Master of Science in Cyber Security
Minor in Data Protection for Faith-Based Organizations

HBI University
Course Duration: 2 years
Credit Hours: 69 (including 15 credit hours for minor)

Program Description

The Master of Science in Cyber Security at HBI University prepares students to address contemporary cybersecurity challenges by equipping them with advanced technical knowledge, leadership skills, and hands-on experience. This program covers key areas such as ethical hacking, digital forensics, risk management, and network security, providing students with a well-rounded education in cyber defense strategies.

The Minor in Data Protection for Faith-Based Organizations focuses on specialized cybersecurity measures tailored for religious and faith-driven institutions. Students will learn to implement security frameworks, develop incident response plans, and ensure compliance with data protection regulations within faith-based communities and organizations.

Admissions Requirements

- Bachelor's degree in a relevant field
- Minimum GPA of 3.0
- GRE scores (if applicable)
- Statement of Purpose (1,000-1,500 words) outlining research interests and career goals
- Three letters of recommendation
- Academic writing sample
- Curriculum Vitae (CV) or resume
- Interview with faculty (if required)

Foundational Courses (30 Credit Hours)

Course Code	Course Name	Credit Hours
CYB 201	Cybersecurity Fundamentals	3
CYB 202	Network Security Principles	3
CYB 203	Cryptography and Data Protection	3
CYB 204	Ethical Hacking and Penetration Testing	3
CYB 205	Cyber Law and Policy	3
CYB 206	Digital Forensics and Incident Response	3
CYB 207	Cloud Security Strategies	3
CYB 208	Secure Software Development	3
CYB 209	IoT and Emerging Threats	3
CYB 210	Human Factors in Cybersecurity	3

Core Courses (24 Credit Hours)

Course Code	Course Name	Credit Hours
CYB 601	Advanced Network Security	3
CYB 602	Cyber Risk Management	3
CYB 603	Threat Intelligence and Analysis	3
CYB 604	Blockchain and Cybersecurity	3
CYB 605	Security Operations and Incident Handling	3
CYB 606	AI and Machine Learning in Cybersecurity	3
CYB 607	Mobile Security and Threats	3
CYB 608	Capstone in Cybersecurity	3

Minor in Data Protection for Faith-Based Organizations (15 Credit Hours)

Course Code	Course Name	Credit Hours
DPF 701	Data Privacy in Religious Institutions	3
DPF 702	Cybersecurity for Non-Profit Organizations	3
DPF 703	Compliance and Legal Issues in Faith-Based Organizations	3
DPF 704	Digital Transformation in Religious Communities	3
DPF 705	Incident Response Planning for Faith-Based Entities	3

Additional Elective Courses

Course Code	Course Name	Credit Hours
ELE 701	Artificial Intelligence in Cybersecurity	3
ELE 702	Social Engineering and Security Awareness	3
ELE 703	Biometric Security and Authentication	3
ELE 704	Cybersecurity in Healthcare	3
ELE 705	Advanced Cryptographic Techniques	3

Practicum Experience

The practicum experience provides students with real-world exposure to cybersecurity operations, security threat mitigation, and policy enforcement in professional settings. Students will collaborate with organizations to develop cybersecurity frameworks and conduct risk assessments.

- A minimum of 200 hours of supervised field experience.
- Submission of a detailed practicum report.
- Participation in cybersecurity workshops and professional development.
- Completion of a final presentation summarizing practical experiences.

Master's Thesis Requirements

The Master's thesis is a comprehensive research project that allows students to contribute to the field of cybersecurity by addressing emerging threats and proposing innovative solutions. The thesis process includes:

- Developing a research proposal approved by faculty.
- Conducting a literature review and methodology selection.
- Data collection, analysis, and interpretation.
- Writing a thesis (minimum 50 pages) following academic guidelines.
- Successful defense before a faculty committee.

Program Outcomes

- Develop expertise in risk assessment and cyber threat mitigation.
- Implement advanced encryption and security protocols.
- Lead security teams in corporate and non-profit environments.
- Ensure compliance with data protection laws in faith-based organizations.

Advocacy in Cyber Security for Faith-Based Organizations

As cyber threats continue to evolve, faith-based organizations must prioritize data security, privacy, and ethical digital management. Graduates of this program will be equipped to advocate for secure IT infrastructures, protect sensitive religious and community data, and implement cybersecurity best practices in faith-based institutions.

Career Outcomes and Potential Pay Scale

Career Path	Average Salary (Annual)
Cybersecurity Analyst	$85,000 - $130,000
Chief Information Security Officer (CISO)	$150,000 - $250,000
Penetration Tester	$90,000 - $140,000
Network Security Engineer	$95,000 - $145,000