WSET® Courses at Approved Program Provider (APP)
Calgary Co-op Wine Spirits and Beer Policies

Terms and conditions
Full payment must be made at time of official registration submission.

Costs of Courses
WSET Level 1 Award in Wines - $349.99
WSET Level 2 Award in Wines - $799.99
WSET Level 3 Award in Wines - $1449.99
WSET Level 1 Award in Spirits - $274.99
WSET Level 2 Award in Spirits - $699.00
Please Note – 5% GST is not included in the above listed course costs. If registering through Event Brite there is an administration fee charged by Event Brite.

Cancellations
Cancellation of a paid registration will be accepted up to 30 calendar days prior to the start of the course. An administration fee of $75.00 plus the full cost of any study materials supplied will be deducted from the original purchase amount.

Cancellations of paid registrations later than 30 calendar days but less than 15 calendar days will be subject to an administration fee of $200.00 plus the full cost of the study materials.

Cancellations later than 15 calendar days prior to the start of the course are non-refundable.

Transfers
Transfer of a paid registration can be made up to 15 working days before the course start date, with payment of a $75.00 admin fee plus the cost of any additional study materials required for the new student.

Transfer requests made within 15 working days of the examination date will incur the admin fee and cost of examination paper which will have been ordered via WSET.

If a paid registration is cancelled anytime during the ten working days prior to the start of the course, or any time after the start of the course, no refund of the course fees or transfer will be made.

Examinations
Examinations are included within the dates that your course is scheduled. Rewrites or makeup exams will be reviewed on a case by case basis pending the exam and administration fees that correspond to the program level.

Examination Resit Costs:
- Level 1 Wines/Spirits - $95.00
- Level 2 Wines/Spirits - $145.00
- Level 3 Wines Theory - $275.00
- Level 3 Wines Tasting - $175.00

Courses Cancelled by Co-op Wine Spirits and Beer
Course fees will be refunded in full if Co-op Wine Spirits Beer changes a course date or cancels a course if enrolments do not reach the required minimum numbers. Notification will be made in the 10 working days prior to the planned start date of the course.

Study Materials
Level 1 course materials are provided to students on the first day of the course. They will not be posted in advance.
Levels 2 and 3 course materials for advance study and reading may be picked up at a selected location or dispatched to a confirmed address of the student.

Release and Waiver
The below Release and Waiver text is as it appears on a separate Release and Waiver form to be signed and dated by course participants.

CALGARY CO-OPERATIVE ASSOCIATION LIMITED
WSET WINE or SPIRITS COURSE
RELEASE & WAIVER

IMPORTANT: THIS IS A LEGAL COMMITMENT; READ IN FULL AND UNDERSTAND BEFORE AGREEING TO, AND ACCEPTING, THE TERMS HEREUNDER.

I, _____, hereby certify, represent, warrant and agree to the following:

1. I certify that I have read, understood and will comply in all respects with the WSET wine course policies and procedures.

2. Any references to Calgary Co-operative Association Limited ("**Calgary Co-op**") in this Release & Waiver shall be deemed to include Calgary Co-operative Association Limited its directors, officers and employees, successors, assigns, licensees and agents and any party, their assigns or individuals, with whom Calgary Co-op engages in association with the WSET wine course.

3. I hereby certify that I am of legal drinking age in Alberta.

4. I acknowledge that the WSET wine course involves the tasting of wine. I agree and acknowledge that I am required to spit out the wine and that the consumption of alcohol is prohibited. Further, I take full responsibility for my actions, safety and welfare during the WSET wine course. I represent that I do not have and am not aware of any medical or physical condition(s) that would make it inadvisable for me to participate in the WSET wine course. I am fully aware that the participation in the WSET wine course involves risks, dangers and hazards including but not limited to the dangers of consuming alcohol, particularly the dangers of drinking and driving, and accept full responsibility in the event my actions are affected by any alcohol I have elected to consume.

5. I take full responsibility for my actions and the amount of wine and or other alcohol that I consume at all WSET wine courses, classes and events held by or associated with Calgary Co-op.

6. I AM AWARE OF THE RISKS, DANGERS AND HAZARDS ASSOCIATED WITH PARTICIPATION IN THE WSET WINE COURSE, AND I FREELY ACCEPT AND FULLY ASSUME ALL SUCH RISKS, DANGERS AND HAZARDS AND THE POSSIBILITY OF PERSONAL INJURY, DEATH, PROPERTY DAMAGE OR LOSS RESULTING FROM THEM. I ALSO ACCEPT RESPONSIBILITY FOR ANY PERSONAL OR PROPERTY DAMAGE CAUSED BY OR AS A RESULT OF MY PARTICIPATION IN THE WSET WINE COURSE.

7. To the fullest extent permitted by law, I hereby forever release, waive, covenant not to sue, exonerate, discharge and agree to hold Calgary Co-op harmless from any and all liability, claims, demands, and causes of action whatsoever that I may have against Calgary Co-op with respect to any injury, illness, death, property damage or other loss that may result, directly or indirectly, arising from my participation in the WSET wine course and/or events. I specifically understand and agree that this Release & Waiver forever discharges Calgary Co-op from any liability or claim that I may have against Calgary Co-op with respect to any injury, illness, death, property damage or other loss that may result arising from my participation in the WSET wine courses and/or events, whether caused by the negligence of Calgary Co-op or otherwise. I further understand and confirm that Calgary Co-op does not assume any responsibility or obligation to provide financial or other assistance, including, but not limited to medical, health, or disability insurance, in the event of injury, illness, death, property damage or other loss.

8. I expressly agree that this Release & Waiver is intended to be as broad and inclusive as permitted by the laws of the Province of Alberta and that this release shall be governed by and interpreted in accordance with the laws of the Province of Alberta and the laws of Canada applicable therein. I agree that in the event that any clause or provision of this Release & Waiver shall be held to be invalid by any court of competent jurisdiction, the invaliding of such clause or provision shall not otherwise affect the remaining provisions of this Release & Waiver which shall continue to be enforceable. I further agree that this Release & Waiver shall bind my assigns, heirs, administrators and executors forever.

9. I have read the WSET wine course description and the conditions of my registration and participation, INCLUDING THIS RELEASE & WAIVER and agree to them.

I hereby certify and represent that I have read the foregoing and fully understand the meaning and effect of same, and, being of legal age in my province of residence and intending to be legally bound, I have executed this document as evidenced below.

Signature: _____ Date: _____

Print Name: _____

Complaints Policy WSET Awards Courses

This complaints policy is designed to set out guidelines and parameters for the management and resolution of complaints against Coop Wine Spirits Beer WSET course administration. This complaints policy outlines the procedures to resolve any such complaint, concern or grievance to the execution, administration, invigilation and instruction of all WSET Awards courses and examinations as provided to consumers or employees at Coop Wine Spirits Beer.

It is the sole responsibility of Coop Wine Spirits Beer as an Approved Program Provider to make available, implement and follow all policies provided by WSET as it concerns Malpractice and Maladministration of WSET Awards courses and all other Policies set in place and outlined in the WSET APP Operating Handbook. Coop Wine Spirits Beer will ensure that all policies set forth by the WSET in regards to these practices be made available to any and all Nominated Educators, Examinations Officers and Invigilators and students.

Coop Wine Spirits Beer will respond openly, honestly and earnestly to any and all complaints as they pertain to the WSET Awards course offerings and their administration and execution.

Definition of a Complaint

Any and all formal expressions of concern, frustration, disappointment or dissatisfaction with the instruction, delivery or quality of service, a policy or procedure, or the conduct of another person as it relates to WSET Awards Courses.

Complaints

Complaints may include, but are not limited to:

a) Failure to follow procedures or adhere to regulations in conduct of examinations
b) Failure to return examination papers within the required timeframe or
c) Returning exam papers by regular post and not recorded delivery or trackable courier
d) Failure to issue results to candidates in a timely manner
e) Poor or dissatisfactory deliverance of WSET Awards courses
f) Providing incomplete, poor or outdated course materials
g) Inappropriate, unprofessional or unorganized course instruction

Responsibilities

- Any and all complaints will receive a direct response within 15 business days of complaint receipt. Email Andrew Paulsen or Kevin Schorath at wset@coopwinespiritsbeer.com
- Every effort will be made to have any and all complaints resolved within 15 business days
- It is the responsibility of the APP Main Contact and Nominated Educator to ensure that all Coop Wine Spirit Beer WSET course offerings adhere to all policies, rules, regulations and procedures as set forth in the APP Operating Handbook from WSET
- It is the responsibility of Nominated Educator to ensure that all WSET examinations offered by Coop Wine Spirits Beer are administered in adherence to the Centre Agreement, Code of Practice, Invigilation Instructions provided in the Operating Handbook and Examination Regulations as issued to this Approved Program Provider

- It will be the responsibility of the Sommelier Coordinator and Examinations Officer to respond to and resolve any and all concerns and complaints as to the deliverance of the WSET Awards courses. This will be done so in the timeliest of manner
- The Sommelier Coordinator and Examinations Officer for WSET APP Coop Wine Spirits Beer will be responsible for the resolution of all complaints with the guidance of and the adherence to all WSET specifications and in line with the Centre Agreement, Code of Practice, Invigilation Instructions provided in the WSET Operating Handbook and Examinations Regulations as issued to this Approved Program Provider
- It is the responsibility of the Sommelier Coordinator and Examinations Officer to ensure the Nominated Educator complies to and adheres to all complaint resolutions
- Coop Wine Spirits Beer will keep an open log of any and all complaints or Grievances as to the WSET Course offerings and their resolutions.
- If complainant is not satisfied with response resolution provided by Calgary Co-op Wine Spirits beer. Please contact Quality Assurance at WSET. Email – qa@wsetglobal.com
- Coop Wine Sprits Beer will remain open to any and all feedback from candidates and remain focused on always striving to become the best Approved Program Provider and WSET Examination instructors. Please email Andrew Paulsen or Kevin Schorath at wset@coopwinespiritsbeer.com

Complainants Responsibility

- To provide a clear and honest account of their concerns and expectations for the outcome of the complaint
- Provide all relevant documents to assist in the investigation and/or resolution of the matter
- Engage openly in the complaint handling process

Conflict of Interest Policy

As an APP, Calgary Co-op Wine Spirits Beer is required to identify to WSET and assist in managing or monitoring actual, potential and perceived conflicts of interest ('Conflicts of Interest') involving both APP staff and students. This policy complements WSET's conflicts of interest policy and works to safeguard the integrity of WSET qualifications and promote confidence in **WSET and Calgary Co-op Wine Spirits Beer** processes and procedures.
This policy applies to all **Calgary Co-op Wine Spirits Beer** staff **and students** and to any individual acting on behalf of **Calgary Co-op Wine Spirits Beer**.
A **Conflict of Interest** exists where an individual has interests or loyalties that could adversely influence their judgement, objectivity or loyalty to WSET or **Calgary Co-op Wine Spirits Beer** when conducting activities associated with WSET qualifications.
Examples of Conflicts of Interest include:
• The assessment of candidates by an individual who has a personal interest in the result of the assessment for any or all individuals concerned;
• The moderation of assessment of candidates by an individual who has a personal interest in the result of the assessment for any or all individuals concerned;
• The undertaking of a WSET qualification by any individual employed by an APP;

• The invigilation of a WSET assessment by any individual involved in the delivery of training leading to the assessment;
• The coaching of candidates by any individual involved in the assessment of candidate scripts;
• The employment by an APP of individuals engaged in the delivery of taught programmes or in the role of Internal Assessor in another APP;
• The investigation of a non-compliance incident by someone who is unable to act impartially.

Some of these Conflicts of Interest are manageable and therefore acceptable. For example, if family member of one of **Calgary Co-op Wine Spirits Beer's** educators or APP staff takes a qualification and exam through **Calgary Coop Wine Spirits Beer, or** when an employee of **Calgary Co-op Wine Spirits Beer,** or of the WSET, takes a WSET qualification through **Calgary Co-op Wine Spirits Beer**, we can notify WSET in advance and work with them to put in place measures to maintain the integrity of the exam. Some Conflicts of Interest are not manageable and are not acceptable. For example, no mitigation efforts overcome the conflict created when an individual when a single individual serves as the educator and exam officer of an exam for a family member where an external invigilator is not available.
Any staff member or student of **Calgary Co-op Wine Spirits Beer** who becomes aware of a Conflict of Interest must inform Andrew Paulsen – apaulsen@coopwinespiritsbeer.com - as soon as possible. Andrew Paulsen will inform the WSET of the possible conflict of interest and will work with WSET to put any protective or mitigating measures in place to manage the conflict on a case-by-case basis. If WSET and **Calgary Co-op Wine Spirits Beer** determine the conflict is not manageable, Andrew Paulsen will inform any impacted APP staff or students.
Please note that the failure to declare a conflict of interest may have consequences for the student or ***Calgary Co-op Wine Spirits Beer*** *because we are required to report conflicts to WSET.*

Calgary Co-op Wine Spirits Beer Policies pertaining to Privacy and Data Protection
WSET APP Calgary Co-op Wine Spirits Beer may share student information such as names, email addresses and birthdate with WSET for the purposes of registering students for WSET courses and exams. All information shared with WSET will be handled under WSET's Privacy & Data Protection policy.

Privacy and Data Protection policies are covered by BULLETIN NO. 240-00-01 and BULLETIN NO. 190-00-02 in the CALGARY CO_OPERATIVE ASSOCIATION LTD's POLICY AND PROCEDURE MANUAL – They are as follows

BULLETIN NO. 240-00-01 – PROTECTION OF PERSONAL INFORMATION
A. PURPOSE
The purpose of this policy is to govern the collection, use and disclosure of personal information held by Calgary Co-operative Association Limited and its wholly-owned subsidiaries ("Calgary Co-op") in a manner that recognizes both the right of individuals to protect their personal information and the need of Calgary Co-op to collect, use, or disclose personal information for the purposes reasonably required to establish, manage and terminate employment relationships and generally operate its business.
B. LEGISLATION
The collection, use and disclosure of personal information is governed by the *Personal Information Protection Act* of Alberta, and, where applicable, the *Personal Information Protection and Electronic Documents Act (Canada)* (the "Acts"). All obligations of Calgary Co-op under this policy are subject to the exceptions in the Acts. In meeting its responsibilities under the Acts, Calgary Co-op shall consider what a reasonable person would consider appropriate in the circumstances.

The Chief Executive Officer has assigned responsibility for ensuring compliance with the Acts to the Chief Financial Officer who also serves as the Privacy and Compliance Officer, at:
Calgary Co-op Privacy Officer
#110, 151 – 86th Avenue S.E.
Calgary, AB T2H 3A5
Email: bwillmore@calgarycoop.com

C. IMPORTANT DEFINITIONS

"**Business Contact Information**" means an individual's name, position or title, business telephone number, business address, business email, business fax number, and other similar business information.

"**Personal Employee Information**" means personal information about an employee or potential employee that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship, but does not include personal information that is not about an individual's employment.

"**Personal Information**" means information about an identifiable individual and includes personal employee information but does not include business contact information or work product Information.

"**Work Product Information**" means information prepared or collected by an individual as part of the individual's responsibilities or activities related to the individual's employment or the business of Calgary Co-op.

D. COLLECTION OF PERSONAL INFORMATION

(i) Personal Employee Information

Personal employee information includes, but is not limited, to the following: name; residential address; age; gender; identification numbers; marital status; dependent status; qualifications and skills; career history; employment and personal references; medical or health records determined to be relevant to an employee's employment; work record; bank account information; security clearance details; social insurance number; driver's license number and driver's abstract; attendance record; and testing results.

Calgary Co-op may collect, use or disclose personal employee information without the consent of the individual where:

a) the individual has been given prior notification of the purposes of the collection, use or disclosure of the personal employee information; and
b) the collection, use or disclosure is reasonable for the purposes of establishing, managing or terminating the employment relationship.

These purposes include, but are not limited to:

 recruiting, hiring, and terminating employees;
 administrating compensation, benefits, pension and other retirement benefits, severance, and other monetary benefits or employment;
 managing, developing and maintaining a workforce that supports the business goals of Calgary Co-op;
 training employees;
 monitoring and fostering employee safety and employee health;
 meeting legal and regulatory requirements;
 protecting the assets of Calgary Co-op;
 administering labour relations; and
 communication with employees.

Calgary Co-op may disclose personal employee information to the following third parties:

a) our benefit providers;
b) our payroll company, if applicable;
c) the union, if applicable;
d) government departments and agencies such as the Canada Revenue Agency, Employment Insurance, Canada Pension Plan, Labour Relations Board, Occupational Health and Safety, and the Worker's Compensation Board;
e) employee assistance program professionals;
f) confidential medical or legal advisors;

(ii) Other Personal Information

Unless otherwise required by law, Calgary Co-op will obtain consent from the individual before collecting, using or disclosing personal information (other than personal employee information) about the individual.

E. SECURITY OF PERSONAL INFORMATION

Calgary Co-op will protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, use or disclosure. The nature of the security arrangements will be determined by the sensitivity of the personal information.

Employees, such as supervisors, who access personal employee information to perform their job duties, have an obligation to keep the information secure.

F. ACCURACY OF PERSONAL INFORMATION

If personal information is likely to be used to make a decision that affects an individual, Calgary Co-op shall make a reasonable effort to ensure that personal information collected is accurate and complete. Employees shall immediately advise Calgary Co-op of any changes to their personal employee information

G. ACCESS TO PERSONAL INFORMATION

On written request by an individual, Calgary Co-op will provide the individual with the individual's personal information under the control of Calgary Co-op, information about the ways in which the personal information has been or is being used and the names of individuals and organizations to whom the personal information has been disclosed. The written request must provide sufficient detail to enable Calgary Co-op, with a reasonable effort, to identify the personal information being sought. Calgary Co-op will respond to the individual not later than 45 days after receiving the request, unless the period to respond is extended in accordance with the Acts.

H. REQUEST FOR CORRECTION OF PERSONAL INFORMATION

An individual may request in writing that Calgary Co-op correct an error or omission in the personal information about the individual that is under the control of Calgary Coop. The written request must provide sufficient detail to enable Calgary Co-op, with a reasonable effort, to identify the correction being sought. Calgary Co-op will respond to the individual not later than 45 days after receiving the request, unless the period to respond is extended in accordance with the Acts.
If Calgary Co-op is satisfied on reasonable grounds that no correction is to be made, Calgary Co-op may annotate the personal information with the correction that was requested but not made.

I. RETENTION

Personal information that is used to make a decision that directly affects an individual will be retained for at least one year following the decision. Personal information will be destroyed when it is reasonable to assume that the purpose for which the personal information was collected is no longer being served by retention of the personal information and retention is no longer required for legal or business purposes. Records, including any containing disciplinary information, may be retained longer or as needed by Calgary Co-op.
Job applicant information received by Calgary Co-op will be retained as per Policy #800-00-00 Employee Files.

J. COMPLAINT PROCESS

A complaint about the application of the Acts may be made in writing to:
Calgary Co-operative Association Limited
Privacy Officer, Finance and Administration
#110, 151 – 86th Avenue S.E.
Calgary, AB T2H 3A5
Or email: bwillmore@calgarycoop.com
The written complaint must provide sufficient detail to enable Calgary Co-op, with a reasonable effort, to identify the concern. Calgary Co-op will respond to the complainant within 45 days of the date the complaint was received.

BULLETIN NO. 190-00-02 – INFORMATION SECURITY

Section references are to sections in Payment Card Industry Data Security Standard (PCI DSS) v3.2 and ISO 27002:2013.

POLICY:

ISO 5.1 / PCI 12.1, 12.6

The Vice President of IT shall maintain a policy framework for Information Technology, including information
security, which shall be reviewed on an annual basis.
All personnel who access the corporate computer network shall acknowledge annually that they have read
and understood applicable policy and procedures.
Any waivers or exceptions to this policy or IT standards must be approved by the Vice President of IT.

SECURITY MANAGEMENT:

ISO 6.1 / PCI 12.4, 12.5

Calgary Co-op shall establish an Information Security Management System of governance, an information
security owner and an information security organization, allocate clear, segregated information security responsibilities with documented procedures and maintain appropriate contact with relevant authorities and

external organizations.
The responsibility for providing an information services environment that provides for confidentiality, integrity and availability of the data and information processed through the corporate applications, systems
and networks is that of the CEO of Calgary Co-op who has delegated the responsibility to the Vice President
of Information Technology. Responsibility for information security on a day-to-day basis is every employee's
duty and specific responsibility for information security is not solely vested in the Information Technology
Department. The CEO, through the designated delegate, is responsible to report on the status of Information Security to the directors on at least an annual basis and to:

- Review the current status of Calgary Co-op's information security;
- Review and monitor security incidents within the company;
- Approve and later review information security projects;
- Approve new or modified information security policies, and
- Perform other necessary high-level information security management activities.

Specifically, the Vice President of IT is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines and procedures.
The Vice President of IT is to provide the direction and technical expertise to ensure that Calgary Co-op's information is properly protected. This includes consideration of the confidentiality, integrity, and availability
of both information and the systems that handle it. The IT department will act as a liaison on information security matters between all Calgary Co-op departments and divisions, and must be the focal point for all information security activities throughout Calgary Co-op. The IT department must perform risk assessments, prepare action plans, evaluate vendor products, participate on in-house system development
projects, assist with control implementations, investigate information security breaches, and perform other
activities which are necessary to assure a secure information handling environment.
The IT Department has the authority to create, and periodically modify, both technical standards and standard operating procedures (SOP) that support this information security policy document. These standards and procedures, when approved by appropriate Calgary Co-op management, have the same scope and authority as if they were included in this policy document.
The IT Department shall conduct (or manage a third party who conducts) an annual threat risk assessment.
The report resulting from this assessment must include a detailed description of the information security risks currently facing the organization, as well as specific recommendations for preventing or mitigating these risks.
The IT Department shall prepare, maintain, and distribute one or more information security manuals that
concisely describe Calgary Co-op's information security policies and procedures.

PERSONNEL SECURITY:

ISO 7.1, 7.2, 7.3 / PCI 12.6, 12.7

The Vice President of IT shall maintain a security awareness program that emphasizes security prior to employment, during employment and upon termination. The security awareness program will provide initial
and annual refresher information security training appropriate to the user's role.

Where a high risk of fraud or attack exists, such as IT system and network administrators, contracts or positions (other than cashiers) that handle payment cards or other highly sensitive information, steps shall
be taken in the recruitment process to examine the background of potential recruits to determine their suitability for handling confidential data. This may include police, credit or criminal background checks.
Managers shall emphasize secure practices to their teams and supervise personnel with access to sensitive
data.
Non-compliance with IT policy may lead to disciplinary action including termination.

CONTRACTORS AND SERVICE PROVIDERS:

ISO 7.1 / PCI 12.8

Service providers with access to cardholder data or the cardholder data environment shall be selected and
managed using practices that incorporate due diligence.
A list will be maintained of service providers who handle credit card data or whose work could impinge on
the security of the cardholder data environment. Contracts with these service providers will incorporate wording to protect information and acknowledgement by the service providers of their responsibility for the
security of cardholder data.
Information will be maintained about which PCI DSS requirements are managed by each service provider.

INFORMATION ASSET MANAGEMENT :

ISO 8.1, 8.2, 12.6 / PCI 2.4, 12.3

The Vice President of IT shall develop, maintain and communicate a standard for information asset management to:

- Assign responsibilities for information asset management.
- Inventory all critical information assets.
- Identify the owner of each critical information asset.
- Ensure that business impact analysis is conducted and maintained for all critical information assets.

The Vice President of IT shall define policy statements for:

- Usage of critical technologies.
- Acceptable use of information systems.
- The destruction and disposal of information assets.
- The return of company-owned assets and the wiping of privately-owned equipment used to store company information upon termination of employment.

Calgary Co-op shall define an information classification standard to:

- Define an information classification scheme.
- Ensure that information is classified according to the classification scheme.
- Define an information and media labelling scheme.

MEDIA:

ISO 8.3 / PCI 9.5, 9.6, 9.7, 9.8

The Vice President of IT shall develop, maintain and communicate a media management standard to:

- Assign responsibilities for media management.
- Ensure the control of physical media, its acquisition, access, secure storage, handling, transfer and disposal

Cardholder data shall not be stored in unencrypted electronic form on any physical media.

Users shall not store sensitive data on uncontrolled removable media (e.g. CD, DVD, USB thumb drive, or external hard drive).

PHYSICAL SECURITY:

ISO 11.1, 11.2 / PCI 9.1, 9.2, 9.3, 9.4, 9.9, 9.10

Access to sensitive areas shall be limited and/or monitored.

Authorization for access to sensitive areas shall be determined according to individual job function. When the individual's justification for access is no longer valid, access and the means to achieve it shall be revoked.

Access to network jacks, network equipment, wireless access points and telecommunications lines shall be limited according to risk.

Activities conducted in sensitive areas shall be minimized.

Visitors shall be required to wear a visitor badge in controlled areas.

Visitor access to sensitive areas shall be logged.

Critical equipment shall be:

- Sited in secure areas or afforded other physical protection according to risk.
- Properly maintained, with records of maintenance activity retained for the life of the equipment.
- Protected according to risk from environmental failure, power failure and natural disasters.
- Protected according to risk when moved off-site.

Users shall:

- Protect equipment in their care that is used to process company information.
- Clear their desks and workspace of sensitive material when not working in the vicinity.
- Ensure that they clear their computer screen of sensitive information when there is the potential for their screen to be viewed by an unauthorized person.

Workstations shall be configured with an inactivity timeout that implements a screensaver and requires re-authentication after no more than 15 minutes of inactivity.

Card readers used for access control shall be protected from tampering.

ACCESS MANAGEMENT:

ISO 9.1, 9.2, 9.3, 9.4 / PCI 7.1, 7.2, 7.3, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8

User access and privileges to services and functions that handle sensitive information (including cardholder data) shall be limited according to the principles of need-to-know and least privilege and assigned according to job function. Segregation of duties shall be applied where there is a high risk of fraud due to a single person performing all the steps in a single process.

Documented approval by an appropriate authority (normally the user's direct line manager) shall be required in order to grant access, stating the date from which access becomes effective and (as necessary for employees and always in the case of non-employees) the date on which access should expire.

User access and privilege shall be reviewed at least annually and access shall be revoked for which there is no longer a business justification.

No user or administrator is permitted to alter their own access privilege nor is an administrator permitted to use their own administration identity to adjust the privileges of their own regular user ID.

User access and electronic identity shall be withdrawn as soon as the user ceases to be entitled to them. Entitlement to access shall cease upon termination or after 90 days of inactivity. The files and mailbox

associated with a user shall, by default, be disposed of one year after cessation of access entitlement unless required for longer for legal purposes or the user's manager determines that earlier disposal is acceptable. After withdrawal of a user's electronic identity, that identity shall not be re-assigned to any other user for a period of 6 months.
Authentication shall be sufficiently strong to establish adequate trust in the user's identity according to the
potential for masquerading in the operating environment, the classification of information that can be accessed and the user's rights within the environment.
Two-factor authentication shall be required (except where sufficient other risk mitigation is in place) to provide access to:
• Sensitive information.
• Sensitive system/network/application administration functions.
• Business functions from outside the network.
Authentication activity shall be protected by strong encryption.
Access to utility programs that can be used to administer the operating environment shall be limited to personnel with a role that justifies the access.
Access to source code shall be limited to personnel with a role that justifies the access.
Unique identification shall be required of users who access sensitive data, including cardholder data, and of users with system/network/application administration privileges. Anonymous or generic accounts for non-sensitive access are only permitted with exception approval from IT Security.
Vendor support accounts shall only be enabled for the duration of actual vendor support work.
User accounts shall be set to lockout for a period of 30 minutes if there are 6 successive unsuccessful attempts to login (5 for systems handling health information), except where explicit approved exemption is
provided.
Unless explicit exemption is approved and compensating security is provided, computing devices connected to the corporate network shall be configured with a 15-minute inactivity timeout that requires reauthentication
to unlock the device.
Users with system/network/application administration privileges shall not use their regular user ID for administration functions and instead shall be provided with unique administrator identification to which the
necessary privileges are given and from which e-mail and internet access are withheld.
Passwords must meet the criteria in the Standard for Passwords.
HR shall promptly inform IT of any changes to employee status that might affect user access privileges; managers shall promptly inform IT of any changes to non-employee user status that might affect user access privileges.
Service accounts (used for non-interactive process identification and authentication) may be permitted exemption of password life and first-use password rules.

STORED DATA:

PCI 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7

Locations and media of stored confidential information shall be identified.
Sensitive data shall not be stored on uncontrolled physical media or cloud storage without security protection and authorization.
Cardholder data shall only be stored if essential for business purposes and then only permitted data values
shall be stored; storage shall be in hashed or strongly-encrypted form (electronic records) or physically secured

containers (physical records) and only for as long as the business need is justified.
Personal Identifying Information (PII) and Cardholder Primary Account Number (PAN) data shall be masked
or truncated where the user has no justification to view the full PII or PAN.
Where data integrity is critical, mechanisms shall be utilized, according to business need, to ensure that either:
• Data is not altered or destroyed in an unauthorized manner.
• Unauthorized data alteration is made readily apparent.
The Vice President of IT shall develop, maintain and communicate a cryptographic management standard.
The Vice President of IT shall develop, maintain and communicate a data backup and restoration process to ensure that:
• Data is backed up at a frequency appropriate to business need
• Data backups are stored in a physically separate location from the original data
• Data restoration is periodically exercised
The Vice President of IT shall develop, maintain and communicate a data management standard to:
• Assign responsibilities for data management.
• Ensure the appropriate protection of data in storage, during use and in transit.
• Ensure the appropriate destruction of data that is no longer required.

NETWORK SECURITY:

ISO 13.1 / PCI 1.1, 1.2, 1.3, 1.4, 1.5

Segmentation shall be used to compartmentalize the network architecture as a means of risk management.
Infrastructure shall maintain a current set of network architecture diagrams.
Firewall rule changes shall be managed through formal change control.
The Vice President of IT shall develop, maintain and communicate a network security standard to:
• Assign roles and responsibilities to internal resources and service providers for network security.
• Define the requirements for network architecture including segmentation.
• Define firewall and router configuration standards
• Define configuration review standards
• Require the maintenance of a current network diagram (or set of diagrams).
• Require the use of a formal change management process to change firewall rules.

TRANSMISSION SECURITY AND CRYPTOGRAPHY:

ISO 8.3 / PCI 9.5, 9.6, 9.7, 9.8

The Vice President of IT shall develop, maintain and communicate a transmission security standard to:
• Ensure that data transmissions comply with PCI DSS.
• Ensure that outgoing transmissions are monitored for policy violations.

SYSTEM ACQUISITION AND CONFIGURATION:

ISO 8.3 / PCI 9.5, 9.6, 9.7, 9.8

System acquirers shall include security considerations in the acquisition process.
Only authorized systems and software shall be added to the operational environment.
Vendor-supplied defaults that could compromise security shall be removed or changed on commissioning a new system or application.
System images shall be defined for commonly-commissioned systems, to which new instances shall be configured.
The Vice President of IT shall develop, maintain and communicate a system and software acquisition standard to:

• Assign roles and responsibilities for system and software acquisition and configuration.
• Ensure that security considerations are included early in the acquisition lifecycle.
• Ensure that systems and software are only added to the operating environment once properly authorized.
• Ensure that vendor-supplied defaults (such as default accounts, default passwords and unnecessary functionality) are changed, where feasible.
• Define system image standards and require new systems to be configured to those standards.
• Define specifications for standard hardware and software with an exception management process for business requirements that cannot be met using the standard specifications

All requests for lease, rental or purchase of computer-related hardware, software or services must be reviewed by Information Technology prior to any commitment being made on behalf of Calgary Co-op.

SYSTEM AND SOFTWARE DEVELOPMENT:

ISO 6.1, 12.1, 14.2, 14.3 / PCI 6.3, 6.4, 6.5, 6.6, 6.7

Project managers shall include security considerations in system and software development.

Critical systems development shall be conducted in protected environments.

Test/development and operational environments shall be logically separated.

The Vice President of IT shall develop, maintain and communicate a system and software development standard to:

• Assign roles and responsibilities for system and software development such that development and operational deployment duties are segregated.
• Ensure that security considerations are included early in the project lifecycle.
• Maintain protected development environments for critical systems.
• Define a critical system software development protocol that is compliant with PCI DSS.
• Ensure that test/development and operational environments are logically separated.

SOFTWARE DEVELOPMENT TESTING:

ISO 14.2, 14.3

Software development testing shall include the testing of critical security functionality.

Live data shall not be used for test purposes unless adequate measures are in place to prevent its compromise.

The Vice President of IT shall develop, maintain and communicate a software development standard to:

• Assign roles and responsibilities for software development testing.
• Ensure that security testing is included at appropriate points in the software development lifecycle.
• Ensure that no live data is compromised through use in testing.

CHANGE CONTROL:

ISO 12.1, 14.2 / PCI 6.4

The Vice President of IT shall develop, maintain and communicate a change management process to:

• Assign responsibilities for change control.
• Define “change” in the IT context.
• Register formal changes.
• Record decisions regarding the change, its approval/rejection, test, execution, user notification and review.

All Production changes require approval from the business owner of the changed asset (or a designated representative) and IT management as detailed in the change management process.

All third parties engaged in a maintenance or change control procedure on Calgary Co-op’s systems, network or application assets shall be required to conform to the change management process and shall be supervised at all times by a Calgary Co-op employee.

VULNERABILITY MANAGEMENT:

ISO 12.6 / PCI 6.1, 6.2

The Vice President of IT shall develop, maintain and communicate a threat and vulnerability process to:

- Assign responsibilities for threat and vulnerability management.
- Identify and rate threats to corporate information and information systems.
- Identify and rate vulnerabilities in the operational environment.
- Initiate action to manage vulnerabilities according to risk.
- Review progress with vulnerability management.

The Vice President of IT shall develop, maintain and communicate a standard for system upgrade and security patching to:

- Assign responsibilities for upgrade and patch management.
- Require operating systems and applications to be upgraded as necessary to remain within vendor support life.
- Require operating systems and applications to be patched with relevant vendor-issued security patches within a defined time period of patch release, with the relevancy and time period to be based on risk and agreed by IT leadership.

MALWARE MANAGEMENT:

ISO 12.2 / PCI 5.1, 5.2, 5.3, 5.4

The Vice President of IT shall develop, maintain and communicate a process and a standard for malware management to:

- Assign responsibilities for malware management.
- Apply and manage anti-malware software tools and techniques.
- Maintain the currency of anti-malware detection and remediation tools.
- Define and maintain anti-malware specifications.

LOGGING:

ISO 12.2 / PCI 5.1, 5.2, 5.3, 5.4

The Vice President of IT shall develop, maintain and communicate a logging standard to:

- Identify the systems to be monitored and the events to be logged from those systems.
- Protect the logs from tampering.
- Ensure that clocks on logged and logging systems are synchronized.
- Define the log retention period.

All creation, amendment, deletion and privilege change of user IDs shall be logged.

Logs from security monitoring shall be under continuous review for indicators of potential security incidents.

SUPPLIERS:

ISO 13.2, 14.1, 15.1, 14.2, 15.2

IT-related supplier agreements and support contracts shall be reviewed by IT Security to ensure that they
include:

- Appropriate security requirements.
- Appropriate provision for security review during the lifetime of the contract.
- Provision for confidentiality agreements where appropriate.

MONITORING AND VULNERABILITY SCANNING:

PCI 11.1, 11.2, 11.3, 11.4, 11.5, 11.6

The Vice President of IT shall develop, maintain and communicate a vulnerability checking (scanning) process to:

- Assign authority and responsibilities for scanning.
- Define the required periodicity of scanning.

• Require periodic scanning for rogue wireless networks.
• Require periodic scanning for network vulnerabilities.
• Require periodic penetration testing.
• Define the follow-up procedures for scan results.

The Vice President of IT is authorized to perform monitoring and audit of the following information handling
activities and grant to appropriate personnel the logical and physical access required to perform such monitoring and audit functions:

• Access provisioning and privilege management.
• User level and/or system level access to any computing or communications device connected to the Calgary Co-op network.
• Storage, transmission and use of information (electronic, hard copy, etc.) that may be produced, transmitted or stored on Calgary Co-op's equipment or premises.
• Access to work areas (labs, offices, cubicles, storage areas, etc.).
• E-mail and messaging using Calgary Co-op systems or networks.
• Internet usage on Calgary Co-op systems or networks.
• Calgary Co-op telephone and cell phone usage (including personal devices formally authorized for conducting Calgary Co-op business).
• Calgary Co-op mobile device usage (including personal devices formally authorized for conducting Calgary Co-op business).

Networks shall be continuously monitored for indicators of potential security incidents.

File integrity checking shall be employed where appropriate to ensure data integrity.

Reviews of scanning activity shall be conducted to ensure compliance.

User internet activity shall be monitored and filtered in order to prevent users from deliberately or inadvertently accessing unauthorized websites. Logs of internet activity shall be retained for one year (3 months on-line) unless required for longer for legal or investigative reasons.

INCIDENT HANDLING:

ISO 16.1 / PCI 12.10

The Vice President of IT shall develop, maintain and communicate an incident response process to:

• Define incidents and security incidents
• Assign responsibilities for incident management.
• Establish incident response planning and preparation.
• Monitor, detect, analyze and report information security events and incidents.
• Log incident management activities.
• Handle forensic evidence.
• Escalate incidents through the management chain and communicate to appropriate parties.
• Contain the impact of an incident.
• Control recovery from an incident.
• Assess information security events and incidents to identify weaknesses and provide management feedback.
• Periodically test the incident response plan.

All users have a duty to report suspected information security incidents.

IT BUSINESS CONTINUITY AND DISASTER RECOVERY:

ISO 17.1, 17.2 / PCI 12.10

The Vice President of IT shall develop, maintain and communicate:

• A continuity plan for all critical IT functions, including security functions.
• A disaster recovery plan for all critical applications, services and dependent systems.

Solution designs will consider availability as part of the security assessment.
The disaster response plan will be tested at least annually.

OPERATIONAL SECURE ACTIVITIES:

ISO 17.1, 17.2 / PCI 12.10

The Vice President of IT shall develop, maintain and communicate an operation security standard to:

• Define roles and responsibilities for operational security.

• Define a regular back-up and restoration process with back-ups stored off-site and periodic exercise of restoration.

• Control the installation of operational software.

RISK ASSESSMENT*:*

PCI 12.2

The Vice President of IT shall develop, maintain and communicate an IT risk assessment process, aligned with the corporate Enterprise Risk Management process, to:

• Assign responsibilities for IT risk assessment.

• Define the methodology for IT risk assessment.

• Ensure that risk assessments are carried out for all initiatives that represent a change to the production environment. Initial risk assessments will determine whether more detailed risk assessment is justified.

• Ensure that risk assessments are periodically refreshed.

REMOTE ACCESS, MOBILE AND TELEWORKING SECURITY:

PCI 12.2

Use of mobile technologies to connect to the network shall be restricted to company-owned devices and only those privately-owned devices that meet an acceptable standard. Use of the devices shall be controlled through the application of mobile device management software to impose defined security settings, monitor and remotely wipe devices.

• Users of mobile devices connecting to the network must acknowledge this policy.

• Teleworking shall be enabled through mobile devices that meet the mobile device policy and through the use of remote access technologies that shall ensure connecting devices are checked for vulnerabilities and excluded if found to pose a risk to the network.

Remote access shall be achieved through a virtual private network connection, employing two factors of authentication or an equivalent management of the risk of malicious impersonation (masquerading).
Remote access connections shall require re-establishment and re-authentication after 8 hours of use.
Any remote access connection found to pose an active threat to the network may be immediately severed without notice to the user.
The IT Department shall maintain sufficient resource capacity and licences to enable all essential business personnel to connect remotely to the network in circumstances where personnel cannot utilize the head office workspace.
Personnel must not allow their remote access connection into the Calgary Co-op network to be utilized by any unauthorized personnel.

AUDIT: ***ISO 12.7, 18.1, 18.2***

IT practices and standards shall comply with legal, regulatory and PCI requirements.
The Chief Financial Officer shall coordinate audit activities of IT facilities.
The Vice President of IT may conduct an internal assessment of IT facilities, services, systems or usage at any time.

Calgary Co-op Wine Spirits Beer Policies pertaining DIVERSITY & EQUALITY
Are covered by BULLETIN NO. 860-00-00 regarding Respectful Workplace in the CALGARY CO-OPERATIVE ASSOCIATION LTD's POLICY AND PROCEDURE MANUAL – They are as follows:

POLICY
Calgary Co-operative Association Limited ("Calgary Co-op"), is committed to a safe, healthy, respectful, rewarding and harassment-free work environment for all employees. Calgary Co-op has developed a company-wide policy intended to prevent all forms of discrimination, and harassment of any type, including sexual harassment of its employees, and to deal quickly and effectively with any incident that might occur.
Harassment and/or discrimination will not be tolerated. Any violation of this policy will lead to discipline up to and including termination of employment.
Complaints of harassment and/or discrimination will be investigated in a timely manner to resolve the problem. Investigations will be undertaken discreetly and all information gathered through investigation will be kept confidential. The name of the complainant and the details of the complaint will not normally be disclosed to any person except when necessary for the investigation of the complaint or as required by law.
This policy is not intended to discourage a worker from exercising rights pursuant to any other laws, including the Alberta Human Rights Act.
This policy applies to all Calgary Co-op employees, both unionized and non-unionized.
Unionized employees are also subject to any relevant provisions of their collective agreement. For any inconsistency between this policy and the collective agreement, the provisions of the collective agreement will prevail in respect to unionized employees.
DEFINITIONS
Discrimination**:**
Calgary Co-op supports the fundamental principle that all persons are equal in dignity and human rights with regard to race, religious beliefs, colour, gender, gender identity, gender expression, physical or mental disability, age, ancestry, place of origin, marital status, family status, source of income, sexual orientation, or any other "Protected Grounds" as listed in the Alberta Human Rights Act. In this policy, discrimination is any distinction based upon one of the protected grounds, which negatively impacts an employee who is a member of the protected group, whether by imposing burdens, obligations, or disadvantages not imposed upon others or withholding opportunities, benefits, or advantages available to others. Discrimination will be interpreted in a manner consistent with any defences available under the law.
Sexual harassment:
Sexual harassment in the workplace is defined as any single or repeated verbal remark or physical contact of a sexual nature that is objectionable or unwelcome and that a person knows or reasonably ought to know will cause offence or humiliation to a student or adversely affect the student's health and safety. It includes unwanted sexual advances or requests for sexual favors, which threatens job security, affects work opportunities, or negatively impacts the working conditions or employment atmosphere in which any employee works. Sexual harassment can occur between people of differing authority or between people of similar authority. Sexual harassment can be directed at an individual or at a group.

Sexual harassment includes but is not limited to unwelcome behavior of a sexual nature such as touching a person or other unwelcome physical contact, sexual innuendos, commenting on one's body, asking questions about a person's sexual relationships, telling sexual jokes in person or emails, or displaying posters or other offensive materials of a sexual nature.

Personal harassment:

Personal harassment in the workplace is defined as any unwanted, unsolicited offensive behavior, comments, or displays, either explicitly or implicitly, directed at any employee, customer, or supplier of Calgary Co-op and made on the basis of any protected grounds. Comments about size or weight, comments about intimate, personal relationships with other employees or any other words or actions that cause, or are likely to cause offense or humiliation to any employee, customer, or supplier, or cause interference with any employee's performance. Personal harassment can be a single incident or repeated actions. It can occur between people of differing authority or between people of similar authority.

PROCEDURE / INVESTIGATING COMPLAINTS

All complaints of discrimination or sexual or personal harassment are to be dealt with in a confidential, timely, and impartial manner. Any complaint brought forward in good faith as well as anyone providing information will be protected from any form of retaliation or reprisals by co-students, APP invigilators and Calgary Co-operative Association Limited.

Complaints of discrimination or sexual or personal harassment will usually require an investigation. The process of any investigation will depend on the nature of the complaint and surrounding circumstances. Some issues can be resolved more easily than others.

At any point in the process, employees have the right to file a complaint with the Alberta Human Rights Commission or seek legal counsel.

Further Information Contact

Please contact bwillmore@calgarycoop.com for any questions regarding diversity and equality.

Calgary Co-op Wine Spirits Beer

Reasonable Adjustment Policy

Both WSET and **Calgary Coop Wine Spirits Beer** want to make WSET assessments accessible for all students, so none are at an advantage or disadvantage based on a disability or differing ability. This policy and the reasonable adjustment process allows us **Calgary Co-op Wine Spirits Beer** to work with you, our student, *before an assessment* to gather the information we need to submit a request to WSET and work with them to make arrangements that give students access to WSET qualifications.

A **reasonable adjustment** is any accommodation or arrangement that helps to reduce the effect of a known disability or difficulty that substantially disadvantages a student's assessment. Using a reasonable adjustment does not impact how WSET grades your exam, or your result, but WSET cannot agree to reasonable adjustments where your particular difficulty directly affects performance necessary to complete the assessment outcomes (e.g. inability to smell or taste for a Level 3 Exam). The goal of a reasonable adjustment is to give you equal access to a WSET qualification, not to give unfair advantages over other students who take an assessment without the same adjustment, or to affect the overall reliability of the assessment outcomes that are explained in the course Specification.

Examples of reasonable adjustments may be:

- Changing standard assessment arrangements, for example allowing candidates extra time to complete the assessment activity;
- Adapting assessment materials, such as providing materials in large text format;
- Providing access facilitators during assessment, such as a sign language interpreter or reader;
- Re-organising the assessment room, such as removal of visual stimuli for an autistic candidate.

Calgary Co-op Wine Spirits Beer will gather the information we need from you to submit a Reasonable Adjustment Application form to WSET. WSET must approve and arrange reasonable adjustments before the assessment activity takes place. Before completing enrolment with **Calgary Co-op Wine Spirits Beer,** we will give all students access to this policy and the chance to identify any special needs that could require a reasonable adjustment. If a student identifies a special need, **Calgary Co-op Wine Spirits Beer** will give the student the Reasonable Adjustment Application form as soon as possible and work with the student to gather the necessary information.

For any student seeking a reasonable adjustment, please contact **Andrew Paulsen –** apaulsen@coopwinespiritsbeer.com with:

- Your full name;
- contact information;
- description of the special need, disability or differing ability that requires an adjustment; and
- supporting documentation.

You must submit this information at least **20 working days** before the exam date for Levels 1-3 qualifications and at least. The information you submit will be shared with WSET and will be handled under WSET's Privacy and Data Protection Policy.

***Calgary Co-op Wine Spirits Beer** will keep records of all reasonable adjustment applications.*

Special Consideration Policy

Special consideration is any adjustment given to a student who has temporarily experienced an illness or injury, or other event outside of their control at the time of the exam that significantly affects their ability to take the exam or their ability to show their knowledge and understanding in the assessment.

Special consideration is only for things that happen *immediately before or during* an exam that have a material impact on your, the student's, ability to take the exam or on your performance. To be eligible for special consideration, you must have completed the whole course and would have been fully prepared if not for the temporary illness, injury or other uncontrollable event. A special consideration may be for an individual (e.g. a student becomes ill the day of the exam) or a group of students (e.g. an exam is interrupted by a natural disaster).
You may be eligible for special consideration if:
• Your performance on the exam is adversely affected by an event outside of your control. This may include temporary illness, temporary injury, bereavement or exam room conditions;

• Reasonable adjustments which were agreed in advance of the exam proved inappropriate or inadequate;

• The application of special consideration would not make a passing result and certificate misleading about the student's ability to satisfy the qualification's assessment criteria.

Applying for special consideration
If you have taken an exam, or your exam is immediately approaching, and you feel that you have a temporary injury or illness, or other uncontrollable event that has interfered with your ability to complete your exam, please contact **Calgary Co-op Wine Spirits Beer** as soon as possible. **Calgary Co-op Wine Spirits Beer** will provide you with a Special Consideration Application Form, which must be completed and returned with supporting documentation within **5 working days** after the effected exam. The information you submit will be shared with WSET and will be handled under WSET's Privacy and Data Protection Policy.
If there has been serious disruption during an exam affecting a group of students, **Calgary Co-op Wine Spirits Beer** will submit a detailed report of the circumstances and candidates affected to WSET to request a special consideration.
Calgary Co-op Wine Spirits Beer *will keep records of all applications for special consideration.*

Malpractice & Maladministration Policy

Both **Calgary Coop Wine Spirits Beer** and WSET have policies and procedures in place to protect WSET students and safeguard the integrity of WSET qualifications. **Calgary Co-op Wine Spirits Beer** ensures compliance with **Calgary Coop Wine Spirits Beer and WSET's** policies through this Malpractice and Maladministration Policy, which gives a framework for both us and you to identify, report and manage potential malpractice or maladministration.
Non-compliance with **Calgary Co-op Wine Spirits Beer or** WSET Policies and Procedures can fall into two distinct, but related, categories:

1. **Maladministration**, where the non-compliance is generally unintentional, or the result of mistakes, carelessness, inexperience or poor processes; and
2. **Malpractice** where the non-compliance is intentional or the result of a negligent or reckless action without consideration of the consequences of the action.

Context is important and the line between maladministration or malpractice is not always clear: for example, maladministration incidents may become malpractice (e.g. if you fail to implement corrective measures, repeat the same or similar incident, or attempt to misrepresent or hide information during an investigation); or there may be mitigating factors that turn potential malpractice into maladministration. Though malpractice and maladministration are distinct concepts, they can shade into one another.

Malpractice and maladministration are always case, context and fact specific. Both APPs and students can commit malpractice and maladministration.

For APPs:
 Failure to adhere to WSET Policies and Procedures;
 Failure to follow WSET requirements for course delivery or exam regulations;
 Failure to follow WSET's candidate registration and certification procedures;
 Late student registrations;
 Fraudulent claim for certificates/fraudulent use of certificates/reproduction or forgery of certificates;
 Withholding critical information from WSET quality assurance;
 Insecure storage of exam materials;
 Revealing or sharing confidential exam materials with candidates ahead of an exam;
 Intentional attempts to manipulate exam results so that they do not reflect the candidate's actual exam performance;
 Issue of incorrect exam results/failure to issue results to students in a timely manner;
 Failure to timely respond to WSET;

 Unauthorised reading/amendment/copying/distribution of exam papers;
 Failure to report changes in APP ownership/personnel/location/facilities;
 Denying WSET access to information, documentation, workforce, facilities;
 Failure to return exam papers within the specified timeframe or to follow delivery and tracking regulations;
 Infringements of WSET copyright, trademarks, intellectual property rights and brand identity;
 Use of unqualified and/or unregistered educators or internal assessors;
 Breach of confidentiality
 Misleading advertising/publicity;
 Any action likely to lead to an adverse effect.
 Failure to disclose a Conflict of Interest;

For students:
 Cheating, or facilitating cheating, including the use of unauthorised devices or materials;
 Disruptive behaviour in an exam;
 Plagiarism of any nature by students;
 Impersonation (including forgery of signatures);
 Unauthorised reading/amendment/copying/distribution of exam papers;
 Any action likely to lead to an adverse effect;
 Breach of confidentiality.

In general, we also expect that both **Calgary Co-op Wine Spirits Beer** staff and our students should treat others and be treated professionally and respectfully at all times. We will treat inappropriate behaviour including verbal or physical abuse, persistent or unrealistic demands, or threats that cause stress to staff as misconduct and may report student misconduct to WSET as necessary.

Reporting and Investigation of Malpractice or Maladministration

As an APP, we aim to ensure compliance with WSET Policies and **Calgary Co-op Wine Spirits Beer** policies and will keep records of potential or actual malpractice or maladministration by you, our students, or our staff.

We are required to notify WSET immediately of any non-compliance issues that could be malpractice or maladministration, so that WSET can investigate the non-compliance under their own Malpractice and Maladministration Policy.
We ask that you also raise any concerns or non-compliance issues that may be malpractice or maladministration with **Calgary Coop Wine Spirits Beer** as soon as possible by following the process outlined in our Complaints policy.

During WSET's investigation, they may reach out to **Calgary Coop Wine Spirits Beer** or to you directly to request further information or conduct an interview. Please respond to any requests promptly and honestly.

Managing Non-Compliance
If WSET identifies malpractice or maladministration, they will consider its impact and may apply sanctions. WSET will take all reasonable steps to ensure the sanctions do not disadvantage uninvolved students affected by malpractice or maladministration. However, in some cases, they may need to disallow or withhold results and/or certificates.

Sanctions Applicable to Students/Candidates
Written Warning

- The student is issued with a written warning that if the offence is repeated within a set period of time then further specified sanctions will be applied

Exam Result Declared Null and Void

- A student's exam result is disallowed. This may include invalidation and recall of a certificate already issued.

Disqualification from a Qualification
The student is disqualified from participating in the concerned qualification with immediate effect and further excluded from participating in any further WSET qualifications for a period of 12 months. This includes access to WSET materials.
Student Disqualification
The learner is disqualified from participating in any courses or assessments leading to WSET qualifications. This includes access to WSET materials.
Disqualification from use of WSET certified logos and postnominals
Actions bringing WSET into disrepute may result in the student or graduate being barred from use of WSET postnominals and WSET certified logos.

Appeals
If you wish to appeal penalties or sanctions WSET has imposed due to Malpractice or Maladministration, please follow the procedures laid out in WSET's Complaints Policy.