



Date: **March 11, 2020**

Date Last Updated: **March 13, 2019**

**To: Chair and Board of Governors**  
**From: President**  
**Subject: MONITORING REPORT – EL-2f Asset Protection**

---

**The President shall not allow corporate assets to be unprotected, inadequately maintained nor unnecessarily risked.**

I hereby present the monitoring report on our Executive Limitations policy “Asset Protection” according to the schedule set out. I certify that the information contained in this report is true and represents compliance with all aspects of the policy unless specifically stated otherwise.

**The President shall not:**

- 1. “Allow the organization, Board members, staff, and volunteers to be uninsured against theft, fire, and casualty losses to a prudent replacement value and against liability losses.”**

I interpret “prudent” and “appropriate” to mean coverage is consistent with industry standards for Colleges.

**Evidence:**

The College is part of a consortium of 20 colleges, which joined forces to purchase insurance in 2012. The contract was recently re-tendered in 2017 with Aon being the successful proponent for a 5-year agreement including 2 additional 1-year renewal periods.

Aon policy renewal coverage continues to be similar to the other Ontario Colleges. Attached is a summary of the College’s 2019-20 insurance coverage, see “Appendix A.”

In addition to the coverage noted in Appendix A, we recently added an additional policy for Kidnap, Ransom & Active Assailant effective October 10, 2019 with a renewal date of April 1, 2023.

I report compliance.

- 2. “Subject facilities and equipment to improper wear and tear or insufficient maintenance.”**

I interpret “adequate” to mean sufficient to support safe operations and to avoid foreseeable accidents or losses.

**Evidence:**

MCU in conjunction with Colleges Ontario, is investing in deferred maintenance systems for colleges across Ontario to update deferred maintenance estimates and to assist in planning to deal with the large maintenance backlog in colleges.

Capital & Special funds provided by the MCU for 2019-20:

- Facilities Renewal Program (FRP) for the maintenance, repair, and renovation of existing facilities: \$452,400 grant. NOTE: September 30, 2019 extension for use of funds.
- College Equipment and Renewal Fund (CERF) to acquire and renew instructional equipment and learning resources: \$451,800 grant; NOTE: September 30, 2019 extension for use of funds.
- Apprenticeship Enhancement Fund (AEF) to purchase new equipment or upgrade shops: \$189,137 grant.

Major Capital Projects:

- TEC Hub Capital Campaign: \$5M goal; Conditional contributions from NOHFC (\$2M); FedNor (\$1M); February 2020 achieved milestone of more than \$1.69M in private contributions (\$2M goal).
- Nakina Drive Bridge: \$2.5M project; Phase 1 completed: December 21, 2018; Phase 2: completed July, 2019.
- Sioux Lookout High School Campus Co-location Project: \$2.3 million project was completed in May 2019.
- Old Fitness Centre (Neebing Building & Bubble): Demolition of the old facilities is currently underway and will be in 2 phases: Phase 1 – abatement and demolition in early spring 2020, Phase II – parking lot, walkway and roadway upgrades complete mid August, 2020..
- Lecture Theatre: \$.7 assessment and engineering work to be complete by March 31, 2020 with renovations to be complete over the summer of 2020.

I report compliance.

**3. “Unnecessarily expose the organization, its Board, or staff to claims of liability.”**

I interpret “unnecessarily” to mean that reasonable processes are in place to foresee areas of risk and to avoid/mitigate claims.

**Evidence:**

Occupational health and safety (OHS) is managed through a strong internal responsibility system supported by a network of internal health and safety partners, including Joint Health and Safety Committee Members, Health and Safety Representatives, Designated First Aiders, Fire Wardens and the Confederation College Campus Response Team. Our external partners, including the member organizations of Health and Safety Ontario and St. John Ambulance further support our OHS efforts.

Lease and contract agreements are reviewed by authorized college representatives, our Insurance Broker (AON) and, where applicable, by legal counsel to identify and mitigate potential areas of risk.

I report compliance.

**4. “Receive process or disburse funds under controls that are insufficient to meet the Board-appointed auditor’s standards.”**

I submit this is clear and requires no further interpretation.

**Evidence:**

The Board-appointed auditors (Grant Thornton) perform a review of the college’s system of internal checks and controls. Their review did not result in the identification of any weaknesses that would materially affect the financial statement disclosure for the year-ending March 31, 2019. The auditors provided an audit opinion that the financial statements of the College are in accordance with Canadian public sector accounting standards and the financial statements present fairly, in all material respects, the results of operations, changes in net assets and cash flows. A surplus of \$17,782,747 of revenue over expenses was reported in the audited financial statements for the year ending March 31, 2019.

On December 11, 2019, the auditors presented their audit plan to the Audit Committee and management for the year ending March 31, 2020. The audit plan is the auditor’s report to the Audit Committee outlining the terms of the audit engagement, the proposed audit strategy and the level of responsibility assumed by the auditors under Canadian Auditing Standards (CAS).

I report compliance.

**5. “Allow intellectual property, information or files to be exposed to loss, improper access or significant damage, or operate without maintaining records in accordance with a records retention schedule approved by legal counsel.”**

I interpret “loss or significant damage” to mean irrecoverable loss or damage. Compliance will be demonstrated when generally accepted principles of secure information management are followed.

**Evidence:**

The College continues to follow industry standard operating procedures for the protection and management of College information and files including:

- Operation of an industry standard computing facility distributed between the McIntyre and Shuniah buildings. Features include controlled access to limited staff, backup emergency generator power supplies, redundant server facilities, regular backups of all central servers, and offsite storage of backup media. The College uses two uninterruptable power supplies (UPS) to maintain power in the Shuniah Building computer room. Both units were serviced in January 2020;

- Implementation in 2019 of the Data Domain backup unit for disaster recovery. The solution is a tiered system that improved on the reliability, speed and capacity for data recovery and archival processes. The unit supplements the existing storage area network (SAN) which provides for on line retrieval of past versions of files. The SAN was also upgraded in 2018 as per manufacturer’s requirements to obtain continued support. Both systems were successfully used to recover from the major cyber security event of Feb 2020;
- Use of a document electronic imaging and archiving solution with the College’s Banner ERP system. The solution has allowed for improved document/record storage, security, and protection within the College. Work continues on eliminating paper-based records used in administrative processes;
- Intellectual Property, Freedom of Information / Protection of Privacy, Information Collection and Retention policy and operating practices are reviewed on an ongoing basis by a sub-committee of the Strategic Leadership Team;
- The College is completing year 3 of the 5 Year Strategic IT Plan with current progress ahead of schedule (75% complete). The plan builds on the IT maturity of the College which is ahead of industry norms in the educational sector and our higher education peer group.
- The College is also engaged with the Ontario Cybersecurity Higher Education Consortium. An assessment identified Confederation College ahead of its peer group in most categories of cyber security management and system implementation. Improvements to meet identified deficiencies are being developed and resourced.

**See also Appendix B: IRM Report for Information Technology**

I report compliance.

- 6. “Invest funds or hold operating capital in instruments or vehicles inconsistent with MCU policies, or without consideration of rate of return, value at maturity and cash flow needs.”**

I interpret this to mean that investments (defined as funds not required in the short term) will be managed professionally to maximize return, value and to meet cash-flow needs.

**Evidence:**

All College investments comply with MCU policy Directives for Investments. The College’s endowment funds are held in vehicles approved by the Trustees Act for public donations or the Financial Administration Act for government contributions. All College operating funds are held in either an interest bearing current account or GIC’s as per the Financial Administration Act and compliance is verified by external financial auditors.

Our Short Term Investments of operating funds are usually in a combination of high yield accounts and GICs to maximize our investment income. The maturities of investments are matched to the College's cash flow needs. Currently, the College does not have any Short-Term Investments.

I report compliance

**7. "Compromise the independence of the Board's audit or other external monitoring."**

I submit this is clear and requires no further interpretation.

**Evidence:**

The Board's Audit Committee consisting of Governors, the President and Senior Finance staff has acted as a Board interface with the external financial auditor, Grant Thornton LLP. The auditors meet at least twice per year with the Audit Committee to present their plan for the current year and subsequently to receive the results of the financial audit and the related financial statements. The auditors are required to report on any conflict of interest to the Audit Committee. The Audit Committee meets 'in camera' with the auditors to provide an opportunity for auditors to comment to the Audit Committee without management present. There were no conflicts of interest expressed by the auditors at the Audit Committee's June 3, 2019 meeting.

The President and senior Finance staff attest in a representation letter, drafted by auditors per audit standards, that we have reported all financial information and not knowingly withheld any information relevant to the preparation of the financial statements.

Other external monitoring and auditing reports are provided to the Ministry of Colleges and Universities, which ask for financial information, enrolment data and key performance indicators from the College. We also comply with Revenue Canada, Ministry of Transport and other regulatory reporting requirements. There have been no reported instances of any compromise to the independence of the audit or other external monitoring.

**8. "Set tuition fees."**

I interpret this to recognize that the Tuition and Ancillary Fees Reporting Operating Procedure under the Minister's Policy Directive states "that the college is responsible for ensuring that tuition and ancillary fees for all programs of instruction and courses operated by the college have been approved by the Board of Governors."

**Evidence:**

The Board of Governors approved the tuition and ancillary fees for the 2020-21 academic year at their January 8, 2020 meeting. On January 17, 2019, the Minister of Colleges and Universities announced changes to the College tuition levels and how ancillary fees are to be categorized (mandatory or optional). Under the new Tuition Fee Framework, colleges are required to reduce

tuition fee levels by 10 percent in 2019-20, relative to 2018-19 levels and tuition levels in 2020-21 are to remain the same as the 2019-20 tuition (tuition freeze).

I report compliance.

**9. “Make a single purchase or commitment of greater than \$1,000,000. Splitting orders to avoid this limit is not acceptable.”**

I interpret this to mean that the President may not make a commitment (i.e. individual purchase order or invoice) that would result in a financial expenditure of greater than \$1,000,000 per year. The routine commitments identified in the Boards approved Purchasing Spending Authorization Limits Practice, ch2-s2-06, (inventory purchases for ancillary operations, Sun Life employee benefit remittances, Revenue Canada payroll remittances, utilities, taxes and postage meter) would continue to be excluded.

**Evidence:**

A computer listing of individual vendors that were approved or paid greater than \$1 million in the last year identified the following: Penn-Co Construction (TEC Hub Project) and SUCCI (Student Ancillary and Other Student Fees collected by the College on behalf of SUCCI).

I report compliance.

**MOTION:**

**THAT we accept Report EL2f – Asset Protection, showing full compliance with a reasonable interpretation of the policy.**

Respectfully submitted,

Kathleen Lynch  
President

**Confederation College  
 Principal property and casualty coverages 2019-2020**

<b>Insurance Coverage</b>	<b>Limits</b>
Property & Business Interruption	200,000,000
Equipment Breakdown	200,000,000
Commercial General Liability	25,000,000
Umbrella Liability	15,000,000
Media Liability	1,000,000
Automobile	1,000,000
Garage Automobile	1,000,000
Directors & Officers and Educational Errors & Omissions	5,000,000
Excess Directors & Officers and Educational Errors & Omissions	5,000,000
Crime	Various
Cyber Liability	1,000,000
Aviation General Liability	10,000,000
Aviation Hull & Liability	10,000,000
Business Travel Accident	200,000
Occupational AD&D ( <i>maximum limit</i> )	500,000
Excess Workers' Compensation	Various
Kidnap, Ransom & Active Assailant/Assault ( <i>new</i> )	5,000,000

EL-2f – Appendix B

**Integrated Risk Management Reporting to the Board**

EL-2f Asset Protection Focus: Information Technology		
Item	Risk	Mitigation Strategy
<ul style="list-style-type: none"> <li>• <b>IT reliability and availability</b></li> <li>• <b>Data privacy, quality and integrity</b></li> <li>• <b>IT security</b></li> </ul>	<ul style="list-style-type: none"> <li>• The risk of information technology systems, business applications and telecommunications systems being unavailable to support operations.</li> <li>• The risk that there are inadequate controls in place to ensure the privacy, quality, integrity and accuracy of electronic information.</li> <li>• The risk of failing to appropriately secure networks, systems and applications.</li> </ul>	<ul style="list-style-type: none"> <li>• Identification of infrastructure renewal priorities in the College 5-year Strategic IT Plan. Implementation is ahead of schedule with 79% funded through the third year.</li> <li>• Implementation of the College’s initial Cyber security strategy following the principle of Protect-Detect-React, and refinement in 2020</li> <li>• Development of a College Cyber security strategy and plan for 2019 following the principle of Protect-Detect-React.</li> <li>• Continued management of appropriate multi-zone firewall technology, anti-virus software, network security, intrusion detection appliances and second-generation firewall;</li> <li>• Continued regular installation of industry software security patches into College servers;</li> <li>• Assessment of College maturity in Cyber Security planning with the Ontario Cyber Security Higher Education Consortium (ON-CHEC)</li> <li>• BitSight 3<sup>rd</sup> party security assessment engaged in Feb 2019 as a cyber security benchmarking exercise.</li> <li>• Planned penetration test of College networks and servers through an industry specialist;</li> <li>• Continued refinement and testing of Computer Services’ Disaster Recovery Plan. Redundant servers to provide continuity in the event of a failure have been</li> </ul>



EL-2f Asset Protection Focus: Information Technology		
Item	Risk	Mitigation Strategy
		<p>implemented and located in the McIntyre Bldg. Full system recovery test exercises are executed each summer to ensure disaster recovery systems provide the necessary recovery capacity and demonstrate that IT staff have the skills necessary to restore service in a timely manner;</p> <ul style="list-style-type: none"> <li>• Password protection and multiple levels of logical security to control access to sensitive electronic information with industry norm strength-of-password protocols.</li> <li>• Biannual audits of student data to confirm compliance with data retention and storage standards;</li> <li>• Communications to staff on topical cyber threats – example Ransomware, <i>Cyber Security 101</i> training seminars and planned online phishing training and testing exercises;</li> <li>• Implementation of multifactor authentication for account logins of high value cyber targets.</li> <li>• Included in the College’s insurance coverage is a Cyber Liability policy.</li> </ul>