Cy-Fair Sports Association Information Security Policy

1.0 Overview

The need for information security is particularly important in Cy-Fair Sports Association's (CFSA) overall IT and Business operations. To be effective, information security must be a team effort involving the participation and support of everyone at CFSA.

2.0 Purpose

The purpose of this document is to define the policies and procedures in place to maintain effective and comprehensive information security at CFSA.

3.0 Scope

All CFSA personnel including but not limited to full-time or part-time employees, volunteers, contractors, and consultants must comply with the information security policies found in this security document.

This policy applies to all computer and network systems owned by and/or administered by CFSA. Similarly, this policy applies to all platforms (operating systems), all computer systems (personal computers through servers), all wireless devices (phones and tablets), and all application systems (whether developed in-house or purchased from third parties).

4.0 Policy

4.1 Classification of Users

In order to define user responsibility, the following categories of users have been defined. The term "user" in this document may refer to one, several, or all of these categories.

Owner — The persons responsible for the acquisition, development, and maintenance of production systems and applications that process CFSA information.

Custodian — The persons in physical or logical possession of either CFSA information or information that has been entrusted to CFSA.

End User — All persons who accesses CFSA information in the course of fulfilling their job functions.

3rd Party — Persons not volunteering for or employed by CFSA.

4.2 Classification of Information

All CFSA information may be described by the following categories:

Private — Need-to-know information specific to CFSA and/or its customers.

Public — Information that may be disseminated to the general public

All information must be assigned an owner and/or custodian who will be responsible for the secure access of such information. Private information must be handled appropriately to mitigate loss and exposure of data. Private information may only be distributed or shared via secure methods. Data at rest must be secured via access controls, password protection, encryption, or a combination thereof.

4.3 Authorization

All CFSA users must be limited to only the "need-to-know" information required for them to fulfill their job functions. To further mitigate risk, duties are separated accordingly where personnel limitations are not a factor.

Unless it has been specifically designated as public, all CFSA's internal information must be protected from disclosure to third parties. Third parties may be given access to CFSA's internal information only when a demonstrable need-to-know purpose exists, when a CFSA non-disclosure agreement has been signed, and when such a disclosure has been expressly authorized by the CFSA President or his/her designee.

4.4 Authentication

To implement the need-to-know process, CFSA requires all users accessing multi-user information systems have a unique user-ID and a private password. These user-IDs must then be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each worker/volunteer is personally responsible for the usage of his or her user-ID and password. Passwords must not be stored in readable form and may not be shared with other users.

With the exception of Internet web sites, intranet web sites, and other systems where all regular users are intended to be anonymous, users are prohibited from logging into any of CFSA's system or network anonymously. When users employ system commands that allow them to change active user-IDs to gain certain privileges, they must have initially logged-in employing user-IDs that clearly indicated their identities.

4.5 Accounting

All users must make reasonable efforts to document the following

- Changes to systems and personnel that access CFSA information
- Transactions detailing the access of CFSA information

New Users, Transfers and Terminations

All changes to systems access and personnel must be submitted to the VP of IT by the Sports Commissioner or Board representative in writing. Access requests or changes to any critical business applications must be approved by the application owner. IT will maintain a list of the critical business applications and the corresponding application owners and will act as the direct liaison with the application owner.

Requests for new users will not be processed until the new user is officially an employee or volunteer. As the VP of IT completes the access of the user to the requested applications, the request will be archived within the VP of IT's email for future verification.

In the event of an employee or volunteer termination, the appropriate committee notify the VP of IT. In the case of an immediate termination, the committee must notify the VP of IT immediately to have access disabled. Based on the request, all access to systems of the terminated users is disabled immediately. After 30 working days, terminated accounts are deleted from the system, unless instructed otherwise by the Committee.

The VP of Information Technology, will perform a semi-annual reviews of the user access to their respective systems to ascertain the appropriateness of their access. Accounts with administrative access to the network, domain, servers, and firewalls will be reviewed by the VP of IT on a quarterly basis.

4.6 Appropriate Usage Policy

CFSA's information systems are intended to be used for business purposes only, and users should perform only those activities for which they are authorized. Incidental personal use is permissible if the use does not interfere with business activity. For a comprehensive overview, refer to the CFSA Acceptable Use Policy.

4.7 Risk Mitigation Policy

Network Access

All in-bound session connections to CFSA's computers from external networks (Internet, public dial-up lines, etc.) must be protected with an approved dynamic password access control system and/ or firewall system.

CFSA's workers must not establish outbound connections with external networks (including Internet Service Providers) unless these connections have been approved by the VP of IT.

All CFSA's computers that store sensitive information, and that are permanently or intermittently connected to internal computer networks must have a password-based access control system. All multi-user systems throughout CFSA must employ an automatic log-out or lock the screen after a defined period of inactivity.

Users with CFSA assigned laptops may work remotely. All users may work with web email from external locations with internet access. In these instances, telecommuters must continue to comply with all existing CFSA security policies and guidelines.

Application Integrity

All 3rd party software and applications used by CFSA must have a valid license for use. Users must not copy software provided by CFSA to any storage media, transfer such software to another computer, or disclose such software to outside parties without advance permission from the VP of IT. Ordinary back-up copies are an authorized exception to this policy.

Anti-virus software must be used to scan all software and data files coming from either third parties or other CFSA groups.

Detection, Response, and Recovery

The VP of IT must have a documented procedure to periodically audit information systems for security violations, to limit the effects of those discovered, and perform any subsequent data restoration necessary. As part of the data restoration requirement, all critical information must be backed up regularly and kept in a secure location. Data saved locally to a computer is not backed up, therefore all critical data must be saved to network servers of file share equivalent.

User Responsibilities

CFSA employees and volunteers should not evaluate or compromise the security of systems or data for which they are not responsible, and should not perform tests which may damage the availability, confidentiality, or integrity of data.

CFSA personnel are responsible for the availability, confidentiality, and integrity of all files and data which they access. Access to this data may be either physical, as in print outs, or virtual, as with files on a server. The disposal of data must be done in a manner that corresponds with the confidentiality of the data, regardless of physical media.

All suspected policy violations, system intrusions, virus infections, and other conditions which might jeopardize CFSA's information or CFSA's information systems must be immediately reported the VP of IT and the President.

5.0 Acceptance Policy

To ensure compliance with CFSA's internal policies, applicable laws and regulations, and to ensure employee and volunteer safety, CFSA's management reserves the right to monitor, inspect, and/or search at any time all CFSA's information systems.

CFSA's management additionally retains the right to remove from its information systems any material it views as offensive or potentially illegal. CFSA's management reserves the right to revoke the system privileges of any user at any time. Users who violate these policies or compromise the integrity of CFSA information may be subject to disciplinary action.

The CFSA VP of IT owns this policy. The policy is subject to change with the appropriate notifications.

6.0 Revision History

12/23/15	Policy Created, Will Morse
03/03/16	Policy Reviewed, Scott Huntsman