1. **Course:** CPSC 525: Principles of Computer Security  
   CPSC 625: Principles of Computer Security  

   **Lecture Sections:**  
   L01, MWF 14:00-14:50, Robin Gonzalez, ICT 555, 403-831-6206, gonzaire@ucalgary.ca  
   Office Hours: By Appointment  

   **Course Website:** [http://pages.cpsc.ucalgary.ca/~gonzaire/CPSC525](http://pages.cpsc.ucalgary.ca/~gonzaire/CPSC525)  

   **Computer Science Department Office, ICT 602, 220-6015, cpsc@cpsc.ucalgary.ca**

2. **Prerequisites:**  
   CPSC 525: CPSC 457 and either MATH 271 or 273  
   CPSC 625: Consent of the Department  
   ([http://www.ucalgary.ca/pubs/calendar/current/computer-science.html#3620](http://www.ucalgary.ca/pubs/calendar/current/computer-science.html#3620))

3. **Grading:** The University policy on grading and related matters is described in sections F.1 and F.2 of the online University Calendar. In determining the overall grade in the course the following weights will be used:  
   
<table>
<thead>
<tr>
<th>Course</th>
<th>Weight</th>
</tr>
</thead>
</table>
   | CPSC 525 | Assignments 75%  
             | Midterm Exam 15%  
             | Final Exam 10%  
   | CPSC 625 | Research Project 100% |

   (in-Class Friday March 4th, 2016)  

   This course **will not** have a Registrar’s Scheduled Final Exam.  

4. **Missed Components of Term Work:** The regulations of the Faculty of Science pertaining to this matter are found in the Faculty of Science area of the Calendar. Section 3.6. It is the student’s responsibility to familiarize themselves with these regulations. See also Section E.6 of the University calendar.

5. **Scheduled Out-of-Class Activities:** REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME ACTIVITY. If you have a clash with this out-of-class activity, please inform your instructor as soon as possible so that alternative assignments can be arranged.

6. **Course Materials:**  
   Computer Security (3rd Edition), Dieter Gollman, *Hamburg University of Technology*  

   **Online Course Components:** None.

7. **Examination Policy:** None. Students should also read the Calendar, Section G, on examinations.

8. **Approved Mandatory and Optional Course Supplemental Fees:** None.

9. **Writing across the Curriculum Statement:** In this course, the quality of the student’s writing in the weighted components of the course will be a factor in the evaluation of these components. See also Section E.2 of the University Calendar.

10. **Human Studies Statement:** Students will be expected to participate as subjects or participants in projects. See also Section E.5 of the University Calendar.
11. OTHER IMPORTANT INFORMATION FOR STUDENTS:

a) **Misconduct:** Academic misconduct (cheating, plagiarism, or any other form) is a very serious offense that will be dealt with rigorously in all cases. A single offence may lead to disciplinary probation or suspension or expulsion. The Faculty of Science follows a zero tolerance policy regarding dishonesty. Please read the sections of the University Calendar under Section K, Student Misconduct to inform yourself of definitions, processes and penalties.

b) **Assembly Points:** In case of emergency during class time, be sure to FAMILIARIZE YOURSELF with the information on assembly points which can be found in each classroom and building.

c) **Student Accommodations:** Students needing an Accommodation because of a Disability or medical condition should contact Student Accessibility Services in accordance with the Procedure for Accommodations for Students with Disabilities available at  
http://www.ucalgary.ca/policies/files/policies/procedure-for-accommodations-for-students-with.disabilities_0.pdf. Students needing an Accommodation in relation to their coursework or to fulfill requirements for a graduate degree, based on a Protected Ground other than Disability, should communicate this need, preferably in writing, to the Associate Head of Computer Science. Dr. Ben Stephenson, by email bdstephe@ucalgary.ca or phone 403-220-6781.

d) **Safewalk:** Campus Security will escort individuals day or night (http://www.ucalgary.ca/security/safewalk/). Call 403-220-5333 for assistance. Use any campus phone, emergency phone or the yellow phones located at most parking lot pay booths.

e) **Freedom of Information and Privacy:** This course is conducted in accordance with the Freedom of Information and Protection of Privacy Act (FOIPP). As one consequence, students should identify themselves on all written work by placing their name on the front page and their ID number on each subsequent page. For more information see also http://www.ucalgary.ca/secretariat/privacy

f) **Student Union Information:** VP Academic (403) 220-3911 suvpaca@ucalgary.ca SU Faculty Rep (403) 220-3913 science1@su.ucalgary.ca, science2@su.ucalgary.ca and science3@su.ucalgary.ca. Student Ombuds Office: (403) 220-6420 ombuds@ucalgary.ca, http://ucalgary.ca/provost/students/ombuds

g) **Internet and Electronic Device Information:** You can assume that in all classes that you attend your cell phone should be turned off unless instructed otherwise. All communications with other individuals via laptop computers, cell phones or other devices connectable to the internet in not allowed during class time unless specifically permitted by the instructor. If you violate this policy you may be asked to leave the classroom. Repeated abuse may result in a charge of misconduct.

h) **U.S.R.I.:** At the University of Calgary feedback provided by students through the Universal Student ratings of Instruction (USRI) survey provides valuable information to help with evaluating instruction, enhancing learning and teaching, and selecting courses (www.ucalgary.ca/usri). Your responses make a difference – please participate in USRI surveys.

Department Approval__________________________________________Date__________________________

Associate Dean’s Approval for Alternate final examination arrangements:__________________________Date:___________________________

*A signed copy of this document is kept on file in the Computer Science Main Office ICT 602*
<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>95-100</td>
</tr>
<tr>
<td>A</td>
<td>90-94</td>
</tr>
<tr>
<td>A-</td>
<td>85-89</td>
</tr>
<tr>
<td>B+</td>
<td>80-84</td>
</tr>
<tr>
<td>B</td>
<td>75-79</td>
</tr>
<tr>
<td>B-</td>
<td>70-74</td>
</tr>
<tr>
<td>C+</td>
<td>65-69</td>
</tr>
<tr>
<td>C</td>
<td>60-64</td>
</tr>
<tr>
<td>C-</td>
<td>55-59</td>
</tr>
<tr>
<td>D</td>
<td>50-54</td>
</tr>
<tr>
<td>F</td>
<td>&lt;50</td>
</tr>
</tbody>
</table>
Tentative Topics Covered:

- Review of networking concepts and basic protocols, OSI reference model, IEEE 802.3, UDP, TCP, IP, ICMP, ARP, DNS, SMTP, HTTP
- Internet routing, forwarding, BGP, OSPF
- Basic cryptographic concepts, constructs, and terminology
  - Block ciphers
  - Stream ciphers
  - Cipher modes (ECB, CBC, OFB, CFB, CTR)
- Secret key / symmetric key cryptography
- Public key / asymmetric key cryptography
- Hash algorithms and message authentication codes (HMAC, MD)
  - DES, 3DES, AES
  - MD2, MD4, MD5, SHA-1, SHA-2
- Review of Mathematical concepts underpinning public key cryptography
  - RSA
  - Diffie-Hellman
- Authentication Protocols, Attacks and Defenses
- Secure Protocol Design, Concepts and Implementations
- Password authentication schemes, strong password protocols
- Security handshakes and protocol primitives
  - SSH
- Social engineering, spam, phishing, complex attacks
- IPsec
- SSL/TLS
- Kerberos v4 and v5
- Certificates and PKI
- Network Defense: Attacks and Countermeasures
- Packet Crafting
- Sniffing
- Intrusion Detection
- DoS, DDoS
- Legal and ethical issues involved in network monitoring
- Secure email, PGP
- Firewalls, tunnels
- Web Security
- Folklore and security protocol design advice