# Information Security Program

| Version | Date | Framework References | Informative References | Approver/s |
|---|---|---|---|---|
| 1.0 | | ID.GV-1 | ISO/IEC 27001:2013 A.5.1.1 | Security Workforce Action Team |

**Introduction**

An Information Security Program details the acceptable processes and practices for an organization to follow in order to protect the interests of CCRI, as well as those of our students, third-parties, employees, and other entities. This Information Security Program is required reading for all users who are granted access to CCRI's assets upon hire (before being granted access to the assets) and then annually. CCRI's assets include anything owned or leased by CCRI for operational and business use, to include (but not limited to) systems, data, computers, personal devices, applications, facilities, connections, individuals, documentation, and electronic media, whether located on CCRI premise or off-site, and all CCRI locations where cardholder data is present.

All users are required to follow this Information Security Program at all times, unless a prior exception request has been reviewed and approved by VP of Business Affairs.

**Scope**

This Program applies to CCRI employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at CCRI, whether conducting activities on CCRI premises or off-site.

This Program applies to all systems, applications, and equipment owned or leased by CCRI whether located on CCRI premise or off-site, and all CCRI locations where cardholder data is present.

**Distribution**

This Program is to be distributed to all users granted access to any CCRI asset, to include CCRI employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

**Acknowledgement**

This Program is to be reviewed and acknowledged via signature by all users granted access to any CCRI asset, to include CCRI employees, third-parties, service providers, contractors, temporary employees, and/or other staff members. Signature must be obtained from the user prior to their initial access.

Acknowledgements are to be incorporated in to the new hire orientation by HR and the purchasing procurement process by purchasing

**Exceptions**

There are no exceptions to this Program. Requests for exceptions may be submitted to the CCRI Security Workforce Action Team which will forward to the VP of Business Affairs for approval.

**Violations**

Individuals found to have violated this Program may be subject to disciplinary action and possible termination of employment.

**Review Schedule**

This Program will be reviewed on an annual basis by the CCRI Security Workforce Action Team.

# Table of Contents

## 1.0 Why Information Security?

Information Security helps to:

- Safeguard CCRI's assets such as systems, data, computers, personal devices, applications, facilities, connections, individuals, documentation, and electronic media as well as assets belonging to CCRI customers, third-parties, employees, and other entities.
- Support CCRI's compliance with regulations, standards, and/or laws.
- Reduce risk to CCRI's assets.
- Support the integrity of information and data.

## 2.0 No Expectation of Privacy

Users are to expect that CCRI may access or view their actions using CCRI systems at any time and without prior notification. CCRI reserves the right to disclose any user actions and communications to law enforcement or other parties without prior consent from the user.

## 3.0 Legal and Compliance Requirements

As an organization, CCRI is required to comply with several regulations, standards, and/or laws, to meet third-party contractual requirements, and consumer compliance efforts.

**Payment Card Industry Data Security Standards (PCI DSS):** Industry requirements put forth by the card brands and acquirer banks to safeguard cardholder data

## 4.0 Roles and Responsibilities

**Users are required to:**

- Follow CCRI policies & controls at all times.
- Help CCRI meet and maintain compliance with this Information Security Program.
- Acknowledge their agreement with this Information Security Program before they first access CCRI's assets.
- Be aware of their role in supporting CCRI's Information Security Program.
- Comply with relevant regulations, standards, and/or laws governing CCRI and CCRI's customers, third-parties, and other applicable entities.
- Safeguard CCRI's assets such as systems, data, computers, personal devices, applications, facilities, connections, individuals, documentation, and electronic media per the controls within this Information Security Control.
- Report any deviation from this Information Security Control to their direct supervisor immediately.

**Supervisors are required to:**

In addition to the above requirements:

- Ensure that their reports follow CCRI policies & controls at all times and understand their roles.
- Designate owners (if not themselves) for CCRI assets such as systems, data, computers, personal devices, applications, facilities, connections, individuals, documentation, and electronic media under their control and management.
- Work with other groups to implement and maintain security controls for assets.
- Participate (as needed and directed) in incident response procedures.

**CCRI IT Department and/or Asset Owner/Managers are required to:**

In addition to the above requirements:

- Manage the definition of user access to the assets under their control and management.
- Receive alerts from users and other systems ~~24/7/365~~.
- Administer user accounts, including additions, deletions, and modifications.
- Monitor and control all access to data.
- Ensure that user access to their assets follows the principle of "least privileges" where access is determined upon their function or role).
- Verify that assets are protected sufficiently with the security controls.
- Properly assess and classify assets.
- Appoint a backup for essential duties when they are unavailable.

**Security Workforce Team is required to:**

In addition to the above requirements:

- Oversee and manage compliance with CCRI's policies and controls.
- Perform risk assessments.
- Evaluate and select solutions that reduce risk to CCRI assets.
- Write and distribute security controls to all users (as defined in the Introduction).
- Monitor and analyze security alerts and information for distribution to appropriate personnel.
- Define and deploy incident response and escalation procedures.
- Develop and implement Security Awareness and Training programs.
- Provide direction to management on best security practices and recommended security controls and initiatives.
-

**Senior Management is required to:**

In addition to the above requirements:

- Champion best security practices from a "top down" approach.
- Take ultimate responsibility for safeguarding CCRI's assets such as systems, data, computers, personal devices, applications, facilities, connections, individuals, documentation, and electronic media.

- Accept residual risk resulting from assessment initiatives.

## 5.0 Individual Controls

### 5.1 Access Control

Without defined access privileges and controls, users would have access to systems and applications in CCRI's cardholder data environment, and have the ability to view, delete, and tamper with stored data, code, and configurations. Therefore, controlling who has access to what information and what actions are allowed to perform is vital to secure systems and applications transmitting, processing, and/or storing sensitive data from unauthorized access.

A careful review of each system and application should be performed based on results from risk assessment performed by CCRI, and user's granted access privileges based upon the principle of "business need-to-know" (where access is determined upon an individual's function or role). The general rule to follow is that all users start with no access privileges and are granted access to systems, applications, tools, etc. individually, as needed. All access granted is to be tracked in standard access/authorization forms, and reviewed on a semi-annual basis as users may: leave the company, temporarily need access to specific systems, or change positions where they no longer require the same access privileges.

Reference: Access Management Control.

### 5.2 Anti-Virus

Viruses, and associated spyware, adware, and malware, can infiltrate CCRI's network, causing incalculable damage to systems and applications transmitting, processing, and/or storing sensitive data.

Viruses can shut down complete systems; spyware can capture user actions and take screenshots of cardholder data; and malware can spread through your network, causing damage to CCRI, customers, and third-parties.

Anti-virus software must be deployed on all corporate servers, workstations, and gateways that are considered to be commonly affected by viruses. This means that Unix-based systems may not require anti-virus protection. (Anti-virus software for Unix is available so CCRI should determine whether it would be recommended to deploy such software for these systems based upon risk assessment results). The anti-virus software should be an up to date/current enough version that it protects against spyware and adware.

Reference: Anti-Virus Control

### 5.3 Change Management

Performing changes to systems and applications in CCRI's environment carries some level of risk, whether the change is a simple code change or applying the latest critical patch to a complete system reconfiguration. Attackers are aware of lax (or simply incorrectly performed) change control processes performed by organizations and have created specific attack methods which allow them to take advantage of vulnerabilities to successfully penetrate systems and applications and then transmitting, processing, and/or storing sensitive data.

A change should be made only when absolutely necessary and managed closely from inception to deployment into the production environment, complete with backout plans in case the change creates vulnerability.

Reference: Change Management Control.

### 5.4 Critical Technologies

Critical technologies include remote access, wireless, removable media, laptops, tablets, personal data/digital assistants (PDAs), and use of e-mail and the Internet. These are all tools used to access CCRI's network in a "non- standard" method, meaning they can be used remotely and not use a CCRI workstation in a CCRI location. Special care should be made when using these technologies as they are accessing CCRI's network from an unknown location, therefore safeguarding the connection to the network is critical. It's also important to limit the ability of users to access these technologies in order to protect cardholder data wherever it is transmitted, processed, and/or stored.

Reference: Critical Technologies Control

### 5.5 Data Retention

The retention period for assets and data sets are determined by legal, industry, financial, and/or regulatory requirements. In order to reduce risk, however, assets and data sets should not be retained longer than absolutely required in the cardholder environment.

Each asset and data set (both electronic and printed formats) should be reviewed by a legal point-of-contact to assess CCRI's legal and regulatory requirements to determine the length of retention. The same exercise should be performed by the system owner as well as management to assess its industry requirements for retention. When completed, an analysis should be performed with the guiding principle that the item should be retained for the least amount of time possible.

Reference: Data Retention Control

### 5.6 Equipment Protection

Equipment (to include hardware and cabling) supports the day-to-day operations of systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmission processing, and/or storage of data. Should the equipment be subjected to harsh conditions, intended or unintended misuse of liquids or other types of physical hazards and/or threats, its ability to function may be impacted, subsequently impacting the security of the environment.

Reference: Equipment Protection Control.

### 5.7 File Integrity

File integrity software is used to ensure that no modifications have been made to content, critical operating systems, executables, configuration, or audit logs for systems and applications transmitting, processing, and/or storing sensitive data. File integrity software must be used on all systems responsible for/involved in transmitting, processing, and/or storing cardholder data in the following places/functions:

Content files

Operating system critical files
System and application executables
System and application configuration files
System audit log files

Reference: File Integrity Control.

### 5.8 Firewall Configuration and Management

Firewalls are critical to the security of CCRI's data environment by filtering access to systems and applications transmitting, processing, and/or storing sensitive data.

Firewalls utilize established algorithms to allow or deny inbound and outbound network traffic between trusted and untrusted environments. Trusted environments include known zones that contain systems which transmit, process, and/or store sensitive data, and the internal network. Untrusted environments include Internet-facing access points, unknown environments, wireless networks, and zones which do not contain systems that transmit, process, and/or store sensitive data. Firewalls are required at all Internet connections (to protect against traffic coming in from outside of CCRI) and between internal network zones (should one zone contain sensitive systems while the other does not).

Reference: Firewall Configuration and Management Control.

### 5.9 Incident Response

Security controls work together to reduce risk in CCRI's environment. These controls include intrusion detection systems, file integrity software, firewalls, logging, and many others. Many of these security controls are also used to notify management whenever a suspected incident takes place or there is a system anomaly detected in CCRI's sensitive data environment. This allows management to promptly respond to and perform necessary activities to limit damage being caused. CCRI users also play an important role in supporting the incident response process, by reporting anomalies they are encountering, such as a suddenly slower computer, accidental viewing of unencrypted cardholder data in the clear, or a lost removable computer drive.

Reference: Incident Response Control.

### 5.10 Intrusion Detection/Prevention

An Intrusion Detection/Prevention System (IDS/IPS) detects suspected intrusions from outside the college (if the attacker has managed to bypass a firewall) or those originating from inside the network, then logs the event, and generates an alert. The IDS/IPS performs its function relying on updated signatures, which are patterns of common attacks, provided by the IDS/IPS vendor. Using these signatures, the IDS/IPS can then detect intrusions which follow the identified patterns before they can cause damage to systems and applications that transmit, process, and/or store sensitive data.

IDS differs from IPS where the former simply detects the suspected intrusion and sends an alert, but the latter actually stops the attack, reconfiguring the firewall, or disabling it. PCI requires that there is 24/7/365 response to suspected intrusions and attacks. If using an IDS, a member of Management needs to respond immediately to the suspected event and perform forensic, remediation, and then investigative

follow-up. Should an IPS be deployed, the IT Department needs to ensure that the attack has been blocked and perform investigative follow-up.

Reference: Intrusion Detection/Prevention Control.

### 5.11 Log Management

Logging enables CCRI to know who logged on to a system and when, and what actions did the user or application do. This is important to proactively monitor access to cardholder data and to identify anomalies, and also to review access should there be concern of an incident or breach to sensitive data being transmitted, processed, and/or stored.

Logging should be enabled on all systems where it is feasible to do so, which includes databases, servers, users desktops, applications (as applicable), networking equipment, wireless access points, etc.

Reference: Log Management Control.

### 5.12 Password Management

Passwords are the most common method of authenticating the identity of the user before allowing access to systems and applications in CCRI's data environment. The effective management of user passwords is critical to support systems and applications transmitting, processing, and/or storing sensitive data from unauthorized access.

The user is responsible for constructing strong passwords, following CCRI policies, and protecting the secrecy of their password. The CCRI IT department is responsible for enforcing password parameters using automated access control methodologies, to include the required length of passwords, reuse, lockouts, history, change upon first login, secure storage, and other security controls. In addition, the CCRI IT department is responsible for deploying additional authentication methods as those resources become available. (i.e: two-factor authentication for remote access or for privileged access to critical systems and applications).

Users may not share their passwords with any other parties, even at their direct request. The user should notify the IT department should they receive a request for their password to initiate the incident response plan. In addition, users must take additional precautions to protect the security of their passwords by not writing it down, making it something which is readily known, or keeping it stored in an accessible location.

Users should not write down their passwords or store them electronically, unless using a pre-approved password storage system. In addition, users may not 'cache' or select an option to remember their password when online, as this may store the password insecurely. The IT Group must store user passwords in a secure manner, protected from unauthorized access and in unreadable format.

Reference: Password Management Control.

### 5.13 Physical Security

An unauthorized person may cause physical damage to CCRI's cardholder environment, which can lead to assets and data being used inappropriately.

An individual may socially engineer their way into the facility, meaning, pretend to be an authorized individual or trick an employee into letting them in under false pretenses. Once inside, the individual may continue to ruse others into granting them continued physical access to secured locations or even logical access to systems and data.

All persons entering, or in the environment of, the CCRI Datacenter or any of CCRI's facilities or locations which transmit, process, and/or store cardholder data must follow these physical protection controls.

Reference: Physical Security Control.

### 5.14 Risk Assessment

The purpose and intent of CCRI's security program is to reduce risk as much as possible to CCRI's environment, while still enabling CCRI to meet strategic and business objectives. Defining the risk level of assets (systems, equipment, applications, data, users, etc.) is critical in order to define the level of security controls required to safeguard those assets from harm. As it is impossible to reduce risk to zero, there will always be an amount of residual risk left. It is up to the Security Workforce Action Team to review risks and make recommendations to the VP of Business Affairs who will review and accept this level of risk. The higher the risk level associated with an asset, the more intensive and comprehensive the layers of security protecting the asset are required for cardholder data being transmitted, processed, and/or stored.

Reference: Risk Assessment Control.

### 5.15 Secure Configuration

As demands on time, productivity, and operations increase, the focus on securely configuring systems and network devices may suffer a lack of attention or a heightened amount of exceptions granted. Common security vulnerabilities, such as default passwords not being changed or a port remaining open after an exception request expires, can open up holes for an individual to gain unauthorized access to systems and applications transmitting, processing, and/or storing sensitive data.

Each system and networking component should be included in the annual risk assessment initiated by the CCRI IT Department, and their configurations compared against documented best security practices and standards. These documents should keep a record of the baseline configuration of the system and network component and deviations reviewed on a quarterly basis to ensure that risk cannot be introduced into the environment.

Reference: Secure Configuration Control.

### 5.16 Security Awareness

Breaches can often be attributed to the actions performed by an organization's employee(s), whether they are intentional or unintentional. If people are not provided with awareness of their roles and responsibilities when it comes to protecting CCRI's assets and data, they cannot be held responsible for their actions or know how their actions impact the security of CCRI's data environment.

Users must receive security awareness training and sign an acknowledgment of their role in safeguarding CCRI prior to being granted physical and logical access to CCRI's environment.

All users that have access to critical data systems and payment card information, for the entire length of time they are, or remain, connected to CCRI's environment, must receive security awareness training on an annual basis. This training may be provided to all users at one time, or may be staggered to take place on an annual basis from the user's first day of employment or access granted. Training may occur in-person or via a computer-based training (CBT) format.
All newly hired employees are to receive training as part of their orientation regardless of job description. Attendance logs for those who attend security awareness training, both, provided upon hire and annually, must be kept by the functional area. Exceptions must be communicated to the user's manager with a defined period of time that the user must take the training. Should the user not take the refresher training within that period, they are to be found in violation of this control.

Reference: Security Awareness Control.

### 5.17 Testing and Scanning

Testing CCRI's systems and network is a critical component of protecting CCRI's sensitive data environment from threats and vulnerabilities.

New vulnerabilities are discovered on a daily basis. Attackers can take advantage of these avenues to launch malicious attacks against CCRI. Scans and penetration tests help find these problem areas proactively so they can be blocked. The difference between scans and penetration tests is that scans are performed using automated tools of CCRI's Internet Protocol (IP) addresses and report on vulnerabilities, rating them by level of criticality. Penetration tests are performed by trained individuals who are granted explicit permission by CCRI to actively try to penetrate systems and applications as if they are an attacker.

Reference: Testing and Scanning Control.

### 5.18 Third-Party Access and Management

Threats can be introduced to CCRI's environment simply by connecting a third-party without efficient security practices and controls in place. Should an attacker penetrate the third-party's network, they may route their way via the connected third-party into CCRI's network. In some cases, third-parties have privileged access (meaning they have direct access to cardholder data in the production environment), thus gaining unauthorized access to the cardholder data environment.

Should an unauthorized user obtain access to CCRI's network via this route, they may do so under the pretense of being the third-party and therefore potentially penetrate systems, applications, and other networks unnoticed to gain additional access to sensitive data. This can lead to a security breach, causing harm to CCRI's finances, operations, and brand name.

A third-party, in data security terms, may either transmit, process, and/or store sensitive data on behalf of CCRI, but also may be connected to perform non related functions. Therefore, it is important to safeguard

CCRI from attackers masquerading as an authorized third-party, as well as proactively validating the security controls and practices in place at connected third-parties.

There are several types of third-parties, the most common being resellers, point of sale (POS) providers, Information Technology support companies, software application developers and vendors, shopping cart vendors, off-site storage vendors, data center and Web hosting providers, and Service Providers (those companies which transmit, process, and store cardholder data on CCRI's behalf.

Reference: Third-Party Access and Management Control.

### 5.19 Time Synchronization

An accurate clock which synchronizes time across systems is critical to safeguard CCRI's cardholder data environment as identical timestamps support systems and applications transmitting, processing, and/or storing this sensitive data.

Identical system timestamps support the effectiveness and accuracy of several processes and technologies, to include services set to run at a specific time, log management and analysis, forensic investigations, server requests, commands, and more. It is common for system components to have their time begin to lag or change over an extended period of time. Subsequently, all system components need to maintain identical timestamps. A clock synchronization system needs to be implemented across all systems-in-scope, with a dedicated server or servers pulling the time from an established external time source. Those servers, in turn, distribute the time to the other systems.

Reference: Time Synchronization Controls.

### 5.20 Cardholder Data

All sending of unencrypted Primary Account Numbers by end-user messaging technologies (i.e., email, instant messaging, and chat) are strictly prohibited.

All paper that contains cardholder data (such as a CWCE mail in form) is to be identified and physically secured until the payment is processed. Upon payment, the cardholder data is to be destroyed immediately by shredding the entire document or by crossing out the cardholder data with a redactor pen or stamp **(ball point pens or markers are not redactor pens).**

A list of cardholder devices is to be maintained by each processing area. Devices are to be physically secured at all times and periodically inspected. Employees are to report suspicious behavior or device tampering to their supervisor immediately.

Reference: Payment Card Industry Data Security Standards (PCI DSS)

### 5.21 Usage of CCRI Assets

CCRI's assets such as systems, data, computers, personal devices, applications, facilities, connections, individuals, documentation, and electronic media may only be used to support CCRI business and

operations. Users may not use CCRI assets for personal use, unless authorized by their manager. Use of CCRI assets must always be in a professional manner.

The following actions are never permitted when using CCRI assets:

- Compromising confidentiality, integrity, and availability of CCRI assets.
- Threatening, obscene, profane, offensive language or content.
- Harassing or violating others.
- Gaming, file sharing, music, and other activities.
- Work for another business, commercial venture, or non-CCRI- sponsored activity.
- Advertising, purchasing, selling, and transacting non-CCRI initiatives.
- Any illegal activities.

Reference: Usage of Assets Control

## 6.0 User Signature

Users are to review this Information Security Program and sign prior to gaining access to CCRI's assets and network.

___ New User

User Name:

User Title:

User Company:

User Email:

User Phone Number:

User Signature:

Date: