McGill | School of Continuing Studies

Final Project

Swimming Natation Canada Information Cybersecurity Policy

Celia Fuentes

CCCS 453 – Security Risk Management and Governance

Table of Contents

Preface

Swimming Natation Canada (SNC) is a real organization. However, the following is a revised version of a final project I did for the Security Risk Management and Governance course in the Certificate in Applied Cybersecurity at McGill's School of Continuing Studies. The purpose is to demonstrate knowledge of the components of an information cybersecurity policy in managing risk by applying them to a real organization.

I have chosen Swimming Natation Canada, a not-for-profit organization, and used publicly available information from the organization's website to make my project as realistic as possible. I have also added fictional information to flesh out the project. During my research, the document "Building the Cybersecurity and resilience of Canada's Non-Profit Sector"[i] written by The Canadian Centre for Nonprofit Digital Resilience helped me keep in mind some challenges faced by organizations in this sector:

- Overall limited funds and personnel, with the focus of resources being allocated to the organization's main mission;
- Lack of funds dedicated to tackling information security issues;
- Lack of internal staff with advanced information technology skills and knowledge, and no internal CIO or CISO to provide leadership in information security;
- Lack of cybersecurity awareness among board members, staff and volunteers;
- The role of volunteers, who may be placed at the last minute, with access to systems.

I did not seek permission to use SNC for my project, SNC did not mandate me to create a cybersecurity policy for their organization, and this project in no way represents an official SNC policy.

1.Introduction

Swimming Natation Canada (SNC) is the not-for-profit[ii] governing body for competitive swimming in Canada. It represents around 50,000 competitive swimmers and an additional 75,000 swimmers that participate in other programs from 350 affiliated clubs across the country in 10 provincial sections[iii]. It organizes and promotes open[iv] and in-pool swimming meets[v] for able-bodied, para[vi] and master[vii] swimmers at all levels. With an annual budget of $3 million CAD, it receives 40% of its funding from the federal government, and 60% from sponsors, fundraising and member fees.[viii]

This policy represents SNC's commitment to its cybersecurity posture. All more specific information security policies and procedures must conform to the guiding principles in this policy. Contact us at security_policy@swimming.ca[ix] should you have questions or concerns.

2.Scope

This Information Security Policy applies to

1. The SNC Board and all staff;
2. Individual and club members, volunteers, and provincial partners throughout Canada when interacting with any of SNC systems and data;
3. It also applies when sharing member information on SNC's behalf with third-party or international partners, specifically World Aquatics and the International Olympic Committee (IOC), but also present and future international partners such as service providers and sponsors;
4. Physical and remote offices, and during temporary meet locations throughout Canada;
5. All information, whether physical or digital, resources including the organization's systems, computers, tablets and mobile devices, network devices and organizational and membership data and metadata, hard-copy files and resources;
6. While elements of third-party data storage, website hosting and social media accounts are out of the scope of this policy, the organization expects the SNC community to follow, where applicable, the policy mentioned herein on these platforms, for example with regards to data privacy, access control, data storage and back-ups.

As informational technology continues to evolve, the scope may be reviewed as required.

3.Objectives

The objectives of this policy include

1. To protect information resources, whether physical or digital;
2. To increase information security awareness of responsibilities and thereby reinforce accountability to strengthen our organization's cybersecurity posture and culture;
3. To provide an organizational-wide policy framework to continue to develop, implement, measure and improve information security policies and procedures in a standardized manner based on the assessment of risk and the SNC budget;
4. Track and report information security metrics to determine if prevention and mitigation measures are being applied and if they improve SNC cybersecurity posture.

4.Roles and Responsibilities[x]

4.1 Board of Directors, Board

The Board will

1. Make the governance and strategic decisions regarding information security policies initiatives;
2. Make decisions informed by the risk reports provided by the IT Senior Manager, the recommendations of the President and the CEO, and the advice provided by legal counsel;
3. Create cybersecurity committees to help create and implement new cybersecurity specific policies or procedures;
4. Approve all information security policy initiatives it deems are in line with the organization's mission, priorities and budget constraints;
5. Once approved, the implementing and monitoring phases of specific policies and procedures do not require direct Board participation but shall be done via committee work authorized by the Board;
6. Set the overall budget for information security.

4.2 The President of the Board, President

The President will

1. As the liaison between the Board and the CEO, stay informed of information security management through the CEO;
2. Provide Board governance guidance to the CEO on information security issues;
3. Be the only person authorized to make emergency funds available for supplemental mitigation measures if they deem it justified within the context of a major incident.

4.3 Chief Executive Officer, CEO

The CEO will

1. Report on their management activities relevant to information security at Board meetings;
2. Communicate with the President on management activities relevant to information security between Board meetings;
3. Ensure that information security policies, standards, guidelines, and procedures developed by the IT Senior Manager are in line with SNC's strategic plan as stated by the Board;
4. Have the authority to sign contracts with information service providers on behalf of the organization;
5. Be the only representative permitted to issue public statements on behalf of the organization regarding security incidents. These statements will be made based on the information gathered from the IT Senior Manager, HR, internal counsel from the President and external legal counsel;
6. Be authorized to formally request from the President emergency funds in the context of a major incident.

4.4 Information Technology Senior Manager, IT Senior Manager

The IT Senior Manager will

1. Report to the CEO;
2. Effectively communicate to the CEO and the Board the security risks concerning risk and vulnerabilities;
3. Guide the organization to ensure SNC security policies and procedures comply with applicable cybersecurity legislation and regulations;
4. Be the Chair on cybersecurity committees created by the Board;

5. Determine the various levels of access control and privileges appropriate for the Board, the President, CEO, Regional Managers, staff, members, and volunteers;
6. Authorize the archiving and eventual deletion of user system accounts;
7. Develop incident recovery plans tailored to the requirements of SNC;
8. Have the authority to declare a major incident;
9. Immediately notify the CEO when a major incident has been declared, and be the acting team lead of the incident response team for major incidents;
10. Notify the CEO of low to medium incidents through reports, and have the authority to delegate medium to minor incidents to Regional Managers;
11. Act as SNC's Privacy Officer in case of a data breach;
12. Negotiate third-party information security contracts that are in line with the organization's cybersecurity posture and budget;
13. Cooperate with the Auditor in all information auditing activities.

4.5 Cybersecurity Committee

The Cybersecurity Committees will

1. Be formed only with the authority of by the Board;
2. Be chaired by the IT Senior Manager
3. Within the budgetary constraints, be the enabler of the information security priorities as set by the Board and communicated by the CEO;
4. Assess, recommend, create and implement specific cybersecurity policies and procedures.

4.6 Operations Regional Manager, Regional Manager

For their region, the Regional Manager will

1. Report to the IT Senior Manager on information technology issues, including those involving cybersecurity;
2. Coordinate with information third-party service providers in their respective SNC region;
3. Handle minor to medium incidents as delegated by the IT Senior Manager;
4. Have the authority to delegate minor incidents to staff, if available;
5. Be responsible for the inventory, configuration, patch, update on all authorized systems, devices, and software in accordance with internal policies and procedures and third-party service provider contract agreements;
6. Configure the access control and privileges of the Board, CEO, staff, members, and volunteers in accordance with internal policies and procedures and third-party service provider contract agreements;
7. Be responsible for IT account management and monitoring in their region;
8. Follow and leverage publicly available tools and resources in the cybersecurity community;
9. Provide timely cybersecurity metrics for their region to the IT Senior Manager for reporting purposes;
10. Provide appropriate access to the Auditor during information auditing activities;
11. Authorize the creation of staff accounts and temporary accounts for volunteers;
12. Develop and implement staff awareness campaigns on security policies and procedures.

4.7 Staff

All staff will

1. Follow all information security training relevant to their job responsibilities at the beginning and during their employment;
2. Follow all SNC information security policies and procedures during their employment;

3. Participate in a cybersecurity awareness campaign once a year;
4. Train meet volunteers with access to information technology assets and systems to follow security policies;
5. Report information security policy violations to their Regional Manager;
6. Cooperate with the Auditor as appropriate for all auditing activities.

4.8 Human Resources, HR

HR will

1. Perform background check for possible new hires;
2. Explain the respective information security responsibilities and disciplinary framework to new employees;
3. Obtain the required signature of employees for policies
4. Assist with information security internal or external investigations;
5. Provide a whistleblower mechanism for the reporting of information security policy violations.

4.9 Communications Agent

The Communications Agent will

1. Help draft, review and issue communications on all relevant media platforms as directed by the CEO during a cybersecurity incident;
2. Provide a temporary mode of communication (email or phone) available for staff not on the incident response team, and for members of the SNC community who may require further clarification regarding an incident.

4.10 Part-time Internal Information Auditor, Auditor (External)

There will be two auditors to ensure the integrity of the audit. The Auditor will

1. Report findings to the Board;
2. Be a certified auditor;
3. Be a part-time consultant from an external service provider;
4. Measure the effectiveness of information security policies and procedures through audits every two years;
5. Provide recommendations to rectify inefficiencies or gaps in audit reporting.

4.11 Legal (external)

The external legal service provider will

1. Provide counsel to ensure compliance with applicable laws and regulations during an incident;
2. Review communications and provide counsel to the CEO during a major incident.

4.12 Members (external)

All members, which include club representatives, coaches, parents of swimmers who are minors, and individual swimmers will:

1. Be made aware of the organization's information security policy relevant to their role within the SNC community;
2. Be expected to follow the organization's information security policies while participating in SNC events.

4.13 Meet Volunteers (external), Volunteers

Volunteers include data entry clerks, timekeepers, referees and other meet officials. Volunteers will:

1. Be made aware of information security issues and mitigations in the context of a SNC meet during their training (access control, tailgating, etc.), with an emphasis on protecting sensitive information and systems;
2. Have valid access rights only for the duration of their shift on deck.

5.Policy Statement

SNC recognizes it must take steps to become resilient to the growing threat landscape in the information security domain. All information assets must be accessed and used in an authorized manner as set forth in this policy.

5.1 Principles

The protection of organizational information equipment, devices, systems, data and metadata, and the data and metadata provided by our membership is a top priority. This is expressed in four guiding principles:

1. **Confidentiality**, to ensure only authorized staff can view sensitive information.
2. **Integrity,** to ensure that information is not tampered with.
3. **Availability**, to ensure that our systems are available to staff, membership and the public depending on their role in the SNC community.
4. **Authenticity**, to reliably confirm the identity of users accessing data to reinforce responsibility and accountability.

5.2 Requirements

The following requirements are applicable throughout the organization:

5.2.1 Human Resources Security

1. A framework to perform background checks for possible new hires;
2. Clear understanding by staff of expected relevant information security responsibilities;
3. Disciplinary framework in case of information security violations for fair accountability;
4. Whistleblower mechanism for the reporting of information security policy violations.

5.2.2 Asset Management

1. The establishment of an inventory with an assigned user for physical devices;
2. Follow manufacturer recommended end-of-life timelines and practices for devices;
3. Establish a file and folder system, including for archiving and deleting digital assets;
4. Put in place a specific policy on the acceptable use of assets.

5.2.3 Access Control

1. All persons interacting with devices and systems are required to follow organizational password best practices in terms of credential protection, length and update;
2. The access of SNC systems shall require multi-factor authentication;
3. As a small organization, SNC often requires staff to wear multiple hats in terms of job responsibilities. A segregation of all roles and responsibility is not always possible. As such, access control of informational assets is based on a fluid need-to-know basis depending on currently assigned roles and responsibilities. Staff awareness programs must clearly explain the meaning of need-to-know so that staff understand access privileges depending on their current job responsibilities;[xi]
4. A clear framework for privileges of information assets shall be put in place;
5. Third-party monitoring of access will be used to detect unauthorized actions, enforce accountability and to provide data for audit reports.

5.2.4 Cryptography

1. Third-party service providers must provide industry-tested and regulation compliant encryption at endpoints and during transit;
2. Staff and volunteers, either by action or omission, shall not weaken cryptographic practices used by the organization or service providers.

5.2.5 Physical and Environmental Security

1. Educate employees on not allowing tailgating in SNC spaces;
2. Clear desk policy for on-site and remote work;
3. Reliable back-ups with trusted third parties;
4. Develop specific policies for possible on-site natural disasters and physical threat incidents (ex. vandalism, dangerous intruder).

5.2.6 Operations security

1. Establish a reliable data entry, storage and back-up framework that is flexible to meet the lows and peaks in demand of the SNC meet calendar;
2. SNC does not store payment data[xii] and requires that payment service providers follow regulatory-compliant standards.

5.2.7 Communications security

1. SNC shall use third-party IT expertise to install, configure and maintain a firewall to protect organizational network infrastructure.

5.2.8 System acquisition, development, and maintenance

1. SNC shall use only third-party, proprietary, and widely used systems, software, and platforms;
2. SNC shall have contractual relationships with suppliers whose information security follows industry norms in information security that meet the needs and size of our organization.

5.2 9 Supplier Relationships

1. All supplier relationships shall be established by contract;
2. Relationships with suppliers must demonstrate a clear division of roles and responsibilities with respect to information security;
3. Suppliers must be able to demonstrate due diligence in their information security while providing their services to SNC;
4. Demonstrate that they have monitoring capabilities while delivering services to SNC.

5.2.10 Information Security Incident Management

Develop specific policies for possible

1. Malware;
2. Ransomware;
3. Incident management must provide a framework to assess incidents as low, medium or major;
4. Depending on the recommendations from audits, new incident management policies may be required depending on the evolving threat landscape faced by SNC.

5.2.11 Security and Business Continuity

1. Establish clear roles and responsibilities to ensure business continuity.

6.Applicable Laws and Regulations

This policy is subject to

1. The Personal Information Protection and Electronic Documents Act (PIPEDA);[xiii]
2. The Canada Labour Code;[xiv]
3. SNC General By-Laws;[xv]
4. And during meets or interactions in Europe, the General Data Protection Regulation (GDPR).[xvi]

7.Compliance

To ensure compliance and monitoring

1. The Board will launch an external audit of SNC cybersecurity practices every two years;
2. The IT Senior Manager will keep abreast of new legislation and regulations to guide the Board;
3. As regulations continually evolve, SNC will monitor and update its practices and procedures to reflect those in the Applicable Laws and Regulations section of this policy.

8.Enforcement and Exceptions

8.1 Enforcement

Depending on the severity of a violation of the information security policy

1. By SNC board members and staff: will result in disciplinary action as specified in the disciplinary policy, and where applicable, could lead to further investigation possibly resulting in civil or criminal liability;
2. By SNC external members, volunteers, contractors or service providers: could lead to investigation possibly resulting in civil or criminal liability, and/or the cancelation of contracts.

8.2 Exceptions

1. Policy exceptions can only be issued if the IT Senior Manager deems it is justified given the context versus the security risks involved;
2. All exceptions must be documented for auditing purposes.

9.Updating, Revision and Approval Requirements

1. The Information Security Policy will be updated, revised and approved by the Board every two years, as per Swimming Canada's Policy Review Policy.[xvii]
2. Updates between Board reviews are permitted if recommended by the IT Senior Manager and authorized by the CEO.

10.Glossary

GDPR: General Data Protection Regulation
PIPEDA: Protection and Electronic Documents Act
SNC: Swim Natation Canada

11.Version Control[xviii]

Author	Swimming Natation Canada Board and IT Senior Manager		
Document Name	Swimming Natation Canada Information Security Policy		
Version	1.2		
Source	Swimming Natation Canada		
Policy Owner(s)	IT Senior Manager		
Date	Version	Author	Changes/Comments
25/04/2022	1.0	CF	Final version approved by the Board
31/02/2023	1.1	CF	Updated Operations security 5.2.6.2 to specify that SNC "does not store payment data"
31/03/2023	1.2	CF	Updated Cryptography 5.2.4.1 to include "industry-tested and regulation compliant"

Endnotes

[i] "Building the Cybersecurity and resilience of Canada's Non-Profit Sector." The Canadian Centre for Nonprofit Digital Resilience, February 2023, https://ccndr.ca/wp-content/uploads/2023/02/Building-the-Cybersecurity-and-Resilience-of-Canada.pdf

[ii] https://www.swimming.ca/en/board-of-directors/

[iii] https://www.swimming.ca/en/resources/swimming-canada-overview/association-profile/association-profile/#:~:text=This%20focus%20holds%20great%20importance,International%20Olympic%20Committee%20(IOC).

[iv] In swimming, ***open*** refers to swimming outdoor in rivers, lakes, bays, oceans, etc., in races that are at least 1 km long. https://blog.myswimpro.com/2018/03/16/swim-meet-terminology-faqs/#:~:text=A%20swim%20meet%20is%20a,also%20include%20a%20diving%20competition

[v] In swimming, ***meets*** are competitions usually organized by a governing body such as Swimming Canada, USA Swimming, etc. https://blog.myswimpro.com/2018/03/16/swim-meet-terminology-faqs/#:~:text=A%20swim%20meet%20is%20a,also%20include%20a%20diving%20competition.

[vi] Para swimmers refer to swimmers with a disability. The Swim Canada's Para-Swimming policy can be found at https://www.swimming.ca/en/para-swimming-2/

[vii] In swimming, **master** swimmers are 18 years old and older who train with an affiliated club and who do not compete at a high level. Competing is not mandatory. The range of skills can include swimmers completely new to the sport to ex-competitive swimmers who continue to train and compete, but at a less demanding level. The Swimming Canada statement on masters can be found at https://www.swimming.ca/en/masters/

[viii] https://www.swimming.ca/en/resources/swimming-canada-overview/association-profile/association-profile/

[ix] This is a fictional email address for the assignment.

[x] The wording in this section was inspired by other Swimming Canada policies available at https://www.swimming.ca/en/board-of-directors/
and https://www.swimming.ca/content/uploads/2019/07/2019_Chief-Executive-Officer-19Jan2019.pdf

[xi] https://nces.ed.gov/pubs98/safetech/chapter8.asp
[xii] https://www.swimming.ca/en/news/2023/01/24/third-party-cybersecurity-incident-important-update-and-next-steps/#:~:text=On%20Jan.,historical%20results%20from%20competitive%20events
[xiii] https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html
[xiv] https://www.canlii.org/en/ca/laws/stat/rsc-1985-c-l-2/latest/
[xv] https://www.swimming.ca/content/uploads/2020/09/2020-General-Bylaws-September-23-2020.pdf
[xvi] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[xvii] https://www.swimming.ca/en/policy-review/
[xviii] Fictional information to demonstrate knowledge of version control in a policy document.