

Doctor of Cyber Security, Minor in Data Protection for Faith-Based Organizations

HBI University

Course Duration: 3 Years

Total Credit Hours: 105

Program Description

The Doctor of Cyber Security with a specialization in Minor in Data Protection for Faith-Based Organizations equips students with in-depth technical expertise and leadership capabilities required to manage complex systems, data infrastructures, and ethical decision-making within healthcare, technology, or humanitarian sectors.

This program integrates research, hands-on applications, and strategic insight across operational and policy-level environments. Graduates of the Doctor of Cyber Security will be prepared to lead initiatives in global and faith-based institutions.

The minor adds essential knowledge and practical skills to support targeted organizational or ministry contexts that serve the public good.

Admissions Requirements

- Master's degree in a related field
- Minimum GPA of 3.5
- 3-5 years of field experience
- Statement of purpose (1,000–1,500 words)
- Three letters of recommendation
- CV or professional résumé
- Faculty interview (if applicable)

Foundational Courses (30 Credit Hours)

Course Code	Course Name	Credit Hours
FND 800	Innovation and Technology in Doctor of Cyber Security	3
FND 801	Advanced Theories in Doctor of Cyber Security	3
FND 802	Cultural Competency in Doctor of Cyber Security	3
FND 803	Global Issues in Doctor of Cyber Security	3
FND 804	Quantitative Analysis for Doctor of Cyber Security	3

FND 805	Community Engagement in Doctor of Cyber Security	3
FND 806	Ethical Frameworks in Doctor of Cyber Security	3
FND 807	Capstone Project in Doctor of Cyber Security	3
FND 808	Policy and Practice in Doctor of Cyber Security	3
FND 809	Leadership in Doctor of Cyber Security	3

Core Courses (24 Credit Hours)

Course Code	Course Name	Credit Hours
COR 800	Advanced Theories in Doctor of Cyber Security	3
COR 801	Leadership in Doctor of Cyber Security	3
COR 802	Capstone Project in Doctor of Cyber Security	3
COR 803	Global Issues in Doctor of Cyber Security	3
COR 804	Quantitative Analysis for Doctor of Cyber Security	3
COR 805	Ethical Frameworks in Doctor of Cyber Security	3
COR 806	Community Engagement in Doctor of Cyber Security	3
COR 807	Policy and Practice in Doctor of Cyber Security	3

Minor Courses (15 Credit Hours)

Course Code	Course Name	Credit Hours
MIN 800	Leadership in Minor in Data Protection for Faith-Based Organizations	3
MIN 801	Policy and Practice in Minor in Data Protection for Faith-Based Organizations	3
MIN 802	Community Engagement in Minor in Data Protection for Faith-Based Organizations	3
MIN 803	Quantitative Analysis for Minor in Data Protection for Faith-Based Organizations	3
MIN 804	Innovation and Technology in Minor in Data Protection for Faith-Based Organizations	3

Additional Elective Courses (Not Included in Total Credits)

Course Code	Course Name	Credit Hours
ELE 800	Ethical Frameworks in Security	3
ELE 801	Advanced Theories in Security	3
ELE 802	Innovation and Technology in Security	3
ELE 803	Global Issues in Security	3
ELE 804	Community Engagement in Security	3

Practicum Experience

Doctoral candidates in the Doctor of Cyber Security complete a field-based practicum in partnership with a public institution or faith-based organization. The practicum allows for critical skill development and reflective evaluation.

Practicum Requirements:

- 600 hours of supervised service
- Midterm and final site evaluations
- Reflection paper and presentation
- Faculty-reviewed practicum portfolio

Doctoral Dissertation Requirements

The dissertation for the Doctor of Cyber Security requires students to identify a current issue or innovation in their field and develop a solution through rigorous research. This original contribution must blend academic insight with practical application within a faith-aligned framework.

Requirements:

- Dissertation proposal approval
- Ethical review (IRB, if applicable)
- Field research, analysis, and synthesis
- Full manuscript (minimum 100 pages)
- Successful oral defense

Program Outcomes

- Lead in the evolving field of doctor of cyber security
- Develop innovative, ethical, and evidence-based strategies
- Conduct interdisciplinary research for applied impact
- Serve organizations and ministries with integrity
- Influence policy and operational effectiveness

Career Outcomes and Potential Pay Scale

Career Path	Average Salary (Annual)
Doctor of Cyber Security Strategist	\$95,000 – \$155,000
Doctor of Cyber Security Consultant	\$90,000 – \$145,000
Doctor of Cyber Security Research Director	\$100,000 – \$160,000
Doctor of Cyber Security Professor	\$85,000 – \$135,000
Doctor of Cyber Security Program Manager	\$88,000 – \$140,000

Dissertation Outline

#	Section	Details
1	Introduction	• Define purpose and research question(s)
2	Literature Review	• Contextualize research with existing theory and practice
3	Methodology	• Describe tools, framework, and rationale
4	Results	• Present evidence-based findings from research
5	Discussion	• Analyze implications for practice, theory, and ethics
6	Conclusion	• Recap findings and recommend next steps
7	References and Appendices	• Source list and supplementary material