Skills Ontario Competition
Olympiades de Compétences Ontario

Contest Scope / Fiche descriptive
2026

TABLE OF CONTENTS

This document was last updated: January 2026

There may be a newer version available: https://www.skillsontario.com/skills-ontario-competition#Scopes. Please check our website to ensure you have the latest version as indicated in the last updated column.

TABLE DE MATIÈRES

Plus récente mise à jour du document : janvier 2026

Il est possible qu'une version plus récente de la fiche descriptive soit disponible sur le site Web : https://www.skillsontario.com/olympiades-de-competences-ontario?na=302#Scopes. Veuillez consulter la version affichée sur notre site Web pour vous assurer que vous avez en main la plus récente version (vérifiez la colonne Plus récente mise à jour).

1. GENERAL CONTEST INFORMATION

The Contest Scope Document for the Cybersecurity competition serves as a comprehensive guide for participants, organizers, and judges, outlining the essential details of the event. It provides a clear framework for the competition, covering critical aspects such as the purpose, schedule, and judging criteria. Designed to showcase practical and theoretical cybersecurity skills, the contest emphasizes key domains such as cryptography, forensics, ethical hacking, network security, and incident response. Participants will engage in real-world scenarios, testing their ability to configure secure networks, perform penetration testing, detect and mitigate threats, and execute robust incident response strategies. The document also highlights the required tools, infrastructure, materials, and safety protocols, ensuring a standardized and professional competition environment. With a focus on promoting technical expertise and innovation, this scope document plays a pivotal role in fostering cybersecurity talent and industry readiness.

1.1 Purpose of the Contest

The purpose of this competition is to provide participants with an opportunity to demonstrate their practical and theoretical expertise in key areas of cybersecurity through focused, skill-based tasks. The competition includes challenges such as attacking and defending a network and network devices, decrypting encrypted messages using cryptographic techniques, analyzing network traffic to uncover vulnerabilities, conducting penetration testing, and scanning networks for open ports and services. Participants will also perform forensic analysis to extract hidden information, verify file integrity, and decode embedded data, as well as analyze logs to detect unauthorized access and suspicious activities. These tasks simulate real-world scenarios, emphasizing precision, technical proficiency, and problem-solving skills in a controlled and supportive environment. Their skills and knowledge in cybersecurity, with a focus on:

- Fundamental knowledge of cryptographic techniques and secure communications.
- Network traffic analysis and identifying vulnerabilities in real-world scenarios.
- Forensic analysis, including metadata extraction and file integrity verification.
- Penetration testing and ethical hacking, including vulnerability scanning and exploitation.
- Network scanning and mapping, including identifying active hosts, open ports, and services.
- Log analysis for detecting unauthorized access and suspicious activities.
- Applying cybersecurity principles to design and implement secure systems and processes.

1.2 Technical Committee

Technical Chair (Contest Lead): Kevin Ramdas, Humber Polytechnic: kevin.ramdas@humber.ca; Francis Syms, Humber Polytechnic: francis.syms@humber.ca

Technical Committee Members
Ahmed Al-Ani, Humber Polytechnic: ahmed.al-ani@humber.ca

Ian Thomson, Fleming College: ian.thomson@flemingcollege.ca
Myles Peterson, Cambrian College: myles.peterson@cambriancollege.ca
Sohrab Farooq, Conestoga College: sfarooq@conestogac.on.ca
Mark Shtern, Seneca Polytechnic: mark.shtern@senecapolytechnic.ca
Haidar Jabbar, Humber Polytechnic: haidar.jabbar@humber.ca

Any questions regarding this scope must be sent at least two weeks prior to the contest date to be guaranteed a response.

For general inquiries and non-technical contest specific questions please email: competitions@skillsontario.com

1.3 Contest Schedule

Monday, May 4, 2026	
Time	**Activity**
7:00 am – 7:30 am	Sign-in at the contest site
7:30 am – 8:00 am	Orientation
8:00 am – 12:00 pm	Competition (Part 1) **3 Activities**
12:00 pm – 12:30 pm	Lunch (mandatory mental health break)
12:30 pm – 4:30 pm	Competition (Part 2) **3 Activities**

*Competitors must be on time for their contest or may be disqualified at the discretion of the Technical Committee.

Closing Ceremony: 9am – 12pm, Wednesday May 6, 2026

This contest is offered as an official demonstration contest for 2025.

This contest is not currently offered at the **Skills Canada National Competition (SCNC)**

Cybersecurity is currently offered as a WorldSkills contest. However, Skills Ontario competitors are not eligible to compete directly at the Worlds event.

1.4 Additional Information – Essential to Review

Competitor Information:

- Scopes: https://www.skillsontario.com/skills-ontario-competition#Scopes
- Student Preparation Manual: https://www.skillsontario.com/files/www/2024_Docs/Student_Preparation_and_Training_Manual_Skills_Ontario_English_April_30_2024.pdf

- Competitor Eligibility: https://www.skillsontario.com/skills-ontario-competition#CompetitorEligibility
- Rules and Regulations: https://www.skillsontario.com/skills-ontario-competition#CompetitorRules
- Competition Floor Plan: https://www.skillsontario.com/competition-visitors#FloorPlan
- Closing Ceremony and Awards: https://www.skillsontario.com/closing-ceremony

2. SKILLS AND KNOWLEDGE TO BE TESTED

The skills competition will have theoretical, practical and writing skills. The Competitors will be evaluated on their ability to perform the following tasks:

- Decrypting encrypted messages using cryptographic methods.
- Analyzing network traffic to identify vulnerabilities and insecure communications.
- Mapping networks, scanning for open ports, and identifying running services.
- Conducting penetration testing and ethical hacking tasks.
- Performing forensic analysis of files to uncover hidden data and verify integrity.
- Analyzing logs to detect intrusions and suspicious activities.
- Applying cybersecurity principles to solve practical challenges in real-world contexts.

3. JUDGING CRITERIA

The Cybersecurity Skills Ontario Competition emphasizes a comprehensive evaluation of participants' technical and practical expertise across key cybersecurity domains. The judging criteria focus on assessing critical skills such as implementing encryption for secure communications, conducting forensic analysis and evidence collection, performing ethical hacking tasks including vulnerability scanning and penetration testing, configuring and managing secure networks, detecting and mitigating cybersecurity threats, and developing effective incident response strategies. These areas reflect real-world cybersecurity challenges, ensuring participants demonstrate a well-rounded understanding and application of essential cybersecurity practices.

Table1: Competitions and Evaluation Criteria

Aspect	**Skills Needed**	**Marks**
Network Security protocols: offensive and defensive aspects	Attack the network with common network attacks and then put into place defensive postures	20
Server operations: offensive and defensive aspects	Identify and exploit vulnerabilities on a network server and then secure the server	15

Aspect	Skills Needed	Marks
Windows Server: offensive and defensive aspects	Use various tools to exploit Windows Server and its databases	20
Forensics: Metadata extraction, file integrity verification, and decoding hidden data.	Ability to extract metadata, verify file integrity, decode hidden data, and document findings.	10
Social Engineering: Vulnerability scanning, penetration testing, and exploitation.	Proficiency in identifying vulnerabilities, conducting scans, and exploiting weaknesses effectively.	10
Malware Analysis: Analyzing network traffic to identify vulnerabilities and insecure communications.	Identify malicious, suspicious and benign events using malware analysis. Determine if file is malicious. Apply Mitre ATT&CK Matrix to your scenario	25
Total Marks		**100**

4. EQUIPMENT, INFRASTRUCTURE AND MATERIALS

To provide a professional and engaging competition experience, the Skills Ontario Technical Committee ensures participants have access to the tools and resources required to tackle real-world cybersecurity challenges. Competitors will be supplied two desktop workstations with enough RAM to run up to three Virtual Machines. The competition will consist of between four and six mini-challenges that are based on different aspects and skill sets within Cybersecurity. Each of the mini-challenges will be supported by preconfigured images with the appropriate tools for cryptography, network analysis, penetration testing, forensics, and log analysis. There is no access to the internet.
These resources allow participants to demonstrate their technical abilities effectively while adhering to professional standards. Competitors are also responsible for bringing a few personal items and following attire guidelines to maintain a fair and uniform environment. Below is a detailed list of items provided by the committee and those required from competitors:

Provided by Skills Ontario Technical Committee:

- **High-performance desktops or laptops** pre-configured with necessary tools for cybersecurity tasks.
- **Pre-installed software** and resources, including:
    - **Kali Linux** for penetration testing and ethical hacking activities.
        - **NMAP/ZenMap**, Y**ersinia, arpspoof, hydra, setoolkit, OpenVAS, Nessus, Metasploit, Bloodhound, Kerberoasting/Mimikatz, impacket secretdump, hashcat, PEStudio, RegShot, ExifTool**
    - **Windows 10 clients**
    - **Window Server 22**
        - **DHCP, DNS, FTP, Active Directory**

- **Packet tracer or GNS3 with Cisco IOS images to set up networks**
- **HTTP server using python**
- **Wireshark** for analyzing network traffic and identifying vulnerabilities.
- **Base64 decoders** for decrypting hidden data.
- **Hashing tools** (e.g., sha256sum, md5sum) for file integrity verification.

- **Preloaded files and PCAP data**, including encrypted messages, network traffic captures, and forensic artifacts for analysis.
- **Virtual Machines (Linux and Windows)** with configured environments for specific tasks such as cryptography, forensics, and scanning.
- **Simulated network environments** with vulnerabilities for scanning and exploitation tasks.
- There are water stations available on every contest site for competitors and volunteers, you must bring your own reusable water bottle, as there will be no cups provided.
- **Lunch Provided:** A simple lunch (sandwich, cookie, water - using your refillable water bottle) will be provided. The following dietary options will be available: vegetarian, vegan, halal, dairy-friendly, gluten-friendly. If you have other dietary needs, prefer additional food, and/or have other tastes then what may be provided, please bring your own nut-free items. Lunch selection will occur during student registration.

Provided by Competitor:

- **Pen or pencil** for documenting processes, taking notes, and completing written components of the competition.
- **Refillable water bottle** for hydration, with water stations available near the contest site.
- Additional snacks (recommended peanut-free)
- **Appropriate attire**, ensuring a professional appearance without external logos, except for those of their school or institution.
- **Competitors must read this scope document and any related documents posted (if applicable) online in full.** Verbal instructions alone are not sufficient for preparation. Each competitor must review the entire scope.
- The provincial contest scope will be posted on the Skills Ontario website by January 31st or earlier each year: https://www.skillsontario.com/skills-ontario-competition#Scopes . The previous year's scope will remain available for reference as well.

5. SAFETY

Safety and security are top priorities at the Skills Ontario Competition, focusing on both human safety and adherence to cybersecurity practices to ensure a secure and ethical competition environment. Competitors must adhere to the following guidelines:

Cybersecurity Practices:

- Handle all simulated or real data with care, following strict data handling and privacy guidelines. This includes:
    - Ensuring that no sensitive data is shared, duplicated, or stored outside the designated competition environment.
    - Using secure authentication methods and avoiding sharing passwords, keys, or other sensitive information.
    - Avoiding actions that may lead to unauthorized access, data leaks, or compromise of systems.
- Comply with all relevant data protection laws and cybersecurity best practices, such as those outlined in GDPR, PIPEDA, or equivalent standards, ensuring simulated environments reflect real-world expectations.

Behavioral Integrity:

- Any form of unethical behavior, including tampering with other competitors' setups, violating privacy protocols, or attempting to exploit the competition environment, will result in immediate disqualification.
- Competitors are expected to interact respectfully and uphold professional standards throughout the competition.

Incident Reporting:

- Competitors are encouraged to promptly report any safety, security, or technical concerns to the technical committee for resolution.

Human and Digital Safety:

- Ensure proper ergonomic practices, such as maintaining a healthy posture and taking necessary breaks, to avoid physical strain during extended sessions.
- Follow all safety guidelines within the venue, such as fire safety, electrical safety, and maintaining a clutter-free workspace to avoid trip hazards.

Safety is a priority at the Skills Ontario Competition. Failure to comply with these safety standards, cybersecurity protocols, or behavioral guidelines may result in disqualification at the discretion of the judges and technical committee. Competitors may be removed from the competition site if they fail to demonstrate competency, disregard safety rules, or breach data handling and privacy standards.

1. RENSEIGNEMENTS GÉNÉRAUX AU SUJET DES CONCOURS

La fiche descriptive du concours Cybersécurité détaille les éléments clés du concours et constitue un guide essentiel pour les concurrents, les organisateurs et les juges. Elle établit un cadre structuré en précisant l'objectif du concours, l'horaire et les critères d'évaluation. Conçu pour valoriser à la fois les compétences pratiques et théoriques en cybersécurité, le concours met l'accent sur des domaines stratégiques tels que la cryptographie, la preuve informatique, les tests d'intrusion, la sécurité des réseaux et l'intervention face aux incidents. Les concurrents seront confrontés à des scénarios réalistes, mettant à l'épreuve leur capacité à sécuriser des réseaux, à effectuer des tests de pénétration, à détecter et neutraliser des menaces, ainsi qu'à déployer des stratégies d'intervention efficaces. La fiche descriptive détaille également les outils, l'infrastructure, les ressources et les protocoles de sécurité requis, garantissant un cadre standardisé et professionnel. En favorisant l'excellence technique et l'innovation, elle joue un rôle clé dans la formation des talents en cybersécurité et leur préparation au monde professionnel.

1.1 But du concours

L'objectif de ce concours est d'offrir aux concurrents l'occasion de faire valoir leur expertise pratique et théorique dans des domaines clés de la cybersécurité à travers des épreuves ciblées et axées sur les compétences. Les défis proposés couvrent un large éventail d'activités, notamment l'attaque et la défense d'un réseau et de dispositifs réseau, le déchiffrement de messages chiffrés à l'aide de techniques de cryptographie, l'analyse du trafic réseau pour détecter les vulnérabilités, la réalisation de tests de pénétration et l'analyse des réseaux à la recherche de ports ouverts et de services actifs. Les concurrents effectueront également une analyse de la preuve informatique pour extraire des informations, vérifier l'intégrité des fichiers et décoder les informations dissimulées, ainsi que pour analyser les journaux pour détecter les accès non autorisés et les activités suspectes. Ces tâches simulent des scénarios réalistes, mettant l'accent sur la précision, la maîtrise technique et les capacités de résolution de problèmes dans un cadre structuré et favorable. Les compétences et connaissances en cybersécurité porteront notamment sur :

- Maîtrise des techniques de cryptographie fondamentales et des protocoles de communication sécurisée.
- Capacité à analyser le trafic réseau et la détection des vulnérabilités dans des contextes réalistes.
- Compétence en analyse de la preuve informatique, incluant l'extraction de métadonnées et la vérification de l'intégrité des fichiers.
- Aptitude à réaliser des tests de pénétration et des tests d'intrusion, avec capacité d'analyse et d'exploitation des vulnérabilités.
- Expérience en mappage et analyse de réseaux, notamment pour identifier les hôtes actifs, les ports ouverts et les services actifs.

- Habileté à analyser les journaux afin de détecter les accès non autorisés et les activités suspectes.
- Capacité à appliquer les principes de cybersécurité dans la conception et la mise en œuvre de systèmes et processus sécurisés.

1.2 Comité technique

Président du comité technique (responsable du concours) : Kevin Ramdas, Humber Polytechnic: kevin.ramdas@humber.ca;
Francis Syms, Humber Polytechnic : francis.syms@humber.ca

Membres du comité technique:
Ahmed Al-Ani, Humber Polytechnic : ahmed.al-ani@humber.ca
Ian Thomson, Fleming College : ian.thomson@flemingcollege.ca
Myles Peterson, Cambrian College : myles.peterson@cambriancollege.ca
Sohrab Farooq, Conestoga College : sfarooq@conestogac.on.ca
Mark Shtern, Seneca Polytechnic : mark.shtern@senecapolytechnic.ca
Haidar Jabbar, Humber Polytechnic : haidar.jabbar@humber.ca

Pour obtenir réponse à vos questions concernant cette fiche descriptive, celles-ci doivent être soumises au moins deux (2) semaines avant la date prévue du concours.

Pour toute question d'ordre général ou non technique, veuillez nous écrire à : competitions@skillsontario.com

1.3 Horaire du concours

Lundi 4 mai 2026	
Heure	**Activité**
7 h à 7 h 30	Enregistrement à l'endroit prévu pour le concours
7 h 30 à 8 h	Séance d'information
8 h à 12 h	Concours (Volet 1) **3 activités**
12 h à 12 h 30	Dîner (pause en santé mentale obligatoire)
12 h 30 à 16 h 30	Concours (Volet 2) **3 activités**

* Les concurrents doivent se présenter à l'heure prévue pour leur concours sans quoi le comité technique se réserve le droit de les disqualifier.

Cérémonie de clôture : mercredi le 6 mai 2026, de 9 h à 12 h

Ce concours est offert à titre de concours en démonstration pour les Olympiades 2025.

Ce concours n'est pas offert dans le cadre des **Olympiades canadiennes des métiers et des technologies (OCMT)**

Le concours de Cybersécurité est offert dans le cadre du Mondial des métiers. Cependant, il n'est pas possible pour les concurrents des Olympiades de Compétences Ontario de participer au Mondial des métiers sans faire partie de l'équipe du Canada.

1.4 Renseignements additionnels – À réviser

Renseignements pour les concurrents :

- Fiches descriptives : https://www.skillsontario.com/olympiades-de-competences-ontario?na=302#Scopes
- Guide de préparation des concurrents : https://www.skillsontario.com/files/www/2024_Docs/Guide_de_preparation_et_dentrainement_des_concurrents_Olympiades_de_Competences_Ontario_French_April_30_2024.pdf
- Admissibilité des concurrents : https://www.skillsontario.com/olympiades-de-competences-ontario?na=302#CompetitorEligibility
- Règles et règlements : https://www.skillsontario.com/olympiades-de-competences-ontario?na=302#CompetitorRules
- Plan d'étage du site des Olympiades : https://www.skillsontario.com/oco-visiteurs?na=62#FloorPlan
- Cérémonie de clôture et remise des prix : https://www.skillsontario.com/ceremonie-de-cloture?na=359

2. COMPÉTENCES ET CONNAISSANCES ÉVALUÉES

Le concours offre aux concurrents l'occasion de faire valoir leurs compétences théoriques, pratiques et rédactionnelles. Les concurrents seront évalués en fonction de leur aptitude à réaliser les tâches suivantes :

- Déchiffrement de messages à l'aide de techniques de cryptographie
- Analyse du trafic réseau pour identifier les vulnérabilités et les communications non sécurisées
- Cartographie des réseaux, recherche des ports ouverts et services actifs
- Réalisation de tests de pénétration et de tests d'intrusion
- Analyse de la preuve informatique afin de découvrir des données dissimulées et vérifier l'intégrité des informations

- Analyse des journaux pour détecter les intrusions et repérer les activités suspectes
- Application des principes de cybersécurité pour résoudre des défis pratiques dans des contextes réels.

3. CRITÈRES D'ÉVALUATION

Le concours Cybersécurité des Olympiades de Compétences Ontario permet d'évaluer l'expertise technique et pratique des concurrents dans des domaines clés de la cybersécurité. Les critères d'évaluation sont centrés sur des compétences essentielles, telles que la mise en œuvre du cryptage pour garantir des communications sécurisées, l'analyse de la preuve informatique et la collecte de preuves, la réalisation de tests d'intrusion, y compris l'analyse des vulnérabilités et les tests de pénétration, ainsi que la configuration et la gestion de réseaux sécurisés. Les concurrents seront également évalués sur leur capacité à détecter et atténuer les menaces de cybersécurité, et à développer des stratégies efficaces d'intervention face aux incidents. Ces domaines sont conçus pour refléter les défis réels auxquels font face les professionnels en cybersécurité, assurant ainsi que les concurrents démontrent à la fois une compréhension approfondie et une application concrète des pratiques de cybersécurité essentielles.

Tableau 1 : Concours et critères d'évaluation

Aspect	Compétences requises	Pondération
Protocoles de sécurité réseau : aspects offensifs et défensifs	Réalisation d'attaques réseau courantes, suivie de l'implémentation de mécanismes de défense pour sécuriser l'infrastructure.	20
Opérations du serveur : aspects offensifs et défensifs	Identification et exploitation des vulnérabilités d'un serveur réseau, suivies de la mise en place de mesures de sécurisation adaptées.	15
Serveur Windows : aspects offensifs et défensifs	Utilisation d'outils pour exploiter les vulnérabilités d'un serveur Windows et de ses bases de données.	20
Preuve informatique : Extraction de métadonnées, vérification de l'intégrité des fichiers et décodage des données dissimulées.	Capacité à extraire des métadonnées, vérifier l'intégrité des fichiers, décoder les données dissimulées et documenter les résultats.	10
Ingénierie sociale : Analyse des vulnérabilités, tests de pénétration et exploitation.	Maîtrise de l'identification des vulnérabilités, de la conduite d'analyses et de l'exploitation efficace des faiblesses.	10
Analyse des logiciels malveillants : Analyse du trafic réseau pour détecter les vulnérabilités et les communications non sécurisées.	Identification des événements malveillants, suspects et bénins par l'examen des logiciels malveillants. Évaluation du caractère malveillant	25

Aspect	Compétences requises	Pondération
	d'un fichier et application du cadre Mitre ATT&CK Matrix au scénario.	
Pointage		**100**

4. ÉQUIPEMENT, MATÉRIEL ET INFRASTRUCTURE

Afin d'offrir une expérience à la fois professionnelle et stimulante, le Comité technique de Compétences Ontario veille à ce que les concurrents disposent des outils et des ressources nécessaires pour relever des défis réalistes en cybersécurité. Chaque concurrent aura accès à deux postes de travail de bureau dotés d'une mémoire vive suffisante pour exécuter jusqu'à trois machines virtuelles simultanément. Le concours comprendra entre quatre et six mini-défis, chacun axé sur un aspect spécifique de la cybersécurité et mettant en avant différentes compétences clés. Les mini-défis seront accompagnés d'images préconfigurées intégrant les outils nécessaires à la cryptographie, à l'analyse de réseau, aux tests de pénétration, à l'analyse de la preuve informatique et à l'examen des journaux. Aucun accès Internet ne sera disponible pendant le concours.

Ces ressources permettent aux concurrents de démontrer efficacement leurs compétences techniques tout en respectant les normes professionnelles. Les concurrents devront également apporter certains effets personnels et se conformer aux directives vestimentaires afin de garantir un environnement équitable et uniforme. Vous trouverez ci-dessous la liste détaillée des éléments fournis par le comité ainsi que ceux exigés des concurrents :

Fournis par le comité technique de Compétences Ontario :

- **Ordinateurs de bureau ou ordinateurs portables haute performance** préconfigurés avec les outils nécessaires pour les tâches de cybersécurité.
- **Logiciels et ressources préinstallés,** y compris :
  - **Kali Linux** pour les activités d'analyse de pénétration et d'analyse d'intrusion.
    - **NMAP/ZenMap**, Y**ersinia, arpspoof, hydra, setoolkit, OpenVAS, Nessus, Metasploit, Bloodhound, Kerberoasting/Mimikatz, impacket secretdump, hashcat, PEStudio, RegShot, ExifTool**
  - **Windows 10 clients**
  - **Window Server 22**
    - **DHCP, DNS, FTP, Active Directory**
  - **Simulateur de réseau (*packet tracer*) GNS3 avec images Cisco IOS pour configurer les réseaux**
  - **Serveur HTTP utilisant Python**
  - **Wireshark** pour l'analyse du trafic réseau et l'identification des vulnérabilités.

  - **Décodeurs Base64** pour le décryptage des données dissimulées.
  - **Outils de hachage** (p. ex., sha256sum, md5sum) pour la vérification de l'intégrité des fichiers.

- **Fichiers préchargés et données PCAP**, y compris les messages chiffrés, les captures de trafic réseau et les artefacts de preuve informatique à des fins d'analyse.
- **Machines virtuelles (Linux and Windows)** avec des environnements configurés pour des tâches spécifiques telles que la cryptographie, la preuve informatique et l'analyse.
- **Environnements réseau simulés** avec des vulnérabilités pour les tâches d'analyse et d'exploitation.
- Des points de ravitaillement en eau seront mis à la disposition des concurrents et des bénévoles dans chaque aire de concours. Il est nécessaire d'apporter une bouteille d'eau réutilisable puisqu'aucun gobelet ne sera fourni.
- **Dîner fourni :** Un dîner simple sera offert (sandwich, biscuit et eau – n'oubliez pas d'apporter une bouteille d'eau réutilisable). Des options adaptées aux régimes alimentaires suivants seront proposées : végétarien, végétalien, halal, intolérance aux produits laitiers et intolérance au gluten. Les personnes suivant un régime alimentaire particulier, ayant des préférences spécifiques ou estimant que le repas offert pourrait ne pas être suffisant peuvent apporter leur propre nourriture sans noix. Le choix du dîner s'effectuera lors de l'inscription des élèves.

Fournis par les concurrents :

- **Stylo ou crayon** pour documenter les processus, prendre des notes et accomplir les tâches écrites du concours.
- **Bouteille d'eau réutilisable,** des postes d'eau seront disponibles près des lieux du concours.
- Collations (sans arachides de préférence)
- **Tenue vestimentaire adéquate,** assurant une apparence professionnelle sans logos, à l'exception de ceux de leur école ou de leur établissement.
- **Les concurrents doivent lire attentivement l'intégralité de cette fiche descriptive ainsi que tout document connexe publié en ligne, le cas échéant.** Les consignes verbales à elles seules ne suffisent pas à une préparation adéquate. Tous les concurrents doivent prendre lire l'intégralité de la fiche descriptive.
- Chaque année, la fiche descriptive du concours provincial est publiée sur le site Web de Compétences Ontario au plus tard le 31 janvier : https://www.skillsontario.com/olympiades-de-competences-ontario?na=302#Scopes. La fiche descriptive pour l'année précédente du concours demeure également accessible à titre de référence.

5. SÉCURITÉ

La sécurité est la priorité absolue des Olympiades de Compétences Ontario, englobant à la fois la sécurité des concurrents et le respect des meilleures pratiques de cybersécurité. Afin d'assurer un environnement sûr, les concurrents doivent respecter les lignes directrices suivantes :

Pratiques de cybersécurité :

- Manipuler toutes les données (simulées ou réelles) avec rigueur, en suivant des protocoles stricts de confidentialité et de traitement des informations. Cela implique :
    - Garantir qu'aucune donnée sensible ne soit partagée, copie ou stockée en dehors de l'aire désignée du concours.
    - Utiliser des méthodes d'authentification sécurisées et ne jamais divulguer de mots de passe, de clés d'accès ou d'autres informations sensibles.
    - Éviter toute action pouvant mener à un accès non autorisé, à une fuite de données ou à la compromission des systèmes.
- Se conformer aux réglementations en vigueur en matière de protection des données et aux normes de cybersécurité reconnues, telles que celles décrites dans la RGPD, la LPRPDE ou des normes équivalentes, afin de garantir que les environnements simulés reflètent les exigences du monde réel.

Règles de conduite :

- Toute violation des règles éthiques, notamment la falsification des configurations d'autres concurrents, la violation des protocoles de confidentialité ou l'exploitation abusive de l'aire du concours, entraînera une disqualification immédiate.
- Les concurrents doivent faire preuve de respect et adopter une conduite professionnelle tout au long du concours.

Signalement des incidents :

- Les concurrents sont encouragés à signaler rapidement toute préoccupation en matière de sécurité ou de technique au comité technique afin de permettre une résolution.

Sécurité des concurrents et sécurité numérique :

- Adopter de bonnes pratiques ergonomiques, telles que maintenir une posture saine et prendre des pauses régulières, afin de prévenir la fatigue et les tensions physiques.
- Respecter toutes les consignes de sécurité dans l'aire du concours, y compris les mesures de prévention des incendies, la sécurité électrique et le maintien d'un espace de travail dégagé pour éviter les risques de chute.

La sécurité est une priorité dans le cadre du concours. Le non-respect des normes de sécurité, des protocoles de cybersécurité ou des règles de conduite peut entraîner une disqualification à la discrétion des juges et du comité technique. Les concurrents peuvent être exclus du concours s'ils ne démontrent

pas les compétences requises, ne respectent pas les règles de sécurité ou enfreignent les protocoles de confidentialité et de protection des données.

This Employment Ontario program is funded in part by the Government of Canada and the Government of Ontario.

Ce programme Emploi Ontario est financé en partie par le gouvernement du Canada et le gouvernement de l'Ontario.