DISCLAIMER

The following document is provided by the Faculty of Business and IT at UOIT in Oshawa, Ontario, Canada as a means to provide staff, students and faculty the ability to understand the policies, procedures and responsibilities that shall be assumed in the networking lab held under the direction of the university. The policies defined by this document are designed as a guideline and are subject to change without notice and where necessary.

THE FACULTY OF BUSINESS AND IT

UOIT

Simcoe 1158 – UOIT Networking Lab

ACCEPTABLE USE POLICY

SECTION ONE

PURPOSE

A. The Faculty of Business and IT and UOIT have invested a significant amount of time and money into designing, building and maintaining the Simcoe 1158 networking lab. To protect these investments, this policy document seeks to clarify any misinterpretations or misconceptions which may be causing confusion among faculty, staff or students.

B. The Faculty of Business and IT and UOIT encourage the use of this lab and the equipment contained within. However, all students, faculty and staff should remember that electronic media and services provided by the university remain property of the school and that the purpose of the facilities is to facilitate and support the learning experience. All individuals have the responsibility to use these resources in a professional, ethical and lawful manner.

C. To ensure that all participants are responsible, the following guidelines have been established. No policy can lay down rules to cover every possible situation. Instead, this document is designed to express the philosophies of the Faculty of Business and IT and UOIT and set forth general principles when using any service provided by this lab environment.

D. All participants must also be familiar with and accept the terms of the Information Technology Acceptable Use Policy as set forth by UOIT Campus IT Services. Details of this document can be found at: http://its.dc-uoit.ca/its/use_policy.php.

SECTION TWO

PROHIBITED COMMUNICATIONS

A. Electronic media cannot be used for knowingly transmitting, retrieving or storing or displaying communication that is:
   1. Discriminatory or harassing;
   2. Derogatory to any individual or group;
   3. Obscene, sexually explicit or pornographic;
   4. Defamatory or threatening;
   5. In violation of any license governing the use of software; or
   6. In violation of any policies already set forth by the IT Services department and/or UOIT.

SECTION THREE

PERSONAL USE

A. The Internet access provided in the networking lab by UOIT and the Faculty of Business and IT is primarily for educational use to facilitate the prosperous learning environment at the school. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-educational purposes is understandable and mildly acceptable and all such use should be done in a manner that does not negatively affect the classroom environment or the systems' use for their educational purposes. However, students, faculty and staff are expected to demonstrate a sense of professional responsibility and not abuse this privilege. Students shall also understand that this privilege may be revoked at any time and at the sole discretion of the presiding faculty and/or staff member.

SECTION FOUR

AFTER-HOURS ACCESS

A. After-hours lab access may be arranged at the discretion of the Faculty of Business and IT. In the case that such after-hours access is granted, a lab monitor will be designated to manage the lab and students during the after-hours lab period. Students will not be permitted into the lab if the lab monitor is not present.
B. Access to the lab after-hours will be limited to students actively enrolled in a course which makes use of the lab on an ongoing basis. Guests and visitors are not permitted during after-hours lab time.

C. Students will be expected to sign in when they arrive at the after-hours lab session. They will be required to provide their name, student number, arrival time, and equipment they are working on when they sign in.

D. During after-hours lab access, the lab monitor is in charge. If he/she feels that a student is acting inappropriately, being abusive to the equipment or other students, or disregarding the lab rules, the student will be asked to leave, and may have their after-hours access privileges revoked.

E. After-hours lab access is limited to a first-come-first-served basis. If there is no available room in the lab, students may be asked to leave and come back later.

F. After-hours lab access is intended to supplement regularly scheduled lab time, not replace it. It is an opportunity for students to catch up on assignments and do independent work or research. Students are still expected to show up for regularly scheduled lab classes, and the availability of after-hours lab access will not be considered as grounds for assignment extensions or other academic provisions.

Section Five

Access to Communications

A. Due to the nature of the academic environment within the lab, absolutely no presumption of privacy shall be expected at any time. Though it is not general practice to globally monitor communications while in the lab, the administrator, staff, faculty and students occasionally use software which can either accidentally or purposefully identify personal communication across the network infrastructure.

Further, it should also be known that the lab administrator does routinely gather activity logs for most electronic activities or monitor isolated communications, e.g. websites accessed, software usage, and downloads, for the following purposes:

1. Bandwidth analysis;
2. Resource allocation;
3. Optimum technical management of information resources; and
4. Detecting patterns of use that indicate students are violating university policies or engaging in illegal activity.

B. Faculty, administrator and staff at UOIT reserve the right, at their sole discretion, to review all student's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other academic policies.

C. Due to the fact that privacy cannot be assumed in this lab environment, all lab users are advised to refrain from accessing any sensitive information while using the lab network.

SECTION SIX

RESTRICTED AREAS

A. Not all areas of the networking lab are accessible to all participants.
   a. There shall be **absolutely no unauthorized access** to the locked storage cabinet in the lab. The only individuals with authorized entry to this secured area are the administrator and management. Faculty members are requested to speak to the administrator if they require any items from this storage area.
   b. There shall be **absolutely no unauthorized access** to the electrical room in the lab at any time, by anyone. If access is required to the electrical room a request must be put in writing to the lab administrator who will arrange the access if it is deemed necessary.

SECTION SEVEN

SOFTWARE

A. To prevent computer viruses and other malicious software from being transmitted through the school's computer system, downloading of any unauthorized software to university computer assets is strictly prohibited. Any and all downloads to these devices must be authorized by faculty, staff or the administrator.

B. It should also be known that there is a zero tolerance policy in regards to pirated software. Anyone found to be downloading illegally pirated software can be subject to expulsion from the school, fines and/or federal prosecution.

HARDWARE

A. The costs associated with replacing and/or repairing any device contained within the networking lab is extensive. It is for this reason that all users of these devices must accept responsibility and understand that the user is responsible for the replacement costs associated with the item should the item break due to damage caused by negligence or any malicious means.

SECTION EIGHT

SECURITY/APPROPRIATE USE

A. At the beginning of each semester, student will be provided with credentials that grant them access to certain resources within the lab. Students will be held accountable for any actions taken using their credentials. For this reason, students should always take appropriate measures to ensure the confidentiality and integrity of their credentials at all times

B. Students must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by faculty, staff or the administrator, students are prohibited in engaging in, or attempting to engage in:

   a. Monitoring or intercepting the files or electronic communications of other students, staff, faculty or other third parties;
   b. Hacking or obtaining access to systems or accounts they are not authorized to use;
   c. Using other people's log-ins or passwords; and
   d. Breaching, testing or monitoring computer or network security measures.

C. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

D. Anyone obtaining electronic access to other software companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

SECTION NINE

PEER TO PEER NETWORKING

A. Unless explicitly stated by the presiding faculty, students are not to download any material using any method of peer-to-peer file sharing. This includes but is not limited to torrents, FTP, Gnutella, eDonkey or Newsbins. Anyone found abusing this policy shall have their computer identification logged and internet access revoked.

SECTION TEN

PARTICIPATION IN ONLINE FORUMS

A. The Faculty of Business and IT and UOIT recognize that participation in some forums might be important to the academic development of a student. For instance, a student may find the answer to a technical problem by consulting members of a news group devoted to the technical area. However, students should remember that any messages or information sent on campus premises to one or more individuals via an electronic network – for example, Internet mailing lists, bulletin boards and online services such as Facebook and Twitter – are statements identifiable and attributable to UOIT and the Faculty of Business and IT. In order to protect the reputation of the university, all communication must always remain professional and in compliance with the details outlined by this acceptable use policy document as well as with the UOIT code of conduct.

SECTION ELEVEN

FOOD AND DRINK

A. Food or drink is prohibited near the equipment in the racks and at any workstation or pod where lab equipment is present. It is expected that all faculty, staff and students will abide by the policy. If any damages occur due to negligence or by not directly following this policy, the individual responsible for causing the damage shall be held liable for the full replacement costs associated with the affected device(s).

B. While food or drink is not strictly prohibited in the lab (except as noted in Section 11. A), if at any time the presence of food or drink becomes an issue for any other person in the lab, the presiding faculty, staff, or administrator may request that the food or drink be taken out of the lab. Failure to comply with this request will result in a zero-tolerance policy being put in place regarding food and drink in the lab.

SECTION TWELVE

REMOTE ACCESS TO EQUIPMENT

A. Students may reserve equipment for remote access personal use outside of regularly scheduled classes by visiting http://networkinglab.uoit.ca/reservations.htm.

B. Remote access to equipment is only for students actively enrolled in a course which makes use of the lab on an ongoing basis. Credentials for the reservation site will be provided to eligible students at the beginning of each semester.

C. All credentials given to students should remain confidential. Students are responsible for any actions performed using their credentials, and should take appropriate precautions to ensure their credentials are not exposed.

D. Students are only permitted to have one active reservation at any time. An active reservation is considered to be any reservation in the database that has an end date and time that has not yet passed.

E. Reservations must be made a minimum of fifteen (15) minutes prior to the scheduled start time of that reservation.

F. Reservations cannot be made more than two (2) weeks in advance.

G. Reservations should only be made if the student is certain that they can access the equipment during the reserved time period. Reservation usage will be monitored for no-show reservations.

H. Remote access to the equipment is by no means guaranteed. Remote equipment access is intended to supplement regular in-class lab time, not replace it. Students are expected to attend their regularly scheduled in-class labs and complete their work there. Problems with remote access to equipment will not be considered as grounds for extensions on assignments or other academic provisions.

I. Remote access to the equipment is provided to the students as a privilege, and abuse of the system or failure to follow the policies outlined in this document may lead to the revocation of the student's remote access privileges.

SECTION THIRTEEN

VIOLATIONS AND COMPLIANCE

A. Any student, staff or faculty member who abuses the privilege of their access to this lab in violation of this policy will be subject to corrective action, including possible suspension, expulsion and/or criminal liability. The Faculty of Business and IT and UOIT have provided this lab so that it may be used as a valuable learning tool to aid in student development and will continue to support this lab in ways to protect their investments.

B. Should any articles contained within this Acceptable Use Policy document be difficult to understand or where it is possible for an item to be misinterpreted, it is the responsibility of the individual to contact the necessary authority in order to obtain clarification.

SECTION FOURTEEN

IMPORTANT ADMINISTRATIVE CONTACTS

Lab Technician
Mr. Josh Lowe
josh.lowe@uoit.ca
Office: UB3062
Phone: 905-721-8668 extension 3781

Planning and Budget Officer
Mrs. Belinda Bambrick
belinda.bambrick@uoit.ca
Office: UB4012
Phone: 905-721-8668 extension 2836