. | CSU Secure Wireless | |
| 3.1.17 | Access Control | Protect wireless access using authentication and encryption. | CSU Secure Wireless | |
| 3.1.18 | Access Control | Control connection of mobile devices. | To be determined as appropriate per project | |
| 3.1.19 | Access Control | Encrypt CUI on mobile devices. | Technology Infrastructure team | |
| 3.1.20 | Access Control | Verify and control/limit connections to and use of external information systems. | Palo Alto NGFW[1] | |
| 3.1.21 | Access Control | Limit use of organizational portable storage devices on external information systems. | To be determined as appropriate per project | |
| 3.1.22 | Access Control | Control information posted or processed on publicly accessible information systems. | To be determined as appropriate per project | |

[1]Clayton State firewalls are Palo Alto firewalls offering Next Generation Firewall (NGFW) capabilities.

| | | | | |
|---|---|---|---|---|
| 3.2.1 | Awareness and Training | Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems. | IT Security | |

| | | | | |
|---|---|---|---|---|
| 3.2.2 | Awareness and Training | Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. | IT Security | |
| 3.2.3 | Awareness and Training | Provide security awareness training on recognizing and reporting potential indicators of insider threat. | IT Security | |
| 3.3.1 | Audit and Accountability | Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. | CSU AD/Local GPO | |
| 3.3.2 | Audit and Accountability | Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. | CSU AD/Local GPO | |
| 3.3.3 | Audit and Accountability | Review and update audited events. | CSU AD/Local GPO | |
| 3.3.4 | Audit and Accountability | Alert in the event of an audit process failure. | CSU AD/Local | |
| 3.3.5 | Audit and Accountability | Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. | CSU AD/Local GPO | |
| 3.3.6 | Audit and Accountability | Provide audit reduction and report generation to support on-demand analysis and reporting. | CSU AD/Local GPO | |

| | | | | |
|---|---|---|---|---|
| 3.3.7 | Audit and Accountability | Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. | CSU AD/Local GPO | |
| 3.3.8 | Audit and Accountability | Protect audit information and audit tools from unauthorized access, modification, and deletion. | CSU AD/Local GPO | |

| | | | | |
|---|---|---|---|---|
| 3.3.9 | Audit and Accountability | Limit management of audit functionality to a subset of privileged users. | CSU AD/Local GPO | |
| 3.4.1 | Configuration Management | Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | Technology Infrastructure team | |
| 3.4.2 | Configuration Management | Establish and enforce security configuration settings for information technology products employed in organizational information systems. | Technology Infrastructure team | |
| 3.4.3 | Configuration Management | Track, review, approve/disapprove, and audit changes to information systems. | Change Control Form in Support Ticketing ServiceNow | |
| 3.4.4 | Configuration Management | Analyze the security impact of changes prior to implementation. | Change Control Form in Support Ticketing ServiceNow | |
| 3.4.5 | Configuration Management | Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system. | Change Control Form in Support Ticketing ServiceNow | |
| 3.4.6 | Configuration Management | Employ the principle of least functionality by configuring the information system to provide only essential capabilities. | Technology Infrastructure team | |
| 3.4.7 | Configuration Management | Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services. | Technology Infrastructure team | |

| | | | | |
|---|---|---|---|---|
| 3.4.8 | Configuration Management | Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. | Technology Infrastructure team | |

| | | | | |
|---|---|---|---|---|
| 3.4.9 | Configuration Management | Control and monitor user-installed software. | Technology Infrastructure team | |
| 3.5.1 | Identification and Authentication | Identify information system users, processes acting on behalf of users, or devices. | CSU AD | |
| 3.5.2 | Identification and Authentication | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | CSU AD | |
| 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. | MS Azure MFA<br>CSU VPN | |
| 3.5.4 | Identification and Authentication | Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. | CSU AD | |
| 3.5.5 | Identification and Authentication | Prevent reuse of identifiers for a defined period. | CSU AD | |
| 3.5.6 | Identification and Authentication | Disable identifiers after a defined period of inactivity. | CSU AD | |
| 3.57 | Identification and Authentication | Enforce a minimum password complexity and change of characters when new passwords are created. | CSU AD | |
| 3.5.8 | Identification and Authentication | Prohibit password reuse for a specified number of generations. | CSU AD | |
| 3.5.9 | Identification and Authentication | Allow temporary password use for system logons with an immediate change to a permanent password. | CSU AD | |
| 3.5.10 | Identification and Authentication | Store and transmit only encrypted representation of passwords. | CSU AD | |

| | | | | |
|---|---|---|---|---|
| 3.5.11 | Identification and Authentication | Obscure feedback of authentication information. | CSU AD | |

| | | | | |
|---|---|---|---|---|
| 3.6.1 | Incident Response | Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. | Information Security | |
| 3.6.2 | Incident Response | Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization. | Information Security | |
| 3.6.3 | Incident Response | Test the organizational incident response capability. | Information Security | |
| 3.7.1 | Maintenance | Perform maintenance on organizational information systems. | Technology Infrastructure team | |
| 3.7.2 | Maintenance | Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. | Technology Infrastructure team | |
| 3.7.3 | Maintenance | Ensure equipment removed for off-site maintenance is sanitized of any CUI. | Technology Infrastructure team | |
| 3.7.4 | Maintenance | Check media containing diagnostic and test programs for malicious code before the media are used in the information system. | To be determined as appropriate per project | |
| 3.7.5 | Maintenance | Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. | Microsoft Azure MFA and CSU VPN | |
| 3.7.6 | Maintenance | Supervise the maintenance activities of maintenance personnel without required access authorization. | Technology Infrastructure team | |

| | | | | |
|---|---|---|---|---|
| 3.8.1 | Media Protection | Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital. | To be determined as appropriate per project | |
| 3.8.2 | Media Protection | Limit access to CUI on information system media to authorized users. | Technology Infrastructure team | |

| | | | | |
|---|---|---|---|---|
| 3.83 | Media Protection | Sanitize or destroy information system media containing CUI before disposal or release for reuse. | To be determined as appropriate per project | |
| 3.84 | Media Protection | Mark media with necessary CUI markings and distribution limitations. | To be determined as appropriate per project | |
| 3.8,5 | Media Protection | Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. | To be determined as appropriate per project | |
| 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. | To be determined as appropriate per project | |
| 3.8.7 | Media Protection | Control the use of removable media on information system components. | To be determined as appropriate per project | |
| 3.8.8 | Media Protection | Prohibit the use of portable storage devices when such devices have no identifiable owner. | To be determined as appropriate per project | |
| 3.8.9 | Media Protection | Protect the confidentiality of backup CUI at storage locations. | Exagrid Backup OneDrive | |
| 3.9.1 | Personnel Security | Screen individuals prior to authorizing access to information systems containing CUI. | HR | |
| 3.9.2 | Personnel Security | Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers. | To be determined as appropriate per project | |

| | | | | |
|---|---|---|---|---|
| 3.10.1 | Physical Protection | Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. | Physical keys<br>Keycard Reader | |
| 3.10.2 | Physical Protection | Protect and monitor the physical facility and support infrastructure for those information systems. | Physical keys<br>Keycard Reader<br>Video Cameras | |
| 3.10.3 | Physical Protection | Escort visitors and monitor visitor activity. | To be determined as appropriate per project | |
| 3.10.4 | Physical Protection | Maintain audit logs of physical access. | Keycard Reader<br>Video Cameras | |
| 3.10.5 | Physical Protection | Control and manage physical access devices. | Keycard Reader<br>Video Cameras | |
| 3.10.6 | Physical Protection | Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites). | To be determined as appropriate per project | |
| 3.11.1 | Risk Assessment | Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI. | Information Security | |
| 3.11.2 | Risk Assessment | Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified. | Information Security<br>Nessus and Trustwave | |
| 3.11.3 | Risk Assessment | Remediate vulnerabilities in accordance with assessments of risk. | To be determined as appropriate per project | |
| 3.12.1 | Security Assessment | Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application. | Information Security | |

Physical keys require the use of a key management and tracking system. This should be reviewed on a periodic basis. Clayton State police department provides key management and central monitoring for a network of video cameras across campus.

| | | | | |
|---|---|---|---|---|
| 3.12.2 | Security Assessment | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems. | Information Security | |
| 3.123 | Security Assessment | Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. | Information Security | |
| 3.12.4 | Security Assessment | Develop, document, periodically update, and implement system security plans for organizational information systems that describe the security requirements in place or planned for the systems. | SSP Template — this document | |
| 3.13.1 | System and Communications Protection | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | Palo Alto NGFW | |
| 3.13.2 | System and Communications Protection | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. | Information Security | |
| 3.13.3 | System and Communications Protection | Separate user functionality from information system management functionality. | Technology Infrastructure team | |
| 3.13.4 | System and Communications Protection | Prevent unauthorized and unintended information transfer via shared system resources. | Technology Infrastructure team | |
| 3.13.5 | System and Communications Protection | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. | To be determined as appropriate per project | |
| 3.13.6 | System and Communications Protection | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). | Palo Alto NGFW | |

| | | | | |
|---|---|---|---|---|
| 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. | CSU VPN | |
| | System and Communications Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | OneDrive<br>CSU VPN | |
| 3.13.9 | System and Communications Protection | Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. | To be determined as appropriate per project | |
| 3.13.10 | System and Communications Protection | Establish and manage cryptographic keys for cryptography employed in the information system; | To be determined as appropriate per project | |
| 3.13.11 | System and Communications Protection | Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. | Dropbox<br>OneDrive<br>Bitlocker<br>CSU VPN | |
| 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. | To be determined as appropriate per project | |
| 3.13.13 | System and Communications Protection | Control and monitor the use of mobile code. | To be determined as appropriate per project | |
| 3.13.14 | System and Communications Protection | Control and monitor the use of Voice over Internet Protocol (VolP) technologies. | Skype for Business<br>Microsoft Teams | |
| 3.13.15 | System and Communications Protection | Protect the authenticity of communications sessions. | Palo Alto NGFW | |
| 3.13.16 | System and Communications Protection | Protect the confidentiality of CUI at rest. | OneDrive<br>Bitlocker | |

BitLocker encryption uses AES to encrypt entire volumes on Windows server and client machines,

Skype for Business is available through Office 365
Microsoft Teams is available through Office 365

| | | | | |
|---|---|---|---|---|
| 3.14.1 | System and Information Integrity | Identify, report, and correct information and information system flaws in a timely manner. | Technology Infrastructure team | |
| 3.14.2 | System and Information Integrity | Provide protection from malicious code at appropriate locations within organizational information systems. | Cylance Protect | |
| 3.14.3 | System and Information Integrity | Monitor information system security alerts and advisories and take appropriate actions in response. | Information Security | |
| | System and Information Integrity | Update malicious code protection mechanisms when new releases are available. | Cylance Protect | |
| 3.14.5 | System and Information Integrity | Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. | Nessus Trustwave Cylance Protect | |
| 3.14.6 | System and Information Integrity | Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | Information Security | |
| 3.14.7 | System and Information Integrity | Identify unauthorized use of the information system. | Information Security | |

## Approvals

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

James Hunter Information Security Officer

Approval Date 8/15/2018

END OF DOCUMENT