WCS2 Cybersecurity Policy

Updated: March 23, 2023

Purpose

1. The purpose of this cybersecurity policy is to ensure the secure storage, processing, and handling of sensitive information collected and maintained by the Women CyberSecurity Society (WCS2) in Canada. This policy also establishes guidelines for reporting data breach notifications.

Scope

2. This policy applies to all employees, contractors, and volunteers of WCS2 who have access to sensitive information or are responsible for the security of WCS2's information technology (IT) infrastructure.

Information Security

3. WCS2 will implement appropriate security controls to protect the confidentiality, integrity, and availability of sensitive information. These controls include, but are not limited to:
    - Encryption of sensitive data in transit and at rest
    - Access controls to limit access to sensitive data to authorized personnel
    - Secure storage and backup of data to prevent loss or unauthorized access
    - Regular updates and patches to software and systems to prevent vulnerabilities
    - Regular security awareness training for all employees, contractors, and volunteers of WCS2

Incident Response

4. WCS2 will have an incident response plan in place to manage cybersecurity incidents, including data breaches. The incident response plan will include procedures for:
    - Reporting and documenting incidents
    - Containing and mitigating the impact of incidents
    - Notifying affected individuals and authorities, as required by law
    - Conducting post-incident reviews to identify opportunities for improvement

Reporting Data Breach Notifications

5. In the event of a data breach, WCS2 will report the incident to affected individuals and regulatory authorities, as required by law. WCS2 will also notify its IT service providers, if applicable, and work with them to mitigate the impact of the breach. The notification will include:
    - Description of the incident
    - Types of data involved
    - Steps taken to mitigate the impact of the breach
    - Steps taken to prevent future incidents

Compliance

6. WCS2 will comply with all applicable laws and regulations related to information security and data privacy, including but not limited to the Personal Information Protection and Electronic Documents Act (PIPEDA) and the General Data Protection Regulation (GDPR).

Enforcement

7. Any employee, contractor, or volunteer who violates this policy may be subject to disciplinary action, up to and including termination of employment or contract.

Review and Update

8. This cybersecurity policy will be reviewed and updated as necessary to ensure it remains current and effective. Reviews will be conducted at least annually or when significant changes occur to WCS2's IT infrastructure or the legal and regulatory environment related to information security and data privacy.

By implementing this cybersecurity policy, WCS2 aims to safeguard the confidentiality, integrity, and availability of sensitive information while also complying with applicable laws and regulations.