RRC POLYTECH Program and Course Catalogue

FULL-TIME | WINNIPEG LOCATIONS

Information Security

Overview

- Two year post-graduate diploma
- Fall entry date
- Exchange District Campus (formerly Princess Street Campus), Winnipeg
- Work Integrated Learning experience
- International applicants please visit Academic Program, Dates and Fees for a listing of programs for international students, current availability and online application instructions

Description
The Information Security industry is facing an ever-changing security landscape creating a need to safeguard data integrity, digital assets, and systems.

In this post-grad program, you will have the opportunity to develop skills to emphasize a security-centric organizational culture, secure architecture and design, governance, risk management, and compliance principles, and advanced cybersecurity threat mitigation techniques. You will apply the latest security measures and technologies to meet evolving threats and business needs while aligning security strategies with organizational goals through collaboration with stakeholders. The program will provide the opportunity to gain real-world experience through practical application of advanced information security frameworks and methodologies in compliance with regulatory requirements.

Admission Requirements

Your Academic History
If your academic history includes any of the following, please visit My Education for important information: post-secondary studies at an institution other than Red River College Polytechnic; Modified (M), English as an Additional Language (E), or GED high school courses; or home schooling; international secondary (high school) studies.

The college requires transcripts verifying your complete academic history including any public or private high school, college, university, or technical institute you have attended.

Please check the Program Overview page, to see if this program is for Manitoba residents only.

DOCUMENT SUBMISSION

Upload Through Your Future Student Account

- Scan your document(s) and save the file. Ensure you keep your original documents as the College may request to see them at any time.
- Go to apply.rrc.ca and log in.
- Click on your application, then Supplemental Items & Documents.

If you do not have a Future Student Account or require assistance, please contact our Student Service Centre at 204-632-2327.

Internationally Educated Applicants - visit www.rrc.ca/credentials for credential assessment information.

Submission of required documentation indicating proof of completion of admission requirements is due within 15 days of applying unless otherwise noted in the program's admission requirements.

However, if you apply within 6 weeks of the program start date, admission requirements are due within 5 days of applying.

Regular Admission Requirements

1. Post-Secondary Education
   - Submit proof of graduation from or enrolment in a certificate, diploma or degree related to Information Technology from a recognized post-secondary institution including:
     - Red River College Polytechnic's Information Security Advanced Diploma
     - Red River College Polytechnic's Application Development and Delivery Program
     - Red River College Polytechic's IT Operations Diploma Prorgram
     - Red River College Polytechnic's Data Science and Machine Learning Diploma Program
     - Red River College Polytechnic's Cybersecurity Diploma Program
     - Manitoba Institute of Trades and Technology Network and Systems Administrator Program
     - Computer Science Degree
     - Computer Engineering Degree
   - If you provide proof of enrolment at time of application, your official final grades indicating successful completion must be submitted by July 15 for fall enrolment or by the deadline specified in your admission letter.
   - Post-secondary transcripts must have been issued within 6 months prior to your application date, and submitted in a sealed envelope directly from the post-secondary institution.
   - If you are required to complete an English language assessment, do not submit your transcripts until requested to do so. See English Language Requirements (ELRs) for more information.

     or

2. Work Experience
   - Submit a Personal Resume to demonstrate relevant information technology or information security work experience, minimum 1 year. As this is a post graduate program the college recommends 2-3 years' work experience.

3. English Language Requirements (ELRs)
   - Answer this question to determine if you meet this program's ELRs:
     Have I successfully completed 3 years of full-time high school (secondary) education in Canada, the United States, or an ELR exempt country where English was the language of instruction?
     - If YES, you meet English language requirements. Apply and then submit your transcripts* for review
       or
     - If NO, submit proof of meeting an ELRs option. If you choose the English language assessment option, review this program's approved assessments and required levels.
       or

- If you completed all of your education in Canada, the United States, or an ELR exempt country in English but you did not graduate high school, submit your transcripts* for review.

- * If your transcripts are from the USA or an ELR exempt country, we will assess an International Credentials Assessment Fee to be paid before your transcripts will be reviewed.

Mature Student Admission Requirements
If you are 19 years of age or older on or before September 30 in your year of registration, have been out of high school for a minimum of one year, and you do not meet the regular admission requirements, you may apply under the Mature Student admission requirements.

1. Work Experience
   - Post Secondary education is not required, but you must submit a Personal Resume to demonstrate proof of having completed a minimum of 1 year of paid employment in an information technology related role.
     and
2. Meet Regular Admission Requirement 3

CybersecurityCybersecurity

English Language Assessments

⚠ The College reserves the right to modify this information without notice or prejudice.
ASSESSMENT RESULTS MUST BE DATED NO MORE THAN TWO YEARS PRIOR TO YOUR APPLICATION DATE!

Approved English Language Assessments

English Language Assessment	Minimum Scores for Certificates, Diplomas and Advanced Diplomas, and Post Graduate Certificates, Post-graduate Diplomas	Minimum Scores for Bachelor Degrees and Creative Communication
CAEL Online or In-Person	Overall band score of 60	Overall band score of 70 and Writing of 60
IELTS Academic Level	Overall 6.0 and No band below 5.5	Overall 6.5 and No band below 6.0
Password Skills	Overall 6.0 and No band below 5.5	Overall 6.5 and No band below 6.0
LINC Certificate	7	8
Duolingo Language Test	115 and above+ with a min. of 95 in each section	125 and above with a min. of 100 in each section
New English for Academic and Professional Purposes	Successful completion of the program 5 (min 70%)	Successful completion of the program 5 (min 70%)
PTE	54 overall Min 50 in each skill	60 overall Min 55 in each skill band
TOEFL-ibt Academic Level	80 (20L, 20S, 19R, 21W)	90 (22L, 22S, 22R, 24W)
Academic English Program for University and College Entrance Program (AEPUCE)	Successful Completion	Successful Completion
CELBAN	N/A	N/A

Locations, Dates and Fees

Next Estimated Term 1 Start Date (subject to change)

Location	Start Date	
Manitou a bi Bii daziigae	Aug 25, 2025	Apply Now

Costs (estimates only; subject to change)

Program/Student Fees	
Year 1	$10,684.00
Year 2	$9,496.00
Books and Supplies	
Year 1	$1,850.00[1]
Program/Student Fees (International)	
Year 1	$14,494.00
Year 2	$12,946.00

[1] Includes an estimate of $1600 for the purchase of a laptop and an estimate of $250 for the purchase of software licenses

Students may apply for financial assistance through the Manitoba Student Aid program. For general information on applying please call 204-945-6321 or 1-800-204-1685, or visit their website at www.manitobastudentaid.ca, which also includes an online application. For detailed information, please visit one of the RRC Polytech Student Service Centres or call 204-632-2327. Applicants requiring financial assistance should complete their student loan applications well in advance of the class start date.

Courses and Descriptions

Year 1	
Term 1	**Credit Hours**
COMP-2046 IT Security Risk Management	6
COMP-2048 Security Architecture and Design	6
COMP-2049 Security Service Delivery	6
Term 2	**Credit Hours**
COMP-2055 Security Program Management	6
COMP-2056 Vulnerability Management and Ethical Hacking	6
COMP-2057 Security Resiliency Planning	3
Year 2	
Term 3	**Credit Hours**
COMP-2058 Advanced Security Infrastructure	6
COMP-2059 Managing Security Operations	

	6
COMP-2060 Digital Forensics and Incident Response	6
Term 4Credit Hours	
COMP-2061 Security and AI	3
COMP-2067 Governance, Audit and Compliance	6
INDP-3004 Industry Project	2

COMP-2046
IT Security Risk Management

Students will be provided with an understanding of the importance and purpose of security risk management, and how it is governed by various internationally recognized frameworks. Students will gain practical experience in performing Business Impact and Risk Assessments as well as IT Risk Audits. Students will acquire a practical understanding of how to establish secure baselines and utilize security controls to manage risks effectively. Emphasis will be placed on the legal, regulatory, and compliance dimensions of risk management and the necessity of cultivating a risk-aware culture within culturally varied organizations.

COMP-2048
Security Architecture and Design

In the ever-changing landscape of cyber threats, it is important to create secure, holistic architectures that are reliable, scalable, and support critical business initiatives and functions. will have the opportunity to gain experience with the foundational principles, frameworks, and practices necessary to design and implement secure digital infrastructures and apply them in the workplace. Students will navigate through core security architecture concepts, security design principles, security controls, and security infrastructure technology architectures that can be applied in varying organizations.

COMP-2049
Security Service Delivery

This course guides students through delivery of essential and effective security services leveraging various project management methodologies. Students will examine the alignment of security services to meet business needs through discovery of what it takes to deliver and operate a service from inception to end-of-life. Operationalization of a service from a management perspective is a key element of this course where students will explore important components such as managing a budget and creating metrics. Students will utilize practices for managing successful projects while incorporating the People, Process, and Technology framework.

COMP-2055
Security Program Management

In the dynamic world of Information Technology, Information Security is paramount for safeguarding assets. Students will have the opportunity to gain a comprehensive understanding of both theoretical and practical aspects of Security Management. Students will examine the importance of building and managing an effective security program that also supports technology projects. Focusing on leadership qualities, emphasis will be placed on student skill development in security strategies for mitigating security risks and fostering a security-centric and inclusive organizational culture. Students will be better positioned as aspiring IT security managers and leaders to integrate security as a core business strategy into diverse organizations.

COMP-2056
Vulnerability Management and Ethical Hacking

Students will be provided with the opportunity to participate in advanced vulnerability management and ethical

hacking practices. Students will utilize tools for vulnerability management and penetration testing as well as learn the importance of vulnerability reporting and communicating the results. The legal and philosophical aspects of hacking will be explored, and students will be able to describe vulnerabilities found in industry specific vulnerability databases. Equipped with a blend of hands-on experience and theory, students will be prepared to conduct vulnerability management in various technological and physical environments.

COMP-2057
Security Resiliency Planning

We live in a world of increasingly interconnected global systems where resiliency planning has become a priority for many governments, businesses, and Indigenous communities. Students will explore multiple aspects of resiliency planning, including Incident response, business continuity, disaster recovery, and risk management. Students will engage in collaborative exercises that assist with resiliency and contingency planning. These stages will allow students to form a comprehensive approach to managing incidents, solving problems, ensuring business continuity, and recovering from disasters, thereby minimizing the impact on business operations and ensuring resilience.

COMP-2058
Advanced Security Infrastructure

This course will provide students with the knowledge and skills to protect an organization from cyber security threats and attacks to safeguard their assets and data. Students will examine security concepts, technologies and best practices for the implementation and maintenance of security controls. The establishment of defense in depth strategies to protect the integrity, confidentiality and availability of IT systems will be examined. The students will explore the process of testing security solutions to ensure that the security technology is ready for deployment, minimizing the risk of security breaches and enhancing the overall security posture of varied organizations.

COMP-2059
Managing Security Operations

This course covers the key areas of managing a security operations organization, from crafting and implementing strategic security policies to daily security management. Students will experience working with threat intelligence systems and services. In addition, students will cover elements of human resource management such as equity, diversity, and inclusion, and vendor management as well as security services maintenance associated with security operations. Students will assess industry trends and measure service effectiveness using capability maturity models. By blending theoretical and practical concepts students will be equipped with skills required to manage security operations.

COMP-2060
Digital Forensics and Incident Response

Increased cyber threats are driving the need for security incident response and digital forensics when breaches occur in an organization. In this course, students will learn to use Incident Response plans that promote the necessary skills and knowledge to detect, respond, manage, and recover from security incidents. Students will engage in an investigative scenario where forensic tools and processes will be utilized to maintain chain of custody and gather evidence. In addition, the course will incorporate student participation in post incident reviews, as well as development of effective communications related to these concepts.

COMP-2061
Security and AI

This course bridges the gap between artificial intelligence (AI) and information security, offering insights into how AI technologies can be harnessed to bolster security defenses and mitigate risks. Students will learn about AI-driven security strategies, machine learning models for threat detection, ethical considerations and bias in AI deployment. Students will gain hands-on experience through application of AI technologies for enhancing security postures, detecting and responding to threats, and automating security tasks. The combination of

artificial intelligence techniques and foundational security principles will help prepare students to engage in protecting organizational digital assets.

COMP-2067
Governance, Audit and Compliance

In this course students will learn about key governance frameworks and integrate them with diverse organizational cultures and roles from the boardroom to operations. Students will develop a model to manage Governance, Risk, and Compliance which will align IT strategy with business objectives. Students will be introduced to topics such as IT risk, legal requirements, and Key Goal Indicators (KGI's) as well as audit and compliance concepts such as preparing for security audits and navigating industry-specific regulation requirements. A blend of theory, real-world scenarios, and practical exercises will provide students with industry knowledge necessary in these fields.

INDP-3004
Industry Project

In this course, students will be challenged to apply their knowledge and skills of information security in a real-world application. Working closely with an industry partner and instructor, students will identify a security risk that requires mitigation. Each project team will analyze, plan, and research a proposed security solution which will be presented to stakeholders. The team will implement and test the proposed solution. Finally, students will critically evaluate the impact of the security solution through a structured 'lesson learned' process, reflecting on areas of success and identifying opportunities for improvement.

Prerequisites:
Take: COMP-2046 COMP-2048 COMP-2049 COMP-2055 COMP-2056 COMP-2057 COMP-2058 COMP-2059 and COMP-2060

CO-OP/Practicum Information

Term 4 offers a 90-hour integrated WIL component where it will be taken concurrently with the other courses in Term 4. Students will choose an industry project where they will be given an opportunity to work with either their current employer, another employer, or a project within the Applied Computer Education (ACE) Project Space where they will work with local entrepreneurs on an interdisciplinary team that includes students from other ACE programs.

Computer/Laptop Requirements

Students need to provide their own laptop and have a high-speed internet connection. Students will require a Standard Type A device under the new College standards for laptops.

The college uses the Microsoft Teams application to host online classes therefore students will need this application on their laptops. There is a web version of Teams, however for optimal function the application is preferred.

All curriculum will be stored and utilized in Learn.

- RRC Polytech Computer Requirements
- RRC Polytech Learning Technologies – Technical and Software Requirements

Objectives/Learning Outcomes

Upon successful completion of the program, the graduate should be able to:

1. Demonstrate interpersonal skills and insights such as collaboration, facilitation, feedback processes, and networking with professionals in the field.
2. Create strategies for business resilience to protect business assets and data.
3. Demonstrate proficiency in delivering adaptable and secure security services that align with evolving organizational needs and industry trends.
4. Manage security initiatives effectively while fostering a security-centric organizational work culture.
5. Develop secure architecture and design for IT infrastructure that adheres to industry standards and regulatory requirements.
6. Apply governance, risk management, and compliance (GRC) principles to maintain security frameworks within organizations.
7. Mitigate cybersecurity threats by using advanced methods and solutions to protect organizations.
8. Apply security measures and technologies to meet evolving threats and business needs, align security strategies with organizational goals, and collaborate with stakeholders for integrated security decision-making
9. Examine how artificial Intelligence impacts cybersecurity in positive and negative ways.
10. Mitigate risk for an organization through identifying and testing security measures for IT infrastructures.
11. Conduct forensic analysis to identify the root cause and trace the timeline of security incidents, using appropriate tools and techniques.
12. Demonstrate the communication skills necessary for communicating with peers, stakeholders, business units and the general public regarding security risk mitigation strategies.

Recognition of Prior Learning

Recognition of Prior Learning (RPL) is a process which documents and compares an individual's prior learning gained from prior education, work and life experiences and personal study to the learning outcomes in College courses/programs. For more information, please visit www.rrc.ca/rpl.

Graduation Requirements

Students will earn the Information Security Post-Grad Diploma by completing a minimum of 62 Credit Units consisting of 990 hours of classroom learning over four (4) academic terms which includes a 90 hour work integrated learning (WIL) component in Term 4. Course-based registration allows students to complete the program on a full-time basis in a minimum of 16 months. Typical full-time students who take a four-month study break each year will complete the program in 20 months. As per College policy, students must complete the program within four years.

Academic Advising Service
Our academic advising service can provide information about our full-time programs, explain program admission requirements, and help you select the right program to meet your career and academic goals. We can also connect you with helpful people, resources, and supports.

- For more information visit academic advising.
- If you are an Indigenous student, you can contact an Indigenous Admissions Advisor.
- If you are an international student, you can contact International Education.

Page produced on 2025-06-02 12:12:43