Research Proposal: Enhancing Cybersecurity at the Applied Computer Science Department, University of Winnipeg

1. **Introduction:**

1.1 Background:

The higher reliance on computer system in a post-COVID world opened up more opportunities for malicious actors to attack and compromise system in higher education institution. In recent years, there is an increase in cyber attacks with higher complexity and the damage of those attacks mounting. This research aims to analyze cyber attack occurrences within the Applied Computer Science department over the past 5 years, analyze existing security measure and evaluate how effective they are in combating current and emergence cyber threats, to find vulnerabilities within current systems of the department, and propose solutions to reduce current and future threats pose to the Applied Computer Science department.

1.2 Rationale:

In a post-COVID world where digital usage is higher than ever, educational institutions are major target for cyber attacks. This research will be a major step in understanding past cyber attack, analyze current system in Applied Computer Science department to increase cyber awareness and preparedness for future cyber attacks. This will increase security posture of the department for current cyber threat as well as emergence security threat. This will increase protection of Applied Computer Science department's sensitive and important information.

2. **Objectives:**

1. To investigate past cyber attacks occurrence within Applied Computer Science department.
2. To analyze the methods of attack, attack surfaces and damage caused due to those past attacks.
3. To review current systems, critical assets, and architectural design of Applied Computer Science department and check with findings of past attacks to assess vulnerabilities within the system.
4. To evaluate current protocols, security policy of Applied Computer Science department for their effectiveness to current and emerging security threats.
5. To evaluate the effectiveness of current control mechanism, defensive measure implemented in Applied Computer Science department's system.

6. To conduct risk analysis and propose strategies to mitigate those risk specific to Applied Computer Science department.
7. To design an incident response plan specific to Applied Computer Science department to increase system security and smoother recovery from breaches.
8. To design and implement penetration testing plan to frequently check for vulnerabilities, keeping Applied Computer Science department system up to date regarding latest attack methods, increase overall cybersecurity of system.

3. Research Questions:

1. What recent cybersecurity incidents have been observed within the Applied Computer Science Department, and what were their impact and implications?
2. How effective are the current security measures implemented within the department in mitigating cybersecurity threats?
3. What vulnerabilities exist in the current cybersecurity infrastructure, and how do they pose a risk to the confidentiality, integrity, and availability of departmental data?
4. How aware are the faculty, staff, and students of the cybersecurity policies and procedures in place, and to what extent do they adhere to them?
5. What measures can be implemented to enhance the cybersecurity awareness and education among the Applied Computer Science Department community?
6. In the event of a cybersecurity incident, what is the readiness of the department to respond effectively and minimize the impact on its operations?
7. What are the potential future cybersecurity threats that the Applied Computer Science Department might face, considering emerging technologies and trends?
8. How do existing security measures align with industry best practices and compliance standards relevant to academic institutions?
9. What comprehensive solutions can be proposed to address current vulnerabilities and enhance the overall cybersecurity posture of the department?
10. How can collaboration between IT administrators, faculty, staff, and students be strengthened to collectively contribute to the cybersecurity resilience of the Applied Computer Science Department?

4. Methodology:

4.1. Literature Review:

- Review existing research papers about cyber security in academic institution setting. Focus on finding trends, best practice, weakness in research paper methodology.

Emphasis with case studies that have similar conditions and system architecture with Applied Computer Science department within University of Winnipeg.

4.2. Interviews:

- Interview with stakeholders within Applied Computer Science department to collect data about past attack attempts and gather requirements for future solution proposal.

4.3. Review and Security Analysis:

- Review documentation in Applied Computer Science department or IT department such as security policy, architectural designs, system components detail to assess current security measures and identify vulnerabilities.

4.4 Policy and Mechanism Review:

- Review security policy at the department, current security mechanism and defensive measure in the department and evaluate their effectiveness against current and emergence security threats.

4.5. Risk Analysis:

- Create a risk analysis documentation based on finding in the department to figure out most severe threats and damage if those threat become attack.

4.6. Mitigation Strategies:

- Create mitigation strategies for those severe threats to minimize the damage cause to the department.

4.7. Incident Response Plan:

- Create incident response plan in case those severe threats become attack, detailing steps needed to be taken to minimize damage and accelerate recovery.

4.8. Penetration Testing:

- Create and implement a penetration testing plan to search for vulnerabilities within Applied Computer Science department's system and provide a stepping stone for future research into future potential attacks.

5. Expected Outcome:

1. Collected detailed information about past cyber attacks occur in Applied Computer Science department.

2. Analyze collected information to figure out the attack pattern, attack surface and vulnerabilities exploded.
3. Assess the current Applied Computer Science department system against known attack pattern, attack surface and vulnerabilities.
4. Risk analysis based on finding from analyzing documents and collected information to find severe threats pose to Applied Computer Science department.
5. Mitigation strategies to reduce threat cause by past cyber attacks.
6. Incident response plan for severe threats found in risk analysis for minimize damage and accelerate recovery.
7. Implement a penetration testing plan to increase readiness of Applied Computer Science department's system for future potential threats and create a base for future research into future potential threats.

6. Project Timeline:

Phase	Activities	Timeline
Preliminary research	Literature review	15 Jan – 29 Jan
Data collection and analysis	Interviews and analysis from gather data	29 Jan – 12 Feb
Security Analysis	Review and assess system architecture, security mechanism and policies	12 Feb – 19 Feb
Risk Analysis	Identify and prioritize risk base on severity	19 Feb – 26 Feb
Mitigation Strategies	Develop a mitigation strategy for severe threats	26 Feb – 4 Mar
Incident Response Plan	Create a comprehensive incident response plan	4 Mar – 11 Mar
Penetration Testing Plan	Create penetration testing plan and implement it	11 Mar – 25 Mar
Final Report	Compile all findings and plans into a comprehensive report	25 Mar – 8 Apr

7. Significance of the Study:

This study is essential for enhancing cybersecurity of Applied Computer Science department, increasing protection of sensitive data and intellectual property of the department. This study also helps to ensure continuous functioning of academic and research activities within the department. This study will set a base for future study into cybersecurity within academic setting in University of Winnipeg.

8. Budgetary Requirements:

8.1 Resources:

- Interview time with relevant staff or personnel within Applied Computer Science department and IT department
- Access to require documentation such as security policy, cyber incident logs, system architecture documentation
- Tools for penetration testing such as OWASP ZAP

8.2 Funding:

- Fund for penetration testing tools

9. Conclusion:

This research will enhance Applied Computer Science department cybersecurity, bring more awareness of cyber threats and foster a culture of preparedness to cyber attacks. The research will also assess current system and architecture of department as well as gather crucial information into preparedness of the department relating to cyber threats. This research will help protect Applied Computer Science department sensitive information and intellectual properties as well as ensure uninterrupted system operation.