

Associate in Cyber Security

Specialization in Faith-Based Cyber Security and Data Protection

HBI University

Course Duration: 2 years

Credit Hours: 60 hours (including 15 credit specialization hours)

Program Description

The Associate in Cyber Security program with a Specialization in Faith-Based Cyber Security and Data Protection at HBI University trains students to secure systems, protect sensitive information, and support digital ministries through ethical and mission-driven cybersecurity practices. Students will develop practical skills in network defense, risk management, and information security with a foundation in Christian integrity and stewardship.

Students will gain hands-on experience in ethical hacking, threat mitigation, system auditing, and security frameworks while exploring how churches and faith-based nonprofits can protect themselves from digital threats and ensure the integrity of their online operations and data.

Graduates will be prepared for entry-level cybersecurity roles within ministry, nonprofit, and private sectors, with the confidence to lead data protection with a servant's heart and a secure strategy.

General Education Courses (15 Credit Hours)

Course Code	Course Name	Credit Hours
GEN 101	English Composition I	3
GEN 102	English Composition II	3
GEN 103	College Algebra	3
GEN 104	Introduction to Psychology	3
GEN 105	Introduction to Sociology	3

Core Cyber Security Courses (30 Credit Hours)

Course Code	Course Name	Credit Hours
-------------	-------------	--------------

CYB 201	Introduction to Cyber Security	3
CYB 202	Networking and Network Security	3
CYB 203	Operating Systems and System Hardening	3
CYB 204	Ethical Hacking and Penetration Testing	3
CYB 205	Cyber Threat Intelligence and Analysis	3
CYB 206	Security Policies and Compliance Frameworks	3
CYB 207	Incident Response and Disaster Recovery	3
CYB 208	Cloud Security and Virtual Infrastructure	3
CYB 209	Digital Forensics and Investigation	3
CYB 210	Security Operations Center (SOC) Practices	3

Elective Courses (15 Credit Hours)

Course Code	Course Name	Credit Hours
CYB 301	Mobile and Wireless Security	3
CYB 302	Cybersecurity for Churches and Ministries	3
CYB 303	Privacy Laws and Ethical Decision Making	3
CYB 304	Introduction to Programming for Security	3
CYB 305	Faith-Based Risk Assessment and Mitigation	3

Specialization in Faith-Based Cyber Security and Data Protection (15 Credit Hours)

Course Code	Course Name	Credit Hours
FSC 401	Theology of Protection and Digital Stewardship	3
FSC 402	Securing Faith-Based Digital Platforms	3
FSC 403	Ethics in Cybersecurity from a Biblical Perspective	3
FSC 404	Cybersecurity Awareness and Congregational Training	3
FSC 405	Building a Secure Digital Ministry Environment	3

Capstone Project (3 Credit Hours)

The Capstone in Faith-Based Cyber Security and Data Protection invites students to apply cybersecurity knowledge in a faith-based or nonprofit environment. Students may:

- Conduct a cybersecurity risk assessment for a church or ministry.
- Develop a training program for data protection in online faith platforms.
- Simulate a network defense strategy for a nonprofit IT system.

Program Outcomes

Graduates of this program will:

- Identify and mitigate cyber threats in ministry and nonprofit environments.
- Apply security frameworks with a foundation in Christian values.
- Promote safe digital practices within congregations and organizations.
- Implement IT defense strategies with integrity and foresight.
- Protect sensitive ministry data with technical and ethical excellence.

Career Outcomes and Potential Pay Scale

Career Path	Average Salary (Annual)
Faith-Based Cybersecurity Specialist	\$48,000 - \$70,000
Church/Ministry IT Security Administrator	\$50,000 - \$72,000
Nonprofit Information Security Analyst	\$52,000 - \$75,000
Cybersecurity Awareness Trainer	\$45,000 - \$65,000

Digital Risk Consultant (Faith-Based)	\$50,000 - \$78,000
---------------------------------------	---------------------