WORLD FEDERATION OF CHIROPRACTIC | FÉDÉRATION MONDIALE DE CHIROPRATIQUE | FEDERACIÓN MUNDIAL DE QUIROPRÁCTICA

2 St. Clair Avenue West | Floor 18 | Toronto | Ontario | M4V 1L5 | Canada
T. +1 647 255 8030 F. +1 888 837 6748 E. info@wfc.org

CYBERSECURITY POLICY AND PROCEDURE

1. Introduction

The World Federation of Chiropractic (WFC) is committed to protecting its information systems and data from cyber threats. This policy outlines the measures to prevent, detect, and respond to cyber hacking incidents. It aims to safeguard the WFC's digital assets, ensure the confidentiality, integrity, and availability of information, and maintain trust with members, stakeholders, and the public.

2. Purpose

The purpose of this policy is to:

- Define the WFC's approach to cybersecurity.
- Outline the procedures for preventing and responding to cyber hacking incidents.
- Ensure compliance with relevant laws, regulations, and best practices.
- Protect the WFC's information assets and minimize the impact of cyber incidents.

3. Scope

This policy applies to all WFC employees, members, contractors, and third-party service providers who have access to the WFC's information systems and data.

4. Cybersecurity Policy

4.1. Governance and Responsibility

- The WFC Board of Directors is responsible for overseeing the cybersecurity policy and ensuring adequate resources are allocated for its implementation.
- The WFC's designated IT contractor, assisted y the WFC Finance and Administration Manager is responsible for managing the cybersecurity program, including risk assessments, monitoring, and incident response.

- All WFC employees, members, and contractors are responsible for adhering to this policy and reporting any suspicious activities.

4.2. Risk Management

- Conduct regular risk assessments to identify and evaluate cybersecurity threats.
- Implement controls to mitigate identified risks, including technical, administrative, and physical measures.
- Review and update risk assessments annually or when significant changes occur.

4.3. Access Control

- Implement strict access control measures to ensure that only authorized individuals have access to sensitive information and systems.
- Use multi-factor authentication (MFA) for accessing critical systems.
- Regularly review and update user access rights based on role requirements.

4.4. Data Protection

- Encrypt sensitive data in transit and at rest.
- Implement data classification and handling procedures to ensure appropriate protection based on data sensitivity.
- Regularly back up data and store backups securely offsite.

4.5. Network Security

- Use firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to protect the WFC's network.
- Regularly update and patch software, systems, and applications to address vulnerabilities.
- Segment networks to limit access to critical systems and data.

4.6. Endpoint Security

- Install and maintain antivirus and anti-malware software on all endpoints.
- Implement endpoint detection and response (EDR) solutions to detect and respond to threats on devices.
- Enforce policies for secure configuration and maintenance of all devices.

4.7. Training and Awareness

- Provide regular cybersecurity training and awareness programs for all WFC employees, members, and contractors.
- Educate users on recognizing phishing attacks, social engineering, and other common threats.
- Conduct periodic simulated phishing exercises to reinforce awareness.

5. Cyber Hacking Incident Response Procedure

5.1. Preparation

- Develop and maintain an incident response plan (IRP) detailing roles, responsibilities, and procedures.
- Establish an incident response team (IRT) comprising the WFC's IT contractor and Finance and Administration Manager.
- Ensure necessary tools and resources are available for effective incident response.

5.2. Detection and Reporting

- Implement continuous monitoring to detect potential cyber incidents.
- Encourage prompt reporting of suspicious activities to the WFC IT contractor or designated contact.
- Establish a clear reporting mechanism, including contact information and reporting templates.

5.3. Assessment and Classification

- Assess reported incidents to determine their validity and severity.
- Classify incidents based on their impact on confidentiality, integrity, and availability of information and systems.

5.4. Containment

- Implement short-term containment measures to prevent the spread of the incident.
- Identify and isolate affected systems or networks to limit damage.
- Preserve evidence for further analysis and investigation.

5.5. Eradication

- Identify the root cause of the incident and eliminate it from affected systems.
- Remove malware, unauthorized access, and other malicious artifacts.
- Apply patches, updates, and configuration changes to prevent recurrence.

5.6. Recovery

- Restore affected systems and data from clean backups.
- Verify the integrity and functionality of restored systems.
- Monitor systems for any signs of lingering issues or further attacks.

5.7. Post-Incident Review

- Conduct a thorough review of the incident to identify lessons learned.
- Update the incident response plan and security measures based on findings.
- Report the incident to relevant stakeholders, including regulatory bodies if required.

6. Compliance and Enforcement

- Ensure compliance with this policy through regular audits and assessments.
- Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or membership.

- Review and update this policy annually or as needed to address emerging threats and changes in the cybersecurity landscape.

7. Conclusion

The WFC is dedicated to maintaining a robust cybersecurity posture to protect its information systems and data from cyber threats. This policy and procedure document provides a comprehensive framework for preventing, detecting, and responding to cyber hacking incidents, ensuring the continued trust and confidence of WFC Members and stakeholders.

Adopted by the WFC Board of Directors this 12th day of August, 2024