	Policy Name	DATA SECURITY POLICY	
	Policy Number	BOD-003	Rev 0
	Created By	R. Campbell (Aug 2021)	
	Approved By	Board of Directors	
	Date Approved	October 30, 2021	

DATA SECURITY POLICY

1. PURPOSE

The purpose of this policy is to establish guidelines for the Alpine Club of Canada ("Club") in managing data security and for the Board of Directors (the "Board") to ensure data security is being proactively managed by Club Staff and Contractors ("Staff").

The Club has a duty to protect the personal, confidential and sensitive information held within their information systems. The Club must ensure processes and procedures are in place to manage security risks (including from outside entities) and maintain continuous access to information for Staff and members.

Failure to protect data could result in extreme financial and reputational consequences to the Club and the wider outdoor community.

The goal of this policy is to provide guiding principals to assist in long-term planning, yearly prioritization and budgeting. Over time, this policy will enable the Club to take reasonable steps to reduce the likelihood of a negative outcome related to data security.

2. APPLICATION AND SCOPE


This policy will apply across all information systems and all Staff, 3rd parties, and members.

The application of this policy includes, but is not limited to, the following areas:

- Software applications (whether developed in-house or 3rd party applications)
- Financial reporting tools
- Servers
- Email
- Computers
- User data

This policy lists minimum requirements the Club must pursue in the following areas:

- A. Security Review and Risk Assessment
- B. Long-term technology roadmaps
- C. Disaster Recovery planning and trials
- D. Proactive security for computers and servers
- E. Data backup
- F. Complex Passwords

	Policy Name	DATA SECURITY POLICY	
	Policy Number	BOD-003	Rev 0
	Created By	R. Campbell (Aug 2021)	
	Approved By	Board of Directors	
	Date Approved	October 30, 2021	

- G. Multi-factor Authentication
- H. Staff Training

3. OUTCOMES

The goals of this policy are to ensure that the Club has taken reasonable steps to ensure Data Security.

It is expected that Club Staff develop a long-term plan and then execute against that plan through yearly budget planning.

4. MANDATORY REQUIREMENTS

At a minimum, Club Staff will complete the following items related to Data Security:

A. Security Review and Risk Assessment Report

Club Staff will complete a complete review of all systems and data sources that the Club uses every three years as part of the Club's Strategic Planning exercise.

This review will include all systems, tools, and data repositories the Club oversees. For each of these, the following will be identified:

1. Name of tool/system/service/data repository
2. Description of Use
3. List users
4. Describe security processes that limit access
5. List recommended actions and their importance to make the item more secure, and for each action provide an estimate of cost and complexity.


A Security Review and Risk Assessment report will be produced and submitted to the Board of Directors for review. It is expected that Club Staff will integrate the results of this report into the Long-term Technology Roadmap.

B. Long-term Technology Roadmap Report

Club Staff will produce a long-term Technology Roadmap. This roadmap will be produced to coincide with the Club's three-year strategic plan and include conclusions from the Security Review, as well as a review of the tools and systems the Club uses to plan future work the Club must undertake.

The report will outline the strategic goals the Club should pursue regarding Data Security and technology services and explanations for why. An order of magnitude cost estimate will be included for each activity. This may lead to the creation of additional roles in the Club or the addition of new 3rd party services.

Each year a budget shall be produced to complete tasks outlined in the 3-year strategic plan, as well as any other tasks that are deemed critical. It is expected that costs and priorities may change as detailed planning takes place and better information is uncovered.

	Policy Name	DATA SECURITY POLICY	
	Policy Number	BOD-003	Rev 0
	Created By	R. Campbell (Aug 2021)	
	Approved By	Board of Directors	
	Date Approved	October 30, 2021	

C. Disaster Recovery Process (DRP)

The Club will produce a DRP that will outline all tools, systems, services and data the Club controls. For each of these the following will be identified:

1. Name of tool/system/service/data repository
2. Description of Use
3. Back-up Process
4. Back-up Timing (hourly, daily, weekly)
5. Location where back-ups are kept
6. Describe access and security of back-ups
7. Most recent actual recovery from back-up
8. List recommended solutions to improve back-up (where applicable)

The DRP will be submitted to the Board of Directors for review and approval. Each year the DRP shall be reviewed, and any changes updated by Club Staff.

Finally, each year a Disaster Recovery simulation will be performed. Under this simulation, systems and data are restored as if a real disaster has occurred. The results of this simulation, specifically the time required to restore and any items that couldn't be restored, will be included in the yearly DRP resubmission to the Board.

D. Proactive Security for all Computers and Servers

The Club will ensure that all computers, servers, and peripheral devices are proactively updated with patches or new operating systems, with no system more than 30 days out of date from updates.

Furthermore, the Club will ensure that anti-virus software is installed on all computers, and that this software is kept updated at least monthly and that virus scans are run daily.


Servers will be kept patched and best practices followed to limit access to unauthorized 3rd parties. Where required, 3rd parties may be engaged to provide these specialized skills.

E. Data Backup

All data shall have at least a daily back-up, unless that data is kept in the cloud with service guarantees to ensure data continuity. For any data kept on-site, backups must be kept in a secure location off-site and backups should be accessible and easily restored.

Data shall include, but not be limited to:

- Email
- Staff working documents
- Member information
- Financial data

	Policy Name	DATA SECURITY POLICY	
	Policy Number	BOD-003	Rev 0
	Created By	R. Campbell (Aug 2021)	
	Approved By	Board of Directors	
	Date Approved	October 30, 2021	

It is expected that the Club consider common tools to manage Staff email/working documents such as Google Drive or Microsoft365 (or other comparable services), which offer simplified implementation and management at a low cost.

F. Multi-factor Authentication

For all critical systems, the Club will use Multi-Factor Authentication (MFA). This will include Admin access to any tools, access to all banking and payment processing systems, and all server access. This will also include any social media accounts.

G. Complex Passwords

The Club will mandate complex passwords that are at a minimum 10 characters long and include UPPERCASE, lowercase, numbers, and symbols. This will apply in every situation where a password is required, such as software, websites, computers, servers, email, and more.

Staff that uses passwords to access Club resources, such as social media accounts, bank accounts, servers, or any administrator account, will use a password service like Last Pass to manage their passwords.

H. Staff Training

The Club will create, integrate, and train all Staff on the following to ensure all Staff follow acceptable technology:

- Acceptable Use Policy
- Security Training
- Information Security Policy

REVISION HISTORY

Date	Description
24-Aug-2021	Rev B: Creation of policy
30-Oct-2021	Rev 0: Approved by Board of Directors