Index

1. Student Residences: Internet Use Policy (updated March, 2018) .......................................................... Page 03
2. IST: Use of Computer Facilities University Policy (updated January 25, 2005) ......................................... Page 05
3. IST: Responsible Computer Usage Policy (updated April 14, 2011) .......................................................... Page 07
4. IST: Software Use Policy (updated April 20, 2011) ....................................................................................... Page 09
5. IST: Using Software (updated April 20, 2011) ............................................................................................... Page 09
6. IST: Computationally Intensive Processes on CCU (updated April 14, 2011) ................................................. Page 12
7. IST: Standards for Wireless Networks (updated February 17, 2012) ............................................................. Page 12
1. Student Residences: Internet Use Policy  (Updated March, 2018)

DEVICES THAT USE WIFI

Many consumer “Internet of things” devices, like the Amazon Echo, require WiFi (no physical ethernet port) but don't support the UofM’s WiFi encryption standard (WPA2 Enterprise).

Some devices like the Apple TV will work on the UofM’s WiFi network but you are required to schedule a meeting with the Residence IT Administrator in order to get the required settings loaded onto the Apple TV. If you are thinking of purchasing a device that requires a WiFi connection, please contact the Residence IT Help Desk to determine if it will work on the UofM WiFi network. Call or Text: 204-226-8951

WIRELESS

All residence buildings contain pervasive IST provided Wi-Fi.

Residents are NOT permitted to set up a device in their room that broadcasts a Wi-Fi signal as it conflicts with IST Wi-Fi and causes poor or no Wi-Fi connections to other residents in that building.

Examples of devices that have the ability to broadcast a Wi-Fi signal are: Wi-Fi routers, wireless printers, mobile phone (when the hotspot feature is turned on), Shaw cable modem, MTS modem, gaming consoles, smart TV’s etc. You are permitted to subscribe to Shaw and MTS for an Internet connection, but you must turn off the Wi-Fi feature of the modem/ router. You may need to install a router in your suite to use a device like an Xbox, but you must turn off the Wi-Fi feature of your router. If you plug in a router improperly it can cause network issues that result in a loss of Internet access to others in the same building.

Please contact the Residence Support Desk for assistance in setting up routers. Any resident found to have a device broadcasting a Wi-Fi will be subject to disciplinary actions. Please see section 4.3 in the residence contract for more info on the disciplinary actions.

Please note that IST is a central IT department and is not a residence department. All of IST’s security, usage, and wireless policies can be found at: http://umanitoba.ca/computing/ist/staff/studentservices.html

COPYRIGHT INFRINGEMENT

Residents are not allowed to download or distribute files through the Internet that would violate a copyright law. This would include downloading and/or uploading any file or information that is copyrighted without proper consent. Examples of copyrighted and/or copy protected items are movies, television shows, songs, and documents. Residents are not allowed to setup a server or peer-to-peer (file sharing) connection to download or
share files that would violate copyright laws. Some examples of peer-to-peer sharing websites are PirateBay.se, isoHunt.com, and Torrentz. Examples of peer-to-peer computer software programs are uTorrent, BitTorrent, and Vuze. All activity on a residence Internet/Intranet connection is subject to provincial and federal laws.

**BANDWIDTH AND DOWNLOADING**

Bandwidth is how much data is being transferred through a network connection. Excessive downloading and/or uploading will slow down your connection speed and may affect the speed of the entire residence building. Bandwidth usage on the wired network will be monitored and disciplinary measures will be applied to any resident who uses excessive bandwidth.

If you consume a disproportionate percentage of the building’s wired bandwidth on a regular basis you will qualify for disciplinary measures. On the wired, in-building network, you are permitted 100GB/month of downloading and 100GB/month of uploading. If you require more bandwidth for academic purposes, please contact us via email at: it.residence@umanitoba.ca. If you require more bandwidth for non-academic purposes, you may sign up for a paid service from an alternate provider such as Shaw or MTS. Note that Shaw and MTS services are available in every residence building except for Arthur V. Mauro Residence, which only offers Shaw.

**WIRELESS, BANDWIDTH, AND COPYRIGHT DISCIPLINE**

Unauthorized wireless, copyright and bandwidth violations will be traced to a student and dealt with in the following manner:
- **1st offence**: Disciplinary write-up attached to residence account.
- **2nd offence**: $50.00 fine, indefinite loss of residence Internet service* and meeting with an RLC.
*Otherwise to be reviewed by and subject to the discretion of the Director of Student Residences and the Residence IT Administrator

**USER ID AND PASSWORD CONFIDENTIALITY**

All residence students will use their own or an assigned UMnet ID and password to log in and access the wired and wireless Internet provided in Student Residence buildings. This account information is intended only for the person it has been given to, and is not to be shared with anyone. If you give out UMNet ID and password to others, you could be held liable for their activities and actions on the Internet/network.

**VIRUS INFECTIONS AND HACKED COMPUTERS**

Computers that become infected by a virus or have been hacked often contribute to network and Internet congestion. They also cause infections and problems with other U of M computers. Residents who have a hacked or virus infected computer will have their
Internet connection suspended immediately upon detection. After the student’s Internet connection has been suspended, Student Residences will attempt to contact and inform the resident about the situation. The resident’s Internet connection will be restored when the Student Residences IT Administrator or IT Coordinator is confident that the resident’s computer no longer poses a risk to the U of M network, nor to the U of M faculty/staff/students.

DSL INTERNET

In University College Residence (UCR) and Mary Speechly Hall (MSH), you can request a DSL modem to be installed in your room in order to use a wired Internet connection. A wired Internet connection is generally faster, and more stable. Contact the Residence Internet Help Desk (204-226-8951) to have one brought to your room and installed. This equipment must be left in good, working condition upon your departure. You will be charged up to $300.00 for any loss and/or damage to the Internet connection equipment (including modem, cables, and the wall jack). In both Arthur V. Mauro (AVM) and Pembina Hall Residence (PHR) there is no DSL modem option. If you wish to use wired Internet in PHR or AVM, you must supply your own Ethernet cable.


<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>January 25, 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Date:</td>
<td>January 25, 2015</td>
</tr>
<tr>
<td>Approving Body:</td>
<td>Board of Governors</td>
</tr>
<tr>
<td>Authority:</td>
<td>President delegated to the Vice-President (Administration)</td>
</tr>
<tr>
<td>Implementation:</td>
<td>Vice-President (Administration) or Executive Director, Information Services Technology (IST)</td>
</tr>
<tr>
<td>Contact:</td>
<td>See List Below</td>
</tr>
</tbody>
</table>

This policy applies to:

(a) Board of Governors members
(b) Senate members
(c) Faculty/School Councils
(d) Students
(e) External Parties Sponsored users
(f) All Employee groups

1.0 Reason for Policy

1.1 Access to University networks and computing facilities is necessary for academic staff, support staff and students to do their work and accordingly
this policy are necessary to ensure the integrity and availability of these resources.

1.2 This policy defines responsibilities and obligations for all users of all computer systems and networks owned and operated by the University of Manitoba.
2.0 Policy Statement

The use of University computer systems and networks imposes certain responsibilities and obligations on users of the facilities. Such use is granted by the University of Manitoba subject to compliance with University policies and procedures as well as with local, provincial and federal laws.

2.1 Responsibilities

2.1.1 Information Services and Technology (IST) Responsibilities:

To provide assurance of consistent equitable service, IST is responsible for:

(a) The safety, integrity and security of University owned and operated systems and networks;

(b) Coordinating the investigation of alleged unauthorized use of University computer systems and network under the authority of the Vice President (Administration);

(c) Providing current security information and anti-virus updates to the University community and where possible installing these updates on machines connected to the campus network automatically via the network; and

(d) Periodically informing and reminding the University community of current procedures to be followed to ensure the integrity of University computing and networking facilities.

2.1.2 Users Responsibilities

To provide equitable access and employment of University owned and operated systems and networks, users have a responsibility to:

(a) Use resources only for authorized purposes as defined by the University;

(b) Protect their userid (is the access word assigned to each user of the University systems by IST) password and system from unauthorized use. Users are responsible for all activities on their userid that originate from their system with their knowledge.

(c) Access only information that is their own, that is publicly available or to which they have been explicitly granted access by the owner of the information;

(d) Comply with local, provincial and federal laws;

(e) Comply with system security mechanisms;

(f) Use only legally licensed versions of copyrighted software or copies of documents and media in compliance with terms and conditions of any vendor licensing agreement, copyright or sale terms and conditions;

(g) Comply with all University policies regarding intellectual property;

(h) Ensure that systems under their control have current security updates and anti-virus software installed regardless of ownership of the equipment;

(i) Engage in ethical workplace behaviors reflecting:

(ii) Acceptable language of discourse;

(iii) Restraint in the consumption of shared resources by refraining from monopolizing systems and/or overloading networks with...
excessive data or activity, degrading services, or wasting any other related resource;
(iv) Respect for intellectual property and ownership of data; and
(v) Respect for individual rights to privacy and freedom from harassment in such forms as intimidating, disrespectful or obscene messages, jokes or images.

3.0 Accountability

3.1 University Secretary for initiating a formal review of this Policy and Secondary Documents.
3.2 Responsibility for investigating alleged unauthorized use of University computer systems and network lies with IST under the authority of the Vice President (Administration).

4.0 Secondary Documents

4.1 The Vice-President (Administration), in consultation with the President, may approve Procedures which are secondary to and comply with this Policy.

5.0 Review

5.1 Formal Policy reviews will be conducted every ten (10) years. The next scheduled review date for this Policy is January 25, 2015.
5.2 In the interim, this Policy may be revised or rescinded if:
   (a) the Approving Body deems necessary; or
   (b) the relevant Bylaw, Regulations or Policy is revised or rescinded.
5.3 If this Policy is revised or rescinded, all Secondary Documents will be reviewed as soon as reasonably possible in order to ensure that they:
   (a) comply with the revised Policy; or
   (b) are in turn rescinded.

6.0 Effect on Previous Statements

6.1 This Policy supersedes the following:
   (a) all previous Board/Senate Policies, Procedures, and resolutions on the subject matter herein;
   (b) all previous Administration Policies, Procedures, and directives on the subject matter contained herein; and
   (c) Policy 238: Use of Computer Facilities.

3. Responsible Computer Usage of Labs and Accounts
(Updated April 14, 2011)
Student computer access other than for specifically assigned coursework is a privilege, not a right. It may be revoked for questionable use or for administrative or other reasons.

Responsible Use of Accounts and Lab Facilities

When you claim your computer account or userid you agree to be responsible for all actions performed using it. The claimed text you agreed to when setting up or renewing your account is available online.

Registered students are entitled to use the computing and networking facilities provided for all students by IST’s Academic Computing & Networking department.

In addition to this document, the University’s Use of Computer Facilities policy governs all UofM computer users.

Misuse of the account or of the facilities may lead to loss of privileges and/or disciplinary and/or legal action by the University.

Please report any misuse or abusive behavior using accounts or facilities to: abuse@umanitoba.ca

Access privileges of an account may be suspended during an investigation.

Labs Usage Guidelines

- PASSWORDS: Keep your password(s) private and pick a secure one. It should be 6 to 8 characters long, a mixture of numbers and letters, and not a name or dictionary word.
- COURTESEY: Maintain quiet in the Academic Computing Labs. Do not occupy a computer to play games or for Internet Chat. During busy periods, keep your sessions as short as possible, keep your personal use for non-busy times, do not use for personal_. Bring headphones for your audio use while working and keep volume levels low.
- ACADEMIC USE PRIORITY: Academic use takes precedence in the labs. If your use is personal or recreational, relinquish your computer if others are waiting. Restrict personal use to outside peak periods (approximately 10 a.m. to 4 p.m. weekdays).
- BASIC LAB RULES: Food and beverages are not permitted in the labs. Please use the garbage bins and help keep the area clean.
- PERSONAL COMPUTING EQUIPMENT: No user-supplied equipment, other than USB storage devices and audio headphones, may be connected to ACN lab computers. Lab computers must not be disconnected from the network. User laptops may be connected only to the netports made available for this purpose. Personal equipment may be confiscated by Campus Security pending investigation of its use.
- REPORT PROBLEMS: Help protect your facilities. Please report misuse or equipment malfunctions to the ACN Trouble Desk, 474-8484, noting the time, location, and workstation.

Report emergency situations to Campus Security: Dial 555.

- PRINTING: Learn how to use the self-service dot-matrix lab printers. Printers are checked daily by staff but you may need to replace paper or ribbon. Separate others’ output carefully when you remove yours from a printer.
- UofM IDENTIFICATION: Use of the labs is for University staff and students. Please be prepared to show your UofM id on request.
Accounts suspended for cause will be subject to a $25 reactivation fee.

Theft, vandalism, or other serious abuse of the Academic Computer Labs may lead to the closure of the lab.

4. IST: Software Use Policy (Updated April 20, 2011)

All U of M students are required to adhere to the terms of the software contracts between the University and the various software vendors, and to exercise due diligence in ensuring that we do not support in any way the unauthorized use or distribution of software.

Software licensed by IST and made available on file servers is for use in IST computer labs only, unless otherwise documented. In those cases where a container administrator is granted shared access to software installed by IST, that container administrator is responsible for confirming that the limitations of their software licenses are respected.

For information on the license terms of software administered by Information Services and Technology, please see the Software Team’s web page at: http://umanitoba.ca/computing/ist/software/ or contact Client Services through the Help and Solutions Centre at: 204-474-8600 or support@umanitoba.ca.

For the Information Services and Technology statement on Ethical and Legal use of Software, please see: http://umanitoba.ca/computing/ist/guidelines/

5. IST: Using Software (Updated April 20, 2011)

A Guide to the Ethical and Legal Use of Software for Members of the U of Manitoba

SOFTWARE enables us to accomplish many different tasks with computers. Unfortunately, in order to get their work done quickly and conveniently, some people justify making and using unauthorized copies of software. They may not understand the implications of their actions or the restrictions of the Canadian Copyright Act, as amended on June, 1988 by Bill C-60.

HERE ARE SOME RELEVANT FACTS:

- UNAUTHORIZED copying of software is illegal. Copyright law protects software authors and publishers, just as patent law protects inventors.
- UNAUTHORIZED copying of software by individuals can harm the entire university community. If unauthorized copying proliferates on campus, the University may incur a legal liability. Also, the University may find it more difficult to negotiate agreements that would make some software more widely and less expensively available to members of the university community.
- UNAUTHORIZED copying of software can deprive developers of a fair return for their work, increase prices, reduce the level of future support and enhancement, and inhibit the development of new software products.

RESPECT for intellectual work and property of others has traditionally been essential to the mission of colleges and universities. As members of the university community, we value the free exchange of ideas. Just as we do not tolerate plagiarism, we do not condone the unauthorized copying of software, including programs, documentation, applications, data bases, and code.
THEREFORE, we offer the following statement of principle about intellectual property and the legal and ethical use of software. This “code” was developed by the EDUCOM Software Initiative.

SOFTWARE AND INTELLECTUAL RIGHTS

Respect for intellectual labour and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the university community.

QUESTIONS YOU MAY HAVE ABOUT USING SOFTWARE

• What do I need to know about software and the Canadian Copyright Act?

  Unless it has been placed in the public domain, software is protected by copyright law, whether it bears a copyright notice or not. The owner of a copyright holds exclusive right to the reproduction and distribution of his or her work. Therefore, it is illegal to duplicate or distribute software or its documentation without permission of the copyright owner. If you purchased your copy, however, you may be able to make a backup for your own use in case the original is destroyed or fails to work (check your license agreement to be sure).

• Can I lend software I have purchased?

  If your software came with a clearly visible license agreement, or if you signed a registration card, READ THE LICENSE CAREFULLY before you use the software. Some licenses may restrict use to a specific computer. Copyright law does not permit you to run your software on two or more computers simultaneously unless the license agreement specifically allows it. It may, however, be legal to lend your software to a friend temporarily as long as you do not keep a copy.

• Can I install software I have purchased on a Local Area Network (LAN)?

  Software generally must be licensed explicitly for a LAN. Do not assume that it is legal to install it on a LAN just because you have purchased one copy legally. A LAN implies multiple users. A software license may have to be acquired for each workstation on the LAN.

• If software is not copy-protected, do I have the right to copy it?

  Lack of copy-protection does NOT constitute permission to copy software in order to share or sell it. “Non-copy-protected” software enables you to protect your investment by making a backup copy. In offering non-copy-protected software to you, the developer or publisher has demonstrated significant trust in your integrity.

• May I copy software that is available through facilities on campus, so that I can use it more conveniently in my own work area?

  Maybe. Software acquired by colleges and universities is usually licensed. The licenses restrict how and where the software may be legally used by members of the community. This applies to software installed on hard disks in microcomputer clusters, software distributed on disks by a campus lending library, and software available on campus mainframe or network. Some institutional licenses permit copying for
certain purposes. Consult Information Services and Technology if you are unsure about the use of a particular software product.

• Isn’t it legally “fair dealing” to copy software if the purpose in sharing it is purely educational?

   No.
   It is illegal for a faculty member or student to copy software for distribution among the members of a class, without permission of the author or publisher.

• What can happen to me if I am caught with unauthorized software?

   The University of Manitoba does not tolerate software piracy. Anyone (staff or student) found to be making or using illegal copies of computer software will be subject to disciplinary or possible legal action. Remember that your copyright violation exposes the University to lawsuits and damage claims from the vendor.

ALTERNATIVES TO EXPLORE

Software can be expensive. You may think that you cannot afford to purchase certain programs that you need. But there are legal alternatives to unauthorized copying.

SITE LICENSED AND BULK-PURCHASED SOFTWARE

The University has negotiated agreements that make software available either to use or to purchase at special prices. Consult Information Services and Technology for information. Software available through institutional site licenses or bulk purchases is subject to copyright and license restrictions, and you may not make or distribute copies without authorization.

SHAREWARE

Shareware, or “user-supported” software, is copyrighted software that the developer encourages you to copy and distribute to others. This permission is explicitly stated in the documentation or displayed on the computer screen. The developer of shareware generally asks for a small donation or registration fee if you like the software and plan to use it. By registering, you may receive further documentation, updates, and enhancements. You are also supporting future software development. The University urges you to respect the shareware agreement.

AUDIO AND VIDEO FILES

Music, movies, and television programs are typically copyrighted. It is illegal to distribute files that are copyrighted. If you are unsure if a particular song, album, DVD, movie, or television program is copyrighted it is a best practice to contact the company that is distributing the item in question.

PUBLIC DOMAIN SOFTWARE

Sometimes authors dedicate their software to the public domain, which means that the software is not subject to any copyright restrictions. It can be copied and shared freely.

Software without copyright notice is often, but not necessarily, in the public domain. Before you copy or distribute software that is not explicitly in the public domain, check with Information Services and Technology.

A FINAL NOTE

Restrictions on the use of software are far from uniform. You should check carefully each piece of software and
the accompanying documentation yourself. In general, you do not have the right to:

1. receive and use unauthorized copies of software, or
2. make unauthorized copies of software for yourself or others.

---

6. Computationally Intensive Processes on CCU
(UPDATED APRIL 14, 2011)

The CCU system is a shared resource used by thousands of students, faculty, and staff of The University of Manitoba. To help facilitate that sharing, Computer and Network Services has developed a policy governing computationally intensive processes.

The policy is intended to allow computing resources, particularly cpu time and virtual memory, to be available for use by all users while still providing the needed computing power for the University community’s academic and research requirements.

On the general CCU system (login servers and workstations), users are asked to run no more than three such jobs at any one time, and no more than one process on any one CCU computer.

Exempt from the policy are:

- “compute” designated computers and
- computers operated as part of CCU on behalf of other University units.

(These exceptions can be identified from the list provided by the machine’s command.)

Processes in excess of the limitations may be killed without notice. Processes within the limit but seriously affecting system function will be killed. CNS may suspend userids responsible for repeated incidents.

Users with research or academic computing requirements in excess of the resources available under this policy should contact Computer and Network Services of Information Services and Technology.

---

7. Standards for Wireless Networks
(UPDATED FEBRUARY 17, 2012)

The use of wireless data networks at the University is growing as technologies improve and prices drop. However, those units planning installation of wireless networking technology should be aware of the following issues;

1. Wireless networks are not a complete replacement for wired switched networks.

2. Unlike wired switched networks, wireless networks are a shared medium and as a result performance decreases as more clients use the same central resource. Performance also decreases as the distance to the nearest base station increases. In most cases performance will not equal that of a wired switched network.
3. The wireless transmission of data from the desk top or laptop to the nearest base station connected to the building backbone network is, by definition, insecure since it uses radio and may be intercepted unless precautions are taken.

Installation of a wireless network requires careful physical planning and a site survey to optimize placement of base stations in any particular area in order to maximize performance. It is also important to estimate how many base stations will be required for current projected usage and to allow for growth. Finally, current wireless networks operate in the same frequency range as other consumer and scientific devices, and are therefore susceptible to interference. A site survey will help identify potential sources of problems.

Wireless networks out of the box do not have any security features turned on. All wireless network products do support some kind of encryption using a standard called WEP. However, this is weak security and should only be used in situations where security is not a major issue. Details on current security standards are available from IST.

Any use of wireless networks for secure applications in administration, teaching or research will need further facilities to bring the level of security up to that of wired switched networks. This will require additions to the central backbone network equipment to ensure that the installation meets required security levels.

Any units planning installation of wireless networks are asked to contact IST for assistance in planning and in ensuring proper security measures are taken to protect the integrity of University data and systems. IST will be pleased to assist in planning for proper security measures.

---


**Purpose:**
These procedures and guidelines are to assist the deployment of wireless networking technology on the University of Manitoba campus. It is intended as a follow-up to the Information Services and Technology (IST) Standards for Wireless Networks http://umanitoba.ca/computing/ist/guidelines/wireless_standards.html

Effective management of this technology is vital to the reliability and security of the wireless network at this University. The wireless network is not intended as a replacement for wired switched networks. It does not have the same level of security, throughput or support and it is not intended for secure applications or bandwidth intensive applications in administration, teaching or research.

The objectives are to ensure interoperability, reliability and security to the wireless network service while protecting the University’s information resources and electronic communications. The inherent nature of the wireless technology requires cooperation and coordination between departments and faculties to facilitate deployment in different buildings and prevent possible radio frequency spectrum interference or network impairments.

**Scope:**
These procedures and guidelines apply to all existing and future installations of wireless networking technologies by faculty, staff and students in the 2.4 GHz and 5 GHz radio frequency spectrums on the University of Manitoba campus, both inside buildings and for outdoor areas.

All University of Manitoba’s information technology policies and procedures: http://umanitoba.ca/admin/governance/governing_documents/community/index.html apply to the use of wireless networks at the University of Manitoba as do all other applicable University of Manitoba policies, guidelines and procedures and all federal, provincial and civic laws.

**Background:**
The Information Services and Technology (IST) department is responsible for the design, installation, support and maintenance of the campus network infrastructure up to and including the wired communications outlets. It extends to include the wireless access points and the authentication and encryption methods used to secure wireless access. Wireless access points are considered to be part of the campus network.

The proliferation of faculty required or personally owned laptops which have built in wireless capability, has caused a rapid demand for wireless networks. Students, faculty and staff want to use their laptops in libraries, lecture theatres, classrooms, study areas and outdoor areas. However, wireless technology is not intended to replace network wiring but rather to complement it. A wireless network can provide network connectivity in large open areas or where restrictions such as asbestos or historical buildings would limit wired access.

The University of Manitoba wireless network standard and central management of the 2.4 GHz and 5 GHz radio frequency spectrum are necessary to protect valuable information resources and ensure the maximum amount of interoperability. The Information Services and Technology department conducted a wireless Request for Information (RFI) in the fall of 2003. The technical requirements for wireless networking on Campus can be found in the document Wireless Networking Hardware and Technical Requirements http://umanitoba.ca/computing/ist/guidelines/media/wireless-technical.pdf

**Wireless Procedures:**

* Compliance with the following procedures is required. IST will not be actively searching for non-compliant wireless networks except when investigating network problems. IST does expect compliance with these procedures and will disconnect any non-compliant devices from the University of Manitoba wired or wireless networks.
  * The University of Manitoba’s Information Services and Technology (IST) department will provide exclusive management and radio frequency channel allocation for new wireless networks which connect to the University of Manitoba wireless data network.
  * The University of Manitoba’s Information Services and Technology (IST) department will provide the design, specification, installation, operation, and maintenance for new wireless networks connected to the University of Manitoba wireless network.
  * IP is the only protocol supported.
  * All wireless networks must be compatible with existing University of Manitoba technology for authentication and encryption.
  * All wireless network access to the University’s campus data network must authenticate with a valid “UMnetID” account on the IST radius server. Restricted network access will be provided until the user has authenticated.
  * Wireless networks owned by other University of Manitoba units or individual faculty, staff or students are permitted provided they are not connected to the University’s campus wired networks and they are approved by IST as meeting the guidelines covered in this document and providing they do not cause interference with the University of Manitoba/IST wireless networks.
  * A site survey and an IST registration for the use of the radio frequency spectrum will be required prior to the installation of any wireless networking equipment onto the University of Manitoba wireless network. In the case of radio interference, IST will work with the owners of the devices to eliminate the interference to the wireless network. In the event that a solution cannot be found, the disruptive devices must be removed.
  * In the event that a wireless network poses a security threat, measures will be taken to protect the integrity of University data and systems.
  * The demarcation point for the network service will be the access point. The IST networking group will be responsible maintenance and support of the IST supported access points and the network connecting them to the campus data network.
  * IST is not responsible for the purchase, installation, configuration and support of the wireless client cards in computers.
  * IST may implement newer security and encryption technologies and standards as they evolve and are ratified.
  * All IP addresses for the University of Manitoba’s wireless network will be provided through the DHCP servers administered by IST.
  * The connection of servers to the University of Manitoba’s wireless network will not be permitted.
  * All installations must be in compliance with the health, safety, building and fire codes.
  * To the best of its abilities IST will provide a secure wireless network meeting currently acceptable practices to prevent intrusion into the wireless network.
* IST does not assume any responsibility for the intrusion into the wireless network, nor the security of the communications on the wireless network.
* Any intruders or otherwise abusive users will be investigated the same as on the wired network.

**Ad-Hoc or Peer-to-Peer Networks:**
Ad-hoc or peer-to-peer networks between laptops, PDAs, access points and other devices are not permitted. These networks can operate on the same channels used by the University of Manitoba wireless network. However ad hoc networks can open your stations to be directly attacked and used as conduits to the network.

**Responsibility:**
The accountability for the adherence to these procedures and guidelines as well as other University of Manitoba information technology policies, which are not maintained by IST, is the responsibility of the dean, director or department head.
This responsibility may be delegated (Service Level Agreement) to IST for the installation, support and maintenance of the wireless network operating in the aforementioned radio spectrum.

**Radio Signal Interference:**
The wireless network operates in the unlicensed 2.4 GHz or 5 GHz radio frequency spectrum and conforms to the IEEE standards. The use of other devices including wireless networking devices, cordless phones, microwave ovens etc., in these same spectrums may disrupt the University of Manitoba’s wireless network. If interference occurs between other devices and the University of Manitoba’s wireless network, the wireless network will have priority. IST will provide assistance in eliminating the interference. Where a recommended solution to interference cannot be provided the wireless network will have priority.

These procedures apply in principal to wireless WAN networks as well.

Please contact Doug Dennis at 474-8290 if you wish to discuss this or if you have any questions.