IMPERIAL COMMUNITY COLLEGE DISTRICT

INFORMATION PROTECTION OPERATIONAL PROCEDURE

Version 1.0

Revision History

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

TABLE OF CONTENTS

0.0 INTRODUCTION

This document is a collection of individual Information Protection policies that together comprise the Information Protection Operation Policy for Imperial Community College District as defined in each policy. The Information Protection Operation Policy has been established in an effort to protect the confidentiality, integrity, and availability of personally identifiable information, trade secrets, intellectual property, and any other sensitive data held by the organization. These policies as a whole constitute the Information Protection Operation Policy program (or Information Protection program).

In addition, the Information Protection Operation Policy specifically defines how computing and communication assets, systems, and resources should be accessed, configured, used, and protected and the types of monitoring activities that should be executed to maintain the security of the operating environment.

The Information Protection Operation Policy document is published under the authority of President's Cabinet and provides a framework for safeguarding people, data, and information including the creation, processing, management, transmission, storage, and disposal of information within the scope of the organization.

1.0 RESPONSIBILITIES AND OVERSIGHT POLICY

Effective Date	*December 12, 2018*
Revision Date	
Policy Version	
Policy Owner	
Executive Sponsors	

This document applies to:

All employees, contractors, and third parties of the afore mentioned entities must support the Information Protection program detailed herein.

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

1.1 PURPOSE

The purpose of this Responsibilities and Oversight Policy is to establish oversight of security policies and control standards that the organization has adopted to mitigate security risks as well as comply with applicable laws, regulations and contractual agreements.

This Responsibilities and Oversight Policy also covers security awareness and training in an effort to promote security awareness, communication, and training through the establishment of an effective security awareness and education program. The Security Awareness and Training program owned by Information Protection ensures the organization documents, communicates, and educates company personnel, contractors, and third parties.

1.2 POLICY STATEMENT

1.2.1 Roles and Responsibilities

1.2.1.1 Management Commitment to Information Security

Management must approve and be committed to all Information Protection initiatives set forth in the set of policies defined in the Information Protection Operation Policy document. As such, Management must identify a sponsor to drive assessment, compliance, and enforcement activities.

a. Information Technology will be responsible for compliance and enforcement activities associated with this set of policies. At the discretion of President's Cabinet, the Information Protection Operation Policy will be the foundation for these activities.

b. Information Technology is the internal group responsible for managing and directing the Information Protection program. Specific responsibilities include:
   - Developing or coordinating the development of data security policies, standards, guidelines, and procedures
   - Ensuring the timely publication of approved information protection related data policies, standards, guidelines, and procedures
   - Coordinating information protection awareness activities across the organization
   - Enforcement of security policies, standards, and procedures
   - Ensuring the coordination of all data security related functions (e.g., event monitoring activities, incident response activities)
   - Identifying key Information Protection program elements
   - Identifying key Information Protection program initiatives
   - Develop and maintain an Information Protection Roadmap which includes key elements and initiatives
   - Identifying Information Protection goals and objectives in support of the Information Protection Roadmap

- Coordinating information protection decisions for future initiatives related to privacy and security of data or other areas as deemed appropriate by the Technology Committee
- Developing and managing an Information Protection program budget
- Working with [Facility Security] as necessary in support of emergency planning
- Working with Human Resources in support of personnel related issues
- Taking appropriate action on violations of Information Protection policies, standards and procedures

1.2.1.2 Allocation of Information Protection Responsibilities

Roles and responsibilities for ensuring support of the Information Protection Operation Policy must be assigned.

a. The Imperial Community College District Technology Planning Committee is responsible for coordinating the review of risks and security implications associated with the use of all technologies within the organization's operating environment.

b. An Information User is any employee, contractor, third party, or other authorized person who uses Imperial Community College District and non-Imperial Community College District information and information resources in the course of their daily work. Information User responsibilities include:
   - Maintaining the confidentiality of credentials. Credentials are defined as anything used to authenticate to an information system, including but not limited to; passwords, PINS, tokens, keys and access cards
   - Reporting suspected information security violations to Information Protection
   - Adhering to Information Protection policies, standards, and procedures
   - Using Imperial Community College District and non-Imperial Community College District information and information resources responsibly and for authorized purposes only

c. An Information Owner is a Group Manager level or above individual responsible for the Imperial Community College District's information assets. All information shall be owned by individual business units. Information Owner responsibilities include:
   - Assigning information classification levels as defined in AP3310
   - Verifying that employee, contractor, and third party access rights are current and commensurate with their role
   - Informing Information Technology of any special backup requirements for the information for which they are responsible

d. An Information Custodian is any employee, contractor, third party, or other authorized person who has the responsibility for the maintenance of information

assets. Information Owners have the right to delegate data maintenance responsibilities to Information Custodians. The Information Owner may designate one or more Information Custodians based on the level of delegated responsibilities. The Information Custodian must provide the following:

- Assistance to the Information Owners in determining appropriate levels of data classification
- Operationally provide assurance for the confidentiality, integrity, and availability of information

e. System Administrators are required to maintain, operate, and implement technology solutions within the organization in accordance with the Information Protection Operation Policy. System Administrators are responsible for deploying, implementing, and monitoring security controls on an operational basis. Guidance for the controls or control objectives must be provided by Information Technology. System Administrators are responsible for:
   - Implementation of technical security controls
   - Communication to Information Technology on security related incidents and issues
   - System security updates including but not limited to patches
   - System documentation
   - System performance
   - Security monitoring

f. Information Technology is responsible for monitoring compliance with the standards and guidelines outlined by the Information Protection Operation Policy. Frequent communication between Information Technology will identify security related risks throughout the organization. These risks must be communicated to management to appropriately assess risks to the organization. Management may address the identified risks through acceptance, mitigation or remediation.

g. Network Administrators are responsible for configuring and maintaining the network. This includes implementing specific security controls for segmenting the network.

1.2.1.3 Independent Review of Information Protection Operation Policy

Information Protection Operation Policy, standards, and security environment(s) must be reviewed annually by an independent third party. Any recommendations from this review must be evaluated and considered for incorporation into the Information Protection Operation Policy and implemented as applicable.

1.2.2 Information Protection Operation Policy Document

The Information Protection Operation Policy must be approved, maintained, and annually reviewed in order to ensure its relevance and effectiveness.

1.2.2.1 Information Protection Operation Policy Approval

The Information Protection Operation Policy must be approved by the Technology Planning Committee.

a. Information Technology is responsible for creating, reviewing, revising and coordinating the approval and coordinating the implementation of any data security policies, standards and procedures and ensuring such approvals follow the proper governance process.

b. Information Technology is responsible for ensuring that this policy document is reviewed and approved by the Technology Planning Committee on an annual basis.

1.2.2.2 Additions & Changes to Policy

Any additions or changes to the Information Protection Operation Policy must be managed and approved. All additions to the Information Protection Operation Policy must be approved by the Technology Planning Committee.

a. Any business unit, group, or department may initiate standards or procedures development with Information Technology. Information Technology will address requests at their discretion based upon an analysis of the request.

b. Information Technology is responsible for ensuring that all new Information Protection policies and standards follow the existing structure and format of the Information Protection Operation Policy or as deemed appropriate by the Technology Planning Committee. At a minimum, the following tasks must be conducted for all new or revised Information Protection policies:
   - A communication plan must be developed, at a minimum including notification of new policies, integration into security awareness materials, and if needed, special training for Information Users
   - An impact analysis must be conducted or coordinated by Information Technology prior to all Information Protection Operation Policy changes. This is to measure the risk and security implications that may result from the requested change and implementation requirements

1.2.2.3 Review of the Information Protection Operation Policy and Standards

An annual review of the Information Protection Operation Policy and Standards must be conducted to ensure relevance and identify any gaps.

a. Information Technology is responsible for initiating an annual review of the Information Protection Operation Policy.

b. Information Technology must perform a technical review and ensure standards remain current against business requirements, third party and industry recommended practices, in addition to being applicable to current technology and regulatory requirements.

c. The annual review must include a review of any impacting legal changes to ensure compliance with all applicable laws and regulatory requirements.

d. The annual review findings must be presented to the Technology Planning Committee. Findings must be addressed and any modifications must be made via the processes outlined by the [Information Protection Operation Policy Change Procedure].

1.2.3 Security Awareness and Training

This policy facilitates the establishment of security awareness and training capability throughout Imperial Community College District. The Security Awareness and Training program consists of a role-based learning model that presents learning as a continuum from developing general awareness through more formalized training.

1.2.3.1 Responsibilities of Information Technology

Responsibility for training on an annual basis must be assigned to ensure all employees and contractors are duly educated on security awareness.

a. Information Technology must create a security awareness, training and education program to promote constant security awareness for employees and contractors.

b. Information Technology is responsible for the development of security awareness and training.

c. The security awareness program must consist of regular awareness briefings to Information Risk Management to measure compliance rates.

1.2.3.2 Security Awareness

Information Technology must provide basic security awareness training to all information users (including managers, senior executives, and contractors) as part of initial training for new users, when required by policy changes, and annually thereafter.

a. Upon permanent or contract employment, all staff members are to be briefed on the Information Protection Operation Policy and procedures. A written summary of the Information Protection Operation Policy is to be provided to new staff and a signed copy is to be kept on file.

b. All users must be made aware of significant policy changes that occur outside of awareness training schedules.

1.2.3.3 Security Training

Business Units must partner with Information Technology to provide data security-related training.

1.2.3.4 Security Training Records

Individual training records must be retained for tracking purposes.

1.3 Exceptions and Escalation

Any exceptions to this policy must be approved in writing by President's Cabinet and the Technology Planning Committee.

1.4 Compliance

Failure to comply with this policy and other security requirements may result in disciplinary action, up to and including termination of employment or contract, and the possibility of civil and criminal liability.

1.5 Additional Definitions

N/A

1.6 Related Policies

N/A

1.7 Related Procedures and Standards

- [Information Protection Operation Policy Approval Procedure]
- [Information Protection Operation Policy Change Procedure]

2.0 PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

Effective Date	*December 07, 2018*
Revision Date	
Policy Version	
Policy Owner	
Executive Sponsors	

This document applies to:

All employees, contractors, and third parties of the afore mentioned entities must support the Information Protection program detailed herein.

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

2.1 PURPOSE

Robust physical and environmental controls must exist to protect information assets and information systems from unauthorized access and errors in order to safeguard against environmental threats.

2.2 POLICY STATEMENT

2.2.1 Equipment Security

All information systems must be protected from potential physical and environmental threats to ensure the confidentiality, integrity, and availability of the information contained within.

2.2.1.1 Network Jacks and Cabling Security

Network jacks and cables must be properly secured from unauthorized physical access and environmental threats.

a. Network Administrators must restrict access to all publicly accessible network jacks or implement network access controls to restrict access to network resources by unauthorized users and systems. Examples include but are not limited to conference rooms, training rooms and lobbies located outside of door access controls.

b. Sites with a high concentration of information assets such as data centers. server rooms or wiring closets must ensure additional cabling security for critical systems which may include one or more of the following:
   - Segregated, locked conduit rooms/boxes
   - Alternative routing or segmented cabling schemes

d. All Sites with information assets must ensure that conduits for network cabling are protected against interference or interruption. This includes avoiding routes through public areas, segregation from power cabling to eliminate interference, and clearly identified labeling on equipment.

e. Network Administrators must ensure that all network connections are removed or deactivated when a site is being vacated.

2.2.1.2 Equipment Maintenance

Systems must be maintained by trained and authorized individuals only.

a. All Sites with information assets must ensure that utilities (e.g., UPS, generator) equipment is monitored in accordance with manufacturer specification and correctly maintained to ensure the availability, integrity, and confidentiality of information contained within each site.

b. All Sites with information assets must ensure that only trained and authorized maintenance personnel are allowed to perform repairs and service that all work is documented.

2.2.1.3 Data Center Environmental Controls

All data center facilities must ensure that new and remodeled computer or communications centers are constructed so they are protected against water damage, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, and other threats known or likely to occur at their respective locations.

a. Smoking, vaping, drinking, and eating in computer processing rooms is strictly prohibited.

b. Walls surrounding computer facilities must be non-combustible and resistant to fire for at least one hour. All openings to these walls (e.g., doors, ventilation ducts, etc.) should be self-closing and resistant to fire for at least one hour.

c. All computer equipment must be operated in a climate-controlled atmosphere at all times. Redundant ventilation must be provided in the event that air conditioning systems in data center facilities fail.

d. Computer equipment must be housed in an environment equipped with fire detection and suppression systems.

e. Procedures must exist for facilities management to test fire suppression system equipment at least once every twelve (12) months. The test results must be documented and any issues must be addressed.

f. All computer room personnel must be trained in the use of any automatic fire suppression systems, the use of portable fire extinguishers, and the proper response to smoke and fire alarms.

g. All network attached environmental management and control systems must be implemented in a segregated network segment that restricts access based on role and source.

2.2.1.4 Data Center Supporting Utilities

All utilities (e.g., water, electricity, etc.) must be adequate for the systems they are supporting. In addition, Disaster Recovery procedures must be properly documented.

a. A suitable, redundant electrical power supply must be in place to avoid power failures. Based on business criticality, the use of a back-up generator must be considered.

b. Uninterruptible Power Supplies (UPS) must be used for equipment supporting critical business operations to facilitate system availability or orderly system shutdown in the event of power disruption. UPS equipment must be checked on a formal maintenance schedule to ensure it has adequate capacity and must be tested in accordance with the manufacturer's recommendations.

c. For emergency situations, data centers must provide for the following:
   - Capability of shutting off power to the information systems or individual system components
   - Emergency shutoff switches or devices must be placed in locations that facilitate safe and easy access for personnel
   - Emergency power shutoff switches must be protected from unintentional activation
   - Must have automatic emergency lighting for information systems that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility

d. Network Administrators must ensure that a suitable, redundant telecommunications infrastructure is in place to avoid communication failures and single points of failure. Based on business criticality, the use of backup communications lines or providers must be considered.

f. Disaster Recovery procedures must include failover and failback processes for the following supporting utilities:
   - Electrical power
   - Communications

g. The Disaster Recovery plan must be tested on a periodic basis. The test results must be documented and any issues must be addressed.

2.2.1.5 Removal of Property

Removal of information assets and intellectual property from premises must be authorized.

2.2.1.6 Security of Off-Site Equipment

Authorized equipment and media taken outside of Imperial Community College District premises must be controlled, secured, protected, and insured.

a. The Information Protection Policies apply to all equipment and information regardless of physical location.

b. Employees that travel with a laptop or other equipment with sensitive information, including briefcases, mobile devices, and portable hard drives,

must be cautious and keep the items with them at all times (e.g., do not include the equipment with checked luggage).

c. Loss of any of the aforementioned items must be reported to Security and Internal Audit within 24 hours including suspicion of loss of equipment.

2.2.2 Secure Areas Containing Information Assets

All facilities must have controls in place to protect information assets contained within from physical and environmental threats.

2.2.2.1 Physical Entry Controls

A process for restricting and monitoring physical access to each facility containing information assets must be implemented.

a. Information Technology must ensure that access rights to all data center facilities are reviewed and approved by an appropriate party on a yearly basis.

b. Facilities used for non-instructional purposes must ensure that physical access to all secure areas is controlled. Doors must be secured at all times and only authorized personnel may have access.

c. Authorized personnel must not allow unknown or unauthorized individuals into secure areas without an escort. Authorized personnel must notify Security of any unrecognized and unescorted personnel within a secure area. Security personnel are responsible for evaluating and addressing the situation as appropriate and notifying the appropriate parties, including IT.

2.2.2.2 Securing Offices, Rooms, and Facilities in Data Centers

Access to all data center facilities must be authorized, monitored, and periodically reviewed to detect and prevent unauthorized access.

a. Data Center Services must ensure that computer room access is limited to only those people with a valid business reason for access. Access must be reviewed periodically and revoked immediately when it is no longer required.

b. All employees, contractors and third parties must ensure that contact directories and other internal documents identifying locations of information processing facilities or any other sensitive or secure areas are not accessible by the public.

c. Data Center Services and Security must ensure that all critical computer rooms and data centers, including those operated by third parties, are

monitored 24 hours per day. This monitoring must include video surveillance and secured and alarmed doors. All data collected through this monitoring, including video surveillance, must be maintained for a rolling 15 day period.

d. Data Center Services must ensure that data centers are not used for printing, faxing, storage of computers, or any other purpose other than to support the computer hardware and information assets contained therein.

e. Data Center Services must ensure that computer facility rooms are equipped with doors that automatically close immediately after they have been opened, and set off an audible alarm when they have been kept open beyond a pre-determined period of time.

f. Facilities personnel must ensure that rooms containing network, wiring, or communications equipment (e.g., wiring closets, etc.) are locked at all times with access restricted to authorized personnel.

g. Signs are not to be posted on wiring closets, telephone rooms, data center facilities, or other equipment components.

2.2.2.3 Working in Secure Areas

All secure work areas (as described by this policy or designated by Information Technology) and all material contained within must be secured to protect from physical threats.

a. Data Center Services and Facilities are responsible for any person working in, or having access to, the secure area. The managers of secure areas must inform personnel that they are working in a secure area and advise them of any additional security requirements they must follow. The manager is also responsible for implementing any additional physical or procedural security controls needed to protect information stored in the secure area.

b. Facilities personnel must ensure that any third party within a secure area, including support services such as cleaning and waste removal, is strictly controlled and monitored at all times.

c. Any relocation of a workspace must ensure that all information assets are protected during the moving process. This includes, but is not limited to, computer and hard copy files.

d. Employees, contractors and third parties must collect all printed documents (e.g., printouts, faxes, photocopies) in a timely manner. Printers, faxes, and photocopiers in secure work areas must be checked regularly (at least every day after business hours) for printouts which were not collected by owners. Uncollected items must be destroyed or secured until the proper owners of

the documents are available. Managers of secure areas are responsible for ensuring business processes incorporate this policy.

2.2.2.4 Protecting Against External and Environmental Threats

All facilities must be properly protected, separated or both from potential external and environmental threats.

a. Facilities personnel must ensure that any hazardous or combustible materials are stored at a safe distance in appropriate containers from any secure area in accordance with local safety regulations and manufacturer specifications.

b. [Facilities personnel must ensure that appropriate firefighting equipment is available at all sites. Equipment must be checked periodically. All firefighting equipment location and maintenance must be in compliance with local fire regulations.

c. Data Center Services must ensure that backup and recovery media and facilities are located at a safe distance from main facilities. The backup facilities must be at a distance that would protect it from damage from any incident at the main site.

2.3 Exceptions and Escalation

Any exceptions to this policy must be approved in writing by Information Technology and applicable business unit management.

2.4 Compliance

Failure to comply with this policy and other security requirements in the organization can result in disciplinary action, up to and including termination of employment or contract, and the possibility of civil and criminal liability.

2.5 Additional Definitions

N/A

2.6 Related Policies

N/A

2.7 Related Procedures and Standards

N/A

3.0 COMMUNICATION MANAGEMENT POLICY

Effective Date	*December 07, 2018*
Revision Date	
Policy Version	
Policy Owner	
Executive Sponsors	

This document applies to:

All employees, contractors, and third parties of the afore mentioned entities must support the Information Protection program detailed herein.

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

3.1 PURPOSE

The way that information is communicated must be clearly defined and managed. Employees, contractors, and third parties are responsible for safeguarding their communications, no matter the form, to adequately protect the organization's information assets.

3.2 POLICY STATEMENT

3.2.1 Exchange of Information

Employees, contractors, and third parties exchanging business information, regardless of the medium (e.g., paper, electronic, verbal, etc.), must follow proper security procedures.

3.2.1.1 Information Exchange Policies and Procedures

Procedures must be developed that address the risks involved when exchanging information.

a. Information Risk Management must ensure that policies and procedures outlining the acceptable use of electronic communication systems are established to:
   - Protect the exchange of information from unauthorized interception, copying, modification, and destruction
   - Protect sensitive information included as attachments through the use of encryption

b. Security awareness and training will include informing employees, contractors, and third parties of the acceptable use of Imperial Community College District's systems

c. When accessing information that is considered "Confidential," the copying, moving, and storing of the data onto local hard drives or removable, unencrypted electronic media is prohibited.

d. All employees, contractors, and third parties must ensure that any data or media waiting to be distributed or produced is secured to a level consistent with its classification. This includes but is not limited to:
   - Printed materials awaiting distribution
   - Printed materials awaiting pickup for external delivery services
   - Media, such as backup tapes, awaiting pickup for off-site storage

e. Employees, contractors, and third parties must not leave sensitive information in messages on any type of telephone answering machine or forward voice messages to an external destination (e.g., a non-company phone).

f. Employees, contractors, and third parties are not to forward their Imperial Community College District mailboxes to personal email accounts nor use external mail aggregation services to manage their email.

3.2.1.2 Exchange Agreements

Formal agreements between Imperial Community College District and external parties must exist prior to sharing information or establishing network connections to external systems.

a. Information Technology must be consulted to conduct a risk assessment prior to interconnecting business information systems. Specific considerations must be based on the classification of data being shared, however, may include the following:
   - Identify risks, threats, vulnerabilities, impacts, and associated compensating controls and safeguards
   - Determine which sensitive information is to be excluded from the system if an appropriate level of protection cannot be provided
   - Determine requirements for individuals working on sensitive projects

b. IT, General Council, and the business units must ensure agreements that include an exchange of sensitive information incorporate the following:
   - Management responsibilities and procedures will be defined for handling transmission, dispatch, and receipt
   - Procedures will be defined to ensure traceability and non-repudiation
   - Packaging and transmission technical standards will be defined
   - Legitimate commercial couriers or shipping services will be used for hard copy data transfer
   - Responsibilities and liabilities are defined in the event of information security incidents
   - Ownership is defined and responsibilities for protecting data, copyrights, and licensing are established
   - Special controls for protecting sensitive information are defined

3.2.1.3 Paper-based Information Transfer

Paper-based transfer of information must be used on an as-needed basis only and must follow proper handling procedures.

a. Employees, contractors, and third parties must ensure that any media sent via interoffice mail, courier, or other means is clearly labeled with the appropriate information to ensure delivery to the intended recipient.

b. Imperial Community College District information must only be generated in hard copy to the extent necessary to complete normal business operations.

c. Sensitive information must be stored in locked drawers, cabinets, or rooms specifically designated for that purpose and accessible only by authorized individuals.

d. All hard copy information must be disposed of properly by either shredding the information or leaving the information in secured, designated Vital Data bins.

3.2.1.4 Verbal Information Transfer

Employees, contractors, and third parties must take caution when exchanging information verbally to avoid unnecessary transfer of information.

3.2.1.5 Removable Media Information Transfer

Transfer of information via removable media must be used on an as-needed basis only and must follow proper handling procedures.

a. Any transfer of removable media containing sensitive information or any other “internal” classified or above information must be labeled with the classification level, logged and authorized by the Information Owner and be sent via a secured courier or other delivery method that can be tracked.

b. Information sent by postal service or courier must be protected from unauthorized access, misuse, or corruption. Employees, contractors, and third parties must ensure packaging for information is sufficient to protect contents from physical damage or tampering. For sensitive information, special controls must be used including:
   - Tamper resistant packaging
   - Delivery by hand
   - Signature required on delivery

3.2.2 Encryption

A key-based encryption solution must be used by the organization to protect sensitive data from unauthorized access while being stored throughout the environment and transmitted across external, publicly accessible networks.

3.2.2.1 Usage of Encryption

Encryption technologies must be approved and used where applicable.

a. IT is responsible for specifying all encryption software, protocols and algorithms to be used and to update the technology standards as appropriate.

b. IT must perform an annual review of the approved encryption software, protocols and algorithms.

c. Employees, contractors, and third parties must not install any encryption software not on the IT Standards List.

d. Information Technology must ensure that only encryption algorithms and protocols approved by IT are used to encrypt data in information systems.

e. IT reserves the right to request any key or password for encrypted files stored on Imperial Community College District's systems or on behalf of Imperial Community College District. This includes but is not limited to passwords for files stored on local or network hard drives, portable media and cloud services.

3.2.2.2 Key Management

Cryptographic keys used for encryption of sensitive data (e.g., payment card account numbers, Personally Identifiable Information (PII)), must be monitored and protected against both disclosure and misuse.

a. Users must treat keys (passwords or private keys) for encrypted data with the same level of confidentiality as passwords for systems or applications. (Refer to [Password Standards] for guidance).

b. Key Custodians must ensure that all hardware either housing key management applications or used for generation of encryption keys is protected at the highest level of security controls. IT must be informed about any proposed alterations to the key management applications or security controls prior to any change.

c. Any contractual or third party agreements involving encryption or key management must be approved by Risk Management and Office of General Council.

d. IT is responsible for developing key management procedures as necessary for the organization. Procedures must be developed for:
   - Generation of keys
   - Management of public key certificates
   - Distribution of keys
   - Storage of keys
   - Revocation of keys
   - Rotation of keys
   - Key recovery
   - Archiving keys
   - Destroying keys
   - Key escrow

3.2.2.3 Data-in-Transit

Encryption must be used for specific data types in transit across open, public networks. Information with a higher classification must be governed by more stringent security controls.

a. Risk Management must ensure that sensitive or personally identifiable information is strongly encrypted whenever traveling over any open, public or wireless network.

b. All non-console administrative access must use approved strong encryption protocols to protect the system from unauthorized access or confidentiality of the Imperial Community College District's information.

c. When passwords are transmitted over any network they must be encrypted using approved strong encryption.

3.2.2.4 Data-at-Rest

Encryption must be used for information that is considered "Confidential Data" when at rest throughout the operating environment.

3.3 Exceptions and Escalation

Any exceptions to this policy must be approved in writing by IT and applicable business unit management.

3.4 Compliance

Failure to comply with this policy and other security requirements in the organization can result in disciplinary action, up to and including termination of employment or contract, and the possibility of civil and criminal liability.

3.5 Additional Definitions

N/A

3.6 Related Policies

N/A

3.7 Related Procedures and Standards

- [Information Classification Guidelines]
- [Password Standards]

4.0 OPERATIONS MANAGEMENT POLICY

Effective Date	*December 07, 2018*
Revision Date	
Policy Version	
Policy Owner	
Executive Sponsors	

This document applies to:

All employees, contractors, and third parties of the afore mentioned entities must support the Information Protection program detailed herein.

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

4.1 PURPOSE

Information systems must be adequately configured, operated, and maintained in order to ensure confidentiality, integrity, and availability. Risk assessments associated with confidentiality, integrity, and availability must be conducted on a regular basis to ensure that appropriate controls are in place to adequately protect all information systems and assets. In addition, monitoring capabilities and technical vulnerability management processes must be implemented, providing the capability of proactively detecting vulnerabilities or events related to the confidentiality, integrity, or availability of information systems and assets.

4.2 POLICY STATEMENT

4.2.1 Operational Procedures and Responsibilities

The development, production, and updating of software (including microcode, firmware, etc.) must be properly managed to ensure availability and security of all information systems. The Imperial Community College District policy is to only use supported versions of any software.

4.2.1.1 Responsibilities for documenting Operating Procedures

a. Documented operating procedures must be established and available to those who require access to them. Procedures must be documented that include but are not limited to:
   - Backup and restore
   - Asset maintenance
   - User administration
   - Data center management
   - System build and configuration
   - Storage and capacity planning
   - Change management
   - Security incident management
   - Problem management
   - Contract management

b. Service Owners must ensure that all system scheduled jobs and dependencies are documented. This documentation must include handling procedures in case of failure or error.

c. Service Owners must ensure that all system restart and shutdown procedures are documented. Restart and shutdown procedures, system validation or verification procedures, and emergency contact information must be available for operations personnel.

d. Service Owners must maintain contact information for relevant external parties responsible for any information system.

e. Changes to the formal operating procedures must be approved by appropriate management.

4.2.1.2 Change Management

All changes to assets in the technical environment must follow the appropriate change management policies and procedures. Refer to Imperial Community College District Change Management Policies and Procedures.

4.2.1.4 Management of Removable Computer Media

All removable media containing “internal” classified or above data must be stored securely and tracked appropriately during transit.

a. IT must ensure that an authorization list for physical access to media is maintained. Only employees requiring access to perform their job functions may be granted physical access to the media. The authorization list must be reviewed periodically for appropriateness.
b. Information Owners must ensure that all media containing “internal” classified or above data including paper and digital media, are stored in a physically secured and environmentally controlled area. Any media leaving the facilities must be authorized by the Information Owner. Media containing Confidential Data, including cardholder data, should be accounted for with an audit log. Media content that is no longer required must be securely erased or physically destroyed using procedures approved by Cabinet.

c. IT must ensure strict control over media containing cardholder data. Specifically, media inventory logs of all cardholder data must be maintained and an inventory must be taken on at least an annual basis.

4.2.2 Risk Assessment & Risk Acceptance

Risk assessments must be performed periodically across the environment to determine, address, and mitigate security deficiencies.

4.2.2.1 Assessing Information Security Risks

Management must employ risk assessment and analysis methods to ensure adequate controls are in place for all areas of responsibility.

a. Risk assessments, under the direction or coordination of IT must be performed annually.

b. IT are responsible for defining the risk assessment process. The risk assessment process must allow for the systematic identification, prioritization, and management of information security risks.

4.2.3 Systems Planning and Acceptance

All information systems must be monitored to identify areas where additional capacity is necessary to continue to support the business. Any changes necessary must follow an approved change management process.

4.2.3.1 System Acceptance

Management must ensure that acceptance criteria for new systems, upgraded systems, and new versions are clearly defined, agreed upon, documented, and tested.
The following must be included in the acceptance criteria:

- System requirements and objectives clearly defined
- Security controls agreed upon
- Determination of impact to the overall security and technical architecture
- Computer performance and capacity requirements
- Business continuity
- Disaster recovery
- Testing of operating procedures
- Training requirements for operational and user support

4.2.4 Media Disposal

Procedures for handling and disposing of media in any form (including removable media and system hardware) must be properly documented and followed by all employees, contractors, and third parties.

4.2.4.1 Disposal of Hardware and Removable Media

All hardware and removable media containing Imperial Community College District information must be disposed of securely.

a. Procurement must ensure that electronic information storage devices (e.g., hard drives, tapes, USB sticks, removable hard disks, floppy disks, CD's, DVD's) are disposed of in a manner commensurate with its information classification. All electronic storage devices must be electronically wiped by a process such that data on the storage device cannot be recovered.

b. Procurement must ensure external firms responsible for disposing of any type of information are held to the standards of the third party contracts. This includes confidentiality agreements and adequate security controls.

c. Procurement must ensure that media containing sensitive data is destroyed when it is no longer needed for business or legal reasons.

d. Procurement must ensure that a log of all disposed of hardware and removable media items that contained sensitive data be kept and maintained.

4.2.5 Monitoring

Logging must be enabled for all information systems. The logs must be time-synchronized and monitor system use for all users, including administrators.

4.2.5.1 Monitoring of System Use

All systems must follow monitoring and logging requirements based on risks associated with the system.

a. Service Owners must ensure that logging is captured for the following types of events:
   - Failed or rejected actions performed by users
   - Failed or rejected attempts to access data or resources
   - Anti-Malware software alerts
   - File integrity monitoring system alerts
   - Intrusion detection and prevention system alerts

b. Service Owners must ensure that system logs are sent to a central location for monitoring by Information Technology

c. Information Technology must ensure that monitoring for system alerts and failures capture the following details:
   - Alerts or messages from consoles
   - Exceptions in system logs
   - Alarms generated by network management devices
   - Alarms generated by access control systems
   - Accessing and alteration of audit log information

d. Information Technology must use automated logging tools to monitor events, specifically:
   - All individual accesses to sensitive data
   - All actions taken by any individual with root or administrative privileges
   - Access to all audit trails
   - Invalid access attempts
   - Use of identification and authentication mechanisms
   - Initialization of the audit logs
   - Creation and deletion of system-level objects
   - IT must ensure that intrusion detection and prevention systems be used to monitor select zone boundaries in the network such that alerts are generated for suspected malicious activity.

4.2.5.2 Audit Logging

All audit logs must be maintained as determined by system and business requirements.

a. Service Owners must ensure that procedures for managing audit trail and system log information are established.

b. Information Technology must ensure that logs for systems identified as performing security-related functions (e.g., intrusion detection/prevention systems, identity management systems, firewalls, etc.) are reviewed on a regular basis. Operations logs must be archived and available for independent verification.

c. Information Technology must ensure that all audit trail log files for systems containing Highly Confidential or Sensitive Regulated Data are stored for a minimum of one year, and that three months of log data is readily available.

d. Information Technology must ensure that where audit trail events are recorded, log entries include, but are not limited to, the following information:
   - User identification
   - Type of event
   - Date and time
   - Success or failure indication
   - Origin of event
   - Identity or name of affected data, system component, or resource

e. Service Owners should track all reports of errors or problems with information processing or communication systems. The records must include at least the following information:
   - Name of person reporting event
   - Date/time of event
   - Description of error/problem
   - Name of party responsible for problem resolution
   - Description of initial operations response
   - Name of operations person entering event report
   - Description of problem resolution
   - Date/time of resolution

4.2.5.3 Protection of Log Information

All log files must be protected by security controls to prevent unauthorized changes or deletions.

a. Service Owners must ensure that security controls are implemented to protect against unauthorized log alteration or deletion.

b. Service Owners must ensure that the viewing of audit trails is limited to those with a specific job-related need to view those files.

c. Service Owners must ensure that all audit trail log files, including those from externally facing systems hosted in the DMZs, are backed up to a centralized log server located within the internal network to prevent manipulation.

d. Service Owners must employ capabilities to detect changes to log data to ensure that data cannot be changed without generating alerts.

4.2.5.4 Clock Synchronization

All information processing systems must synchronize system time with a standardized time source.

a. System Administrators and Network Administrators must ensure that information processing systems and devices be configured to utilize an agreed standard and synchronized with an accurate time source.

4.2.6 Malicious Software Detection

Malicious software detection capabilities must be installed and properly configured and maintained on information systems.

4.2.6.1 Detection Software and Product Configuration

All systems within the technical environment must utilize an anti-malware solution if available and supported.

a. Open System Services must define and implement an anti-malware product configuration capable of detecting and removing known malicious software.
b. System Administrators must ensure that all systems utilize approved anti-malware software.

c. System Administrators must ensure that all anti-malware mechanisms are current, actively running, and capable of generating alerts and audit logs.

d. Open System Services must ensure that anti-malware software programs are configured in a central location and deployed to systems from that location.

e. Open System Services must ensure that users do not have access to modify the anti-malware product configuration.

4.2.6.2 Product and Definition Updates

All anti-malware software updates must be implemented within an agreed upon timeframe.

a. Open System Services must ensure that anti-malware software product are updated in a timely manner after the software manufacturer has released any new patches, version upgrades or updates.

b. Open System Services must ensure that any anti-malware software that relies on frequent updates such as definition files, signature files or other updates that support the ability to detect new threats are updated on a schedule as recommended by the software manufacturer.

4.2.7 Technical Security Vulnerability Management

Roles and responsibilities for managing and addressing technical vulnerabilities must be assigned throughout the organization.

4.2.7.1 Roles and Responsibilities

a. Information Technology must establish processes to identify, evaluate, prioritize, and resolve security vulnerabilities.

b. Information Technology is responsible for identifying and distributing information on events, incidents, threats, and vulnerabilities to internal parties related to information systems and software.

c. Service Owners, System Administrators and Network Administrators must define and maintain accurate lists of contacts for each technical platform to facilitate resolution of identified issues. All operational groups must provide these lists to Information Technology anytime there is a change or addition.

d. Information Technology is responsible for maintaining the records of the analysis produced by the vulnerability management processes.

e. Information Technology is responsible for the evaluation of vulnerability risk and communicating changes as appropriate.

f. Information Technology must ensure that the vulnerability management process is reviewed on an annual basis.

g. Service Owners, System Administrators and Network Administrators are responsible for developing processes for asset management, classification, and prioritization of systems in support of the vulnerability management process. This includes a detailed asset inventory with appropriate documentation to facilitate prioritization and implementation of vulnerability assessment and remediation activities.

4.2.7.2 System Security Baselines

Service Owners, System Administrators and Network Administrators must create and maintain security baselines for all system components. These baselines must address all known security vulnerabilities and be consistent with industry accepted system hardening standards.

4.2.7.3 Vulnerability Management Task Force (VMTF)

IT will meet, at least monthly (as needed), to discuss required patches, identified vulnerabilities, and remediation efforts in support of the vulnerability management program.

4.2.7.4 Patch Methodology

IT will assess the criticality of vulnerabilities and patches as they are released for applicability and risk to information systems.

4.2.7.5 Vulnerability Scanning

IT will own and maintain the system by which system scanning is performed. Service Owners or their designee(s) will be provided access to this system to perform, as needed, vulnerability scans of organization-wide information assets.
Service Owners, System Administrators and Network Administrators are responsible for the resolution of vulnerabilities identified on information systems.

4.2.7.6 Vulnerability Scan Frequency

All information assets must have regularly scheduled scans and must be scanned after significant changes. The minimum scan frequency for each asset is monthly.
IT must conduct information asset discovery scans on a regular basis to identify new and unauthorized assets introduced into the technical environment.

4.2.7.7 Vulnerability Resolution

Vulnerability scanning will result in issues identified that must be resolved. The timeline required to address any vulnerabilities will be determined by the severity of the vulnerability and the business criticality of the information asset.

IT will be responsible for the tracking of critical and high risk vulnerabilities as well as the resolution timeline.

4.2.7.8 Vulnerabilities with No Third Party Security Patch

Vulnerabilities will exist without the availability of a third party security patch. In other cases a security patch may exist but does not function correctly or cannot be immediately applied to systems. For such cases, mitigating controls must be implemented in order to reduce the overall risk to an acceptable level. Service Owners affected by such cases must work with IT and Information Owners to determine appropriate mitigating controls to meet the acceptable level of risk.

4.2.8 Backup

Information backup schedules and procedures must be employed based on information criticality and classification.

a. If backups are performed at the server or host level, the backup schedule of the most critical application on the server as determined by the Information Owners or an assigned delegated Information Custodian must determine the backup frequency of the server.

b. Information Owners or an appointed Information Custodian must develop off-site backup rotation and retention schedules for each application.

c. Each Service Owner must have documented backup and recovery procedures.

d. Users must backup critical files by leaving the files in their “My Docs” folder which is backed up on a scheduled basis. This includes all user data created on workstations (e.g., files created in Microsoft Office).

e. IT must ensure that backups of all critical applications are sent off-site to a remote location on a schedule designed to meet the specific application recoverability requirements. The remote location must have appropriate security controls in place, including physical and environmental protection.

f. Information stored on backups classified as “internal” or higher must be encrypted.

4.3 Exceptions and Escalation

Any exceptions to this policy must be approved in writing by IT and applicable business unit management.

4.4 Compliance

Failure to comply with this policy and other security requirements in the organization can result in disciplinary action, up to and including termination of employment or contract, and the possibility of civil and criminal liability.

4.5 Additional Definitions

N/A

4.6 Related Policies

- Patch Management Policies (v2.0)

4.7 Related Procedures and Standards

- Change Management Policies and Procedures
- Change & Deployment Risk Mitigation (CDRM) scheduling and approval process
- Cyber Incident Response Plan
- Data Incident Response Plan

5.0 DEVICE BUILD AND CONFIGURATION MANAGEMENT POLICY

Effective Date	*December 07, 2018*
Revision Date	
Policy Version	
Policy Owner	
Executive Sponsors	

This document applies to:

All employees, contractors, and third parties of the afore mentioned entities must support the Information Protection program detailed herein.

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

5.1 PURPOSE

A set of well-defined, organization-wide device build and configuration management controls must be implemented to ensure the appropriate levels of information protection have been applied across all IT infrastructure supporting the business operations. Strong device build and configuration management processes must be implemented to ensure an appropriate analysis of IT requirements and allow for the application of controls based on the risks associated with each platform.

5.2 POLICY STATEMENT

5.2.1 Security Requirements Analysis and Specification

IT must ensure that all development projects for new or existing applications processing confidential data include a security assessment to document adherence or deviation from control requirements.

5.2.1.2 Platform and Device Build Standards

Platform and device build standards must exist to ensure proper security controls are placed on all devices that contain or transmit information.

5.2.2 Configuration Management

The Configuration Management Policy establishes a configuration management program framework for managing system changes impacting baseline configuration settings, system configuration, and security. The Configuration Management program helps document, authorize, manage, and control system changes impacting information systems.

5.2.2.1 Baseline Configuration

Service Owners, System Administrators and Network Administrators must develop, document, and maintain, under defined Change Management Policies and Procedures, a current baseline configuration of information systems and system components including communications and connectivity-related aspects of systems.
Service Owners, System Administrators and Network Administrators must update baseline configurations or create new baselines as information systems change over time to reflect current architectures. Baseline configurations include:

- Details about information system components
- Data flow diagrams
- Network topology
- The logical placement of those components within the system architecture

5.2.2.2 Configuration Change Control

The configuration change control process for critical information systems must include:

- Determining the types of changes to the system that are configuration-controlled
- Approving or denying configuration-controlled changes with explicit consideration for security impact analysis
- Documenting configuration change decisions
- Implementing approved configuration-controlled changes
- Retaining records of configuration-controlled changes
- Auditing activities associated with configuration-controlled changes
- Coordinating and providing oversight for configuration change control activities through Change and Deployment Risk Management weekly meetings

5.2.2.3 Security Impact Analysis

IT must analyze changes to information system configurations to determine potential security impacts prior to change implementation.

5.2.2.4 Access Restrictions for Changes

Change control procedures must:

a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to any information system.
b. Maintain records/logs to ensure that configuration change control is implemented and to support after-the-fact actions should the organization discover any unauthorized changes.

5.2.2.5 Configuration Settings

Change control procedures must:

a. Establish and document configuration settings for information technology products utilized within the information system using security configuration checklists (e.g., lockdown and hardening guides, security reference guides, security technical implementation guides) that reflect the most restrictive mode consistent with operational requirements and meet IT's defined policies.

b. Identify, document, and approve any deviations from established configuration settings for information system components based on operational requirements.

c. Monitor and control changes to the configuration settings per the Change Management Policies and Procedures.

5.2.2.6 Software Usage Restrictions

Service Owners, System Administrators and Network Administrators must:

a. Ensure Imperial Community College District uses software and associated documentation in accordance with contract agreements and copyright laws.

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

5.3 Exceptions and Escalation

Any exceptions to this policy must be approved in writing by IT and applicable business unit management.

5.4 Compliance

Failure to comply with this policy and other security requirements in the organization can result in disciplinary action, up to and including termination of employment or contract, and the possibility of civil and criminal liability.

5.5 Additional Definitions

N/A

5.6 Related Policies

N/A

5.7 Related Procedures and Standards

- Change Management Policies and Procedures

6.0 NETWORK SECURITY POLICY

Effective Date	*December 2018*
Revision Date	
Policy Version	
Policy Owner	
Executive Sponsors	

This document applies to:

All employees, contractors, and third parties of the afore mentioned entities must support the Information Protection program detailed herein.

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

6.1 PURPOSE

Network infrastructure must be configured securely in order to protect information assets and maintain network integrity and availability. All employees, contractors, and third parties must ensure that specific processes are in place and Imperial Community College District networks are only accessible to authorized parties.

6.2 POLICY STATEMENT

6.2.1 Network Administration/Security Management

Documentation for properly securing network devices must exist and be followed when configuring and managing all network devices within the environment.

6.2.1.1 Device Configuration

Network device configuration standards must be established and followed to provide consistency in configuration and ensure security of the network.

a. Network Administrators are required to create and maintain technical configuration standards for all devices that make up the network infrastructure.

b. Network Administrators must ensure that security hardening is a component of the technical configuration standard.

c. Network Administrators must ensure that all device implementations and changes are performed and tested as described in the Change Management Policies and Procedures.

6.2.1.2 Network Documentation

Network configuration and topology must be adequately documented.

a. Network Administrators must maintain appropriate network documentation, including a high-level network diagram specifically noting inbound and outbound network connections, including wireless network components.

b. Network Administrators are responsible for maintaining network documentation including network diagrams, network segmentation, network address schemas and (internal and external) data flows between systems. Data flows must highlight the points at which cardholder data is transferred throughout the network including connections to external organizations.

c. This documentation must be kept current to reflect any changes to network infrastructure or business processes.

6.2.2 External Networks

All connections into and out of the internal network, including the DMZs, must be documented and managed.

6.2.2.1 Connection Approval

Any connections inbound or outbound, including but not limited to Cloud service providers and other external networks, must be properly documented.

a. Network Administrators must manage and implement a formal process for approving new external connections, inbound or outbound, to the internal network, specifically requiring approval from IT.

6.2.2.2 Demilitarized Zones

Demilitarized Zones (DMZ) and network segmentation must be used between networks and other untrusted networks.

a. Network Administrators must ensure that a Demilitarized Zone has been implemented in order to limit traffic into the network to only protocols that are necessary for the environment.

b. Network Administrators must ensure that any DMZ is configured such that inbound Internet traffic is only allowed into the DMZ, and that no direct inbound traffic is allowed between the Internet and the internal network.

c. Network Administrators must ensure anti-spoofing controls are in place to prevent spoofed address traffic from passing through external networks including the Internet into the DMZ.

d. Network Administrators must ensure that outbound traffic from the internal network to the Internet is restricted based on business need and as approved by IT.

e. Network Administrators must ensure that any database containing sensitive data is placed securely on the internal network and properly segmented from the DMZs.

6.2.3 Firewalls

All firewalls and their associated rules must be documented, approved, and managed.

6.2.3.1 Use of Firewalls

Firewalls must be deployed to restrict inbound and outbound connections to Imperial Community College District networks.

a. Network Administrators must ensure that firewalls are placed at each external connection including the Internet, between DMZs, between any DMZ and the internal network, and between internal network segments.

b. Open System Services must ensure that personal firewalls are implemented on all mobile devices (including laptops, tablets, smart phones and any device that is offsite or outside of Imperial Community College District properties).

c. Network Administrators must ensure that firewalls are installed and configured to deny or control all traffic between any wireless networks and other networks.

6.2.3.2 Rules Management

Firewall rules must be implemented to prevent unauthorized access to, from, and between segments of the Imperial Community College District network and must be reviewed regularly.

a. Network Administrators must ensure that all allowed traffic rules are appropriately documented and approved before implementation. All traffic inbound and outbound between network segments must be restricted to those connections required to conduct business.

b. Network Administrators must ensure that the use of all services, protocols, and ports allowed are documented with a specific business justification.

c. Network Administrators must review rule sets of all firewalls and routers that govern access to sensitive data environments every six months. This activity must include a review of specific ports, protocols and services allowed into the environment and proper documentation of the review.

6.2.4 Wireless Security

All wireless networking technology must be authorized, secured, managed and monitored.

6.2.4.1 Approval of Wireless Infrastructure

All wireless infrastructures (including controllers, access points, etc.) are the responsibility of IT.

a. Ad-hoc wireless networks are not permitted.

6.2.4.2 Use of Pre-Shared Keys

Wireless networks that require the use of pre-shared keys for authentication must have the key changed on a regular schedule and when any restricted wireless network key is exposed.

a. Publicly accessible wireless networks must have the pre-shared key changed on at least a six-month schedule.

b. Restricted wireless networks (Executive and Board Member) must have pre-shared keys changed on a regular basis.

c. Wireless networks that provide access to internal information assets must not use pre-shared keys. These networks must authenticate individual users with multi-factor authentication.

6.2.4.3 Unauthorized Access Point Detection

A periodic process must be in place to identify and remove unauthorized access points connected to Imperial Community College District network or systems.

a. IT must ensure that unauthorized access points are not deployed anywhere throughout Imperial Community College District network. IT must perform quarterly wireless scanning or deploy appropriate tools to identify unauthorized wireless access points. All suspected unauthorized access points must be investigated and disabled if determined to be unauthorized.

6.2.4.4 System Configuration

All wireless infrastructures must be configured securely to avoid unauthorized access to Imperial Community College District network.

a. Network Administrators must ensure that all wireless networks implement encryption, per Encryption Standards, to adequately secure traffic for wireless systems and users.

b. Network Administrators must ensure that proper procedures are followed to ensure that all wireless infrastructure components are kept up-to-date. This includes all software (including firmware).

6.3 Exceptions and Escalation

Any exceptions to this policy must be approved in writing by IT and applicable business unit management.

6.4 Compliance

Failure to comply with this policy and other security requirements in the organization can result in disciplinary action, up to and including termination of employment or contract, and the possibility of civil and criminal liability.

6.5 Additional Definitions

N/A

6.6 Related Policies

N/A

6.7 Related Procedures and Standards

- Encryption Standards
- Change Management Policies and Procedures

7.0 ACCESS CONTROL POLICY

Effective Date	*December 07, 2018*
Revision Date	
Policy Version	
Policy Owner	
Executive Sponsors	

This document applies to:

All employees, contractors, and third parties of the afore mentioned entities must support the Information Protection program detailed herein.

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

7.1 PURPOSE

All employees, contractors, and third parties must be positively authenticated and authorized prior to gaining access to all information assets. Access controls must be in place to ensure that access is provided to information based on role and business need. Appropriate access controls must be implemented in a manner commensurate with the classification level of the information being accessed.

7.2 POLICY STATEMENT

7.2.1 Business Requirement for Access Control

Access controls must be in place and documented for all information assets. Access must be granted only when required and restricted otherwise.

7.2.1.1 Access Control Responsibilities

a. System Administrators are responsible for ensuring that logical access controls are established, and that access controls are based on the business need and Risk Management.

b. IT is responsible for ensuring that access rights granted and revoked from systems are approved by management. Access rights granted to systems must be limited to the minimum access rights necessary for the user to fulfill their responsibilities as determined by their role.

c. IT must document user access authorization and approval for the specific privileges provided.

d. The Information Owner must work with IT to identify and remove access to information as soon as that access is no longer required.

e. The Information Owner and the user's Manager must ensure that access privileges are aligned with the needs of the business, assigned on a need-to-know basis, proper access lists are communicated and approved access termination processes are followed.

f. System Administrators must ensure that all access to computer systems is controlled by an authentication method involving a minimum of a username and password combination. The username and password combination must meet minimum lengths and complexity requirements as defined by the Password Standards to provide verification of the user's identity.

g. System Administrators must ensure that any special privileges granted to users on technical platforms (e.g., administration accounts, databases, applications, accounts that can override system, or application controls) are based upon job

function and necessity. These privileges must be granted on a need-to-have basis and formerly documented and approved.

7.2.2 User Responsibilities

All employees, contractors, and third parties must maintain a secure working environment to avoid theft of information or information systems.

7.2.2.1 Unattended User Equipment

a. Users must ensure that any workstation, laptop, tablet or mobile device is locked before leaving the system unattended, for example, by activating the password protected screen saver.

b. Cable locks must be securely fixed to non-removable furniture and connected to any laptop or tablet before left unattended. Cable locks must be connected to laptops or tablets and secured to a non-removable source before being left unattended.

c. Users must log off of information systems manually or automatically when no longer using the systems. This includes but is not limited to Imperial Community College District desktops, mobile devices, application sessions, servers and networking devices.

d. Company owned mobile devices must be protected at all times. Users must never leave laptops, tablets, smart phones or other devices in a car, checked baggage during travel or in other vulnerable locations.

7.2.3 User Identification

Employees, contractors, and third party users must have a unique identifier and be registered on the systems they use to conduct business. Additionally, initial account passwords must be changed at first login and safeguarded to avoid unauthorized access before first login.

7.2.3.1 User Identification

Users must provide their unique user identification prior to gaining access to any information assets.

a. IT must ensure that all users have their own unique username for access to the network and systems. Sharing of usernames and passwords is strictly prohibited.

b. IT must ensure that preexisting shared user IDs may only be used if there is a clear business case and are approved by both the Information Owners and Risk Management. The Information Owners must be aware of all the risks associated with using shared IDs such as the loss of individual accountability.

This risk must be accepted by the Information Owner and documented using the policy exception process. See section 8.3 of this document.

c. IT must ensure that all users that have access to privileged accounts have a different account for normal business use. Privileged accounts should not be used for normal business use.

7.2.3.3 Default Accounts

Default, system, and non-user accounts must be changed and the account details must be safeguarded.
Users including administrators must not use these accounts to access information systems.

7.2.3.4 Third Party Account Management

Security measures must be implemented to monitor the activity of third party accounts.
System Administrators must ensure that any accounts used by third parties for remote maintenance are only activated during the time period needed to complete the current task.

7.2.4 Authentication

Authentication to all information systems must meet minimum lengths and complexity requirement standards set in the Password Standards in addition to strong session management.

7.2.4.1 Password Standards

Standards for the creation and distribution of first-time passwords must be documented and enforced.

a. IT must ensure that security awareness training covers password procedures and policies to all employees, contractors and third parties.

b. Help Desk must ensure that specific procedures are implemented to verify a user's identity prior to conducting a password reset.

7.2.4.2 Inactive Accounts

IT must implement procedures to ensure that inactive accounts are disabled and removed in a timely manner.

7.2.4.4 Secure System Login

Controls must be in place to ensure user credentials are safeguarded throughout the login process.

7.2.5 Authorization

All users must be authenticated before being granted access to any system.

All information system accounts must be reviewed regularly in order to ensure proper authorization for access to the systems.

7.2.5.1 Review of User Access Rights

Information Owners are responsible for reviewing user access on a periodic basis and must promptly revoke or amend access rights when no longer required.

7.2.5.2 Privileged Access

Additional safeguards must be implemented to protect accounts of elevated or privileged access.

a. IT must ensure that all privileged access accounts have an identified account owner.

b. Prior to access being granted, IT is responsible for ensuring that the authorization for privileged access is obtained from the Information Owner.

c. IT and Information Owners must periodically review privileged accounts and revoke any privileges that are no longer required.

d. Privileged administrative access to PCI systems must utilize multi-factor authentication.

7.2.6 Remote Access

Security controls must be implemented and enforced for all devices providing remote access capabilities to adequately restrict access to the network and infrastructure.

a. Network Administrators must ensure that all remote access into the network use multi-factor authentication (e.g., tokens).

7.3 Exceptions and Escalation

Any exceptions to this policy must be approved in writing by IT and applicable business unit management.

7.4 Compliance

Failure to comply with this policy and other security requirements in the organization can result in disciplinary action, up to and including termination of employment or contract, and the possibility of civil and criminal liability.

7.5 Additional Definitions

N/A

7.6 Related Policies

- VPN Policy

7.7 Related Procedures and Standards

- Password Standards

8.00 THIRD PARTY SECURITY POLICY

Effective Date	*December 07, 2018*
Revision Date	
Policy Version	
Policy Owner	
Executive Sponsors	

This document applies to:

All employees, contractors, and third parties of the afore mentioned entities must support the Information Protection program detailed herein.

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

8.1 PURPOSE

Imperial Community College District must ensure that contracted third parties apply equally stringent controls in managing and protecting all sensitive data shared with them. Adequate contracts and due diligence processes protecting Imperial Community College District brand and its customers must be in place. Information shared with third parties must be limited to the minimum amount necessary in order to perform the contracted services.

8.2 POLICY STATEMENT

8.2.1 Third Parties

Standard contractual language must exist specifically ensuring that third parties have in place the same or more rigorous information security controls.

8.2.1.1 Identification of Risks Related to External Parties

All connections to third parties must be managed to ensure adequate security controls are in place. Risk assessment activities defined by IT must take place for all connections to Imperial Community College District information assets.

a. Where business needs require a direct connection between Imperial Community College District and a third party network, IT must be involved to determine security implications and control requirements.

b. IT must ensure that all inbound connections from third parties are limited to specific hosts and specific applications. External parties must be granted limited access to computers or networks to perform contracted services as required.

c. IT must ensure that all outbound connections to third parties are restricted to only those users, hosts and applications required.

d. All contract personnel must sign a Non-Disclosure agreement including a statement indicating that they will adhere to the information protection third party policy and standards. For third party service providers, a blanket confidentiality agreement must be signed and retained. The Business Owner responsible for the contract must ensure that third parties sign Non-Disclosure or Confidentiality Agreements.

e. IT must ensure that all third party personnel who require access to information assets have a manager sponsoring them. Access will not be granted until formal authorization is obtained from the business sponsor.

f. IT must set a minimum requirement that third party service providers adhere to the same access restrictions as internal users when accessing information assets.

8.2.1.2 Addressing Security in Third Party Agreements

All contracts between IT and third parties must include specific IT provisions and the right to audit.

a. If a third party is managing any non-public data, the department managing the contract will maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the private data they possess.

b. To the extent possible, all contracts must include a "Right to Audit" clause ensuring that Imperial Community College District or an authorized representative may physically, logically and electronically evaluate a third party's control environment at any time.

c. Any third party working under contract must immediately notify Imperial Community College District manager responsible for the contract if a security incident is confirmed to or is suspected of occurring. A security incident is any event that has the potential to impact the confidentiality, integrity, or availability of data or computing resources. Additionally, any employee who is aware of security violations by third parties must report them to IT and the VP of that area.

8.3 Exceptions and Escalation

Any exceptions to this policy must be approved in writing by IT and applicable business unit management.

8.4 Compliance

Failure to comply with this policy and other security requirements in the organization can result in disciplinary action, up to and including termination of employment or contract, and the possibility of civil and criminal liability.

8.5 Additional Definitions

N/A

8.6 Related Policies

N/A

8.7 Related Procedures and Standards

- Information Security Risk Assessment
- Vendor Risk Management Program
- Vendor Risk Management Guidebook
- Vendor Risk Management Process Procedure
- Third Party Security Review Report

9.0 COMPLIANCE POLICY

Effective Date	*December 07, 2018*
Revision Date	
Policy Version	
Policy Owner	
Executive Sponsors	

This document applies to:

All employees, contractors, and third parties of the afore mentioned entities must support the Information Protection program detailed herein.

Changes	Approving Manager	Date
Initial Draft	Technology Planning Committee	12/07/2018

9.1 PURPOSE

Employees, contractors, and associated business processes must fully comply with the Information Protection Operation Policy in addition to any other legal or industry-specific regulatory requirements.

9.2 POLICY STATEMENT

9.2.1. Licensing of Software

All software used must be appropriately licensed and in compliance with Imperial Community College District's software license agreements.

9.2.2. Records Retention

All information systems will be governed by AP 3310

9.3 EXCEPTIONS AND ESCALATION

Any exceptions to this policy must be approved in writing by IT and applicable business unit management.

9.4 COMPLIANCE

Failure to comply with this policy and other security requirements in the organization can result in disciplinary action, up to and including termination of employment or contract, and the possibility of civil and criminal liability.

9.5 ADDITIONAL DEFINITIONS

- N/A

9.6 RELATED POLICIES

- N/A

9.7 RELATED PROCEDURES AND STANDARDS

- N/A

This Page Intentionally Left Blank