Cy-Fair Sports Association Cloud Computing Policy

1.0 Overview

Cloud computing offers a number of advantages including low costs, high performance, and quick delivery of services. However, without adequate controls, it also exposes individuals and organizations to online threats such as data loss or theft, unauthorized access to corporate networks, and risk to Cy-Fair Sports Association's (CFSA) reputation.

2.0 Purpose

This cloud computing policy is meant to ensure that cloud services are not used in a manner that is inconsistent with CFSA security policies. It is imperative that employees and volunteers do not open cloud services accounts or enter into cloud service contracts for the storage, manipulation, and exchange of CFSA related communications or CFSA owned data without the VP of IT's approval. This is necessary to protect the integrity and confidentiality of CFSA data.

CFSA's VP of IT remains committed to enabling employees and volunteers to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby CFSA employees and volunteers can use cloud services without jeopardizing CFSA data and computing resources.

3.0 Scope

This policy applies to all employees and volunteers in all committees and the CFSA office without exception.

This policy pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

If you are not sure whether a service is cloud-based or not, please contact the VP of IT.

4.0 Policy

4.1 Regulatory and Policy Requirements

- Use of cloud computing services for work purposes must be formally authorized by the VP of IT. The VP of IT will certify that security, privacy, and all other IT management requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the VP of IT and presented to the Operations Board for approval.
- The use of such services must comply with CFSA's existing Information Security Policy and Acceptable Use Policy.

- The use of such services must comply with all applicable laws and regulations governing the handling of personally identifiable information, CFSA financial data, or any other data owned or collected by CFSA.
- CFSA's Operations Board decides what data may or may not be stored in the Cloud.

4.2 Security Requirements

- Employees and volunteers must not use personal email accounts to sign up for cloud services that are used for CFSA business.
- Conversely, employees and volunteers must not sign up for personal cloud services or other such online services with CFSA email accounts. This includes such services as mobile app stores, online shopping, and personal email lists.
- Employees must not share log-in credentials with anyone, including co-volunteers, contractors, vendors, clients, friends, or family.
- All cloud services must have an administrative console or function to allow appropriate personnel to retrieve data or prevent access to data if an employee or volunteer decides to leave CFSA.
- All cloud services must have user logs that can be reviewed by the VP of IT for forensics.
- All cloud services must have a distributed architecture to minimize downtime.
- Cloud services which are certified compliant with SSAE16 or similar service provider standards are preferred.
- All cloud services must have password standards that comply with or exceed CFSA password standards.
- All cloud services must provide secure communications via SSL or similar industry standard encryption algorithms.
- Personal cloud services accounts must not be used for the storage, manipulation, or exchange of CFSA-related communications, CFSA-owned data, client data, and vendor data.

4.3 Support Requirements

- All cloud services must undergo User Acceptance Testing. Users of the cloud service will work with the VP of IT to ensure that the functionality and usability of the service meets expectations before the service is deployed to the target audience.
- All cloud service providers must have a formal support structure in place. This can be via email, a support phone number, or online support forms.
- Cloud services that require software downloads or browser plug-ins will require additional review. The software and browser plug-ins must be tested and approved by the VP of IT before any installation on CFSA computers and equipment. The VP of IT will handle distribution of the software and browser plug-ins unless otherwise stated after review.
- Software downloads and browser plug-ins must support an updating mechanism to ensure that any bugs or security holes are patched in a timely manner.

4.4 Requesting Cloud Service Approval

- Send an email to the VP of IT with the following information:
    - Name of the service.
    - A description on how the service will be used.
    - A description of the type of data that will be stored, manipulated, or accessed with this service.
- The VP of IT will review the service and communicate with the requestor to discuss the information provided above.
- The vendor will be reviewed.
- Alternate services which have been previously approved may be recommended if they provide a similar service as the newly requested service.
- If the cloud service meets the criteria in sections 4.1 – 4.3 and it does not duplicate the functionality of an approved service, it will be added to the approved cloud service list in section 4.6.

4.5 Cloud Services that do not meet requirements

- Cloud services which do not meet the criteria in sections 4.1 – 4.3 will not be permitted.
- Cloud services which are not approved will be blocked at the firewall level.

4.6 Approved cloud computing services

- SportsPilot
- Office 365
- Box.com
- Adobe Creative Cloud

5.0 Enforcement

Any employee or volunteer found to have violated this policy may be subject to disciplinary action, up to and including termination of access. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with CFSA. A violation of this policy by a guest or visitor will result in the termination of their access privileges.

6.0 Acceptance Policy

To ensure compliance with CFSA's internal policies, applicable laws and regulations, and to ensure employee 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 removal of office and/or reduction in authority, access and duties.

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

7.0 Revision History

12/23/15	Document created; Will Morse
04/04/16	Document reviewed; Scott Huntsman