New Academic Degree Program
Full Proposal Application
South Dakota Board of Regents
Academic Affairs Forms

Internal Ticket ID: 8992
Created: 5/30/2023
Modified: 7/22/2025

Use this form to propose a new degree program. The Board of Regents, Executive Director, and/or their designees may request additional information about the proposal. After the university President approves the proposal, submit a signed copy to the Executive Director through the System Academic Officer (through the online submission process).

Note: Within the proposal, all references to external sources should be documented with a footnote (including web addresses where applicable).

University DSU - Dakota State University
Degree MS : Master of Science
Name of Major X999 : New Major Requested **Data Privacy**
Specialization Required? No
Note: If the new proposed program includes specific specializations within it, complete and submit a New Specialization Form for each proposed specialization and attach it to this form. Since specializations appear on transcripts, they require Board approval.
College/Department 8N : DSU Beacom Comp Cyber Sciences/DCSI : Computer Science
Planned CIP Code 111003
WICHE WRRGP Eligibility Yes

Program Description

1. Provide the working program description that may appear in the university catalog.

The Master of Science in Data Privacy (MSDP) at Dakota State University (DSU) equips graduates with the expertise to navigate the complex and evolving landscape of data privacy. This program explores the critical role of data in government, corporate, and nation-state contexts, applying technical, legal, and policy frameworks to ensure its protection and ethical use.

Students develop in-depth knowledge in privacy regulation, data governance, and privacy-enhancing technologies, gaining the skills to design policies, implement safeguards, and measure compliance effectively. Designed for working professionals, this fully online, asynchronous program provides students with the flexibility to advance their career while mastering the future of data privacy.

2. Does the university request any exceptions to any Board policy for this program?
Explain any requests for exceptions to Board Policy. If not requesting any exceptions, indicate ***"None."***

None

Strategic Impact

3. Describe how the program fits in with the institutional mission, strategic plan, existing institutional program array, and academic priorities.

The proposed MSDP aligns closely with DSU's mission as outlined in SDCL § 13-59 and BOR Policy 1.2.2, which identifies DSU as a leader in providing undergraduate and graduate education in computer management, computer information systems, and related technologies. This program advances DSU's commitment to offering cutting-edge education in the areas of cybersecurity, data protection, and computing, emphasizing innovation and excellence in technology.

Institutional Mission Alignment

- SDCL § 13-59 establishes DSU's unique role in South Dakota as a center for expertise in computing and cyber sciences. The MSDP reflects this mandate by addressing the critical and growing challenges of safeguarding digital information in a highly connected world.
- The program builds on DSU's strengths in cybersecurity, artificial intelligence, and cyber operations, further solidifying its reputation as a national leader in these fields.

Strategic Plan Alignment

- The program aligns with DSU's Strategic Plan ADVANCE 2027, which outlines five pillars of focus, particularly:
  - Enhancing Student Success: The program equips students with in-demand skills to secure employment in high-growth fields like cybersecurity and data privacy. The goal of placing 100% of graduates in relevant roles within six months is directly supported by the program's emphasis on technical expertise, policy knowledge, and compliance capabilities.
  - Increasing Sustainability and Resilience: By addressing the demand for graduates in computer science, cyber operations, and related areas, the program contributes to the university's goal of increasing graduates in these disciplines by at least 10%.

Integration with Existing Program Array

- The program complements existing offerings in DSU's Beacom College of Computer and Cyber Sciences, including the MS in Cyber Defense and the Ph.D. in Cyber Operations. While those programs focus heavily on technical and offensive cybersecurity strategies, the MSDP emphasizes the legal, ethical, and policy governance of the data protection life cycle, creating a broader, more interdisciplinary array of graduate-level offerings.
- The program builds on the Graduate Certificate in Data Privacy, which has already demonstrated demand and success, providing a seamless pathway for certificate holders to advance to a full master's degree and increase the number of qualified professionals in the workforce.

Academic Priorities

- The MSDP represents a multidisciplinary effort, integrating coursework and expertise from the Beacom College of Computer and Cyber Sciences, the College of Arts and Sciences, and the College of Business and Information Systems.
  - Beacom College of Computer and Cyber Sciences: Technical foundations in data governance, privacy-enhancing technologies, digital forensics, and incident response are core to the program.
  - College of Arts and Sciences: Ethical considerations, international privacy laws, data sovereignty, digital democracy, and related topics at the intersection of law, technology, and societal impacts of data privacy are explored, reflecting DSU's broader commitment to fostering critical thinking and global awareness.
  - College of Business and Information Systems: The program incorporates management principles and regulatory compliance to address practical organizational needs.

Regional and National Impact

- The program meets a critical workforce need in South Dakota, where industries like healthcare, finance, agriculture and government require professionals with expertise in data privacy. By training specialists in this field, DSU contributes to the state's economic development and fulfills its role as a strategic partner for workforce readiness.
- Nationally, the surge in interest in AI, quantum, and spatial computing (virtual and augmented realities) demands more expertise around critical data privacy issues. The proposed MSDP positions DSU as a premier institution not only for informing issues around privacy legislation and policy, but in providing privacy

education, attracting students from multiple disciplines across the country to study in South Dakota or online, thereby enhancing the university's reputation and reach.

In summary, the proposed MSDP not only advances DSU's mission but also strategically aligns with its academic priorities, institutional strengths, and the broader goals of the South Dakota Board of Regents to create paths into STEM careers for students and elevate the national reputation of the state. This program exemplifies DSU's dedication to innovation in education and its commitment to producing graduates who are prepared to tackle some of the most pressing challenges in today's digital landscape.

If the program does not align to the strategic plan, provide a compelling rationale for the institution to offer the program.

NA

4. How does the program connect to the Board of Regent's Strategic Plan?

Goal 1: Student Success and Educational Attainment

- The MSDP prepares graduates for high-demand, high-reward careers in data privacy and cybersecurity. With data privacy being a rapidly expanding field, the program directly supports student success by equipping graduates with the technical, legal, and ethical expertise required to thrive in a competitive job market.
- The fully online, asynchronous delivery model increases access for working professionals and nontraditional students, supporting broader participation and degree completion, which aligns with SDBOR's focus on improving educational attainment across South Dakota.

Goal 3: Academic Excellence, Student Outcomes, and Workforce Readiness

- The MSDP exemplifies academic excellence by integrating cutting-edge curriculum based on national standards such as the National Institute of Science and Technology (NIST) Privacy Framework and General Data and Privacy Regulation (GDPR) and EU Artificial Intelligence (AI) Act. It offers students real-world applications, capstone projects, and industry-relevant skills that enhance workforce readiness.
- Graduates will be equipped to fill key roles such as Privacy Manager, Data Privacy Auditor, and Governance Risk and Compliance Manager, addressing the workforce gaps identified in South Dakota and nationally.

Goal 4: Workforce and Economic Development

- Data privacy professionals are essential for industries critical to South Dakota's economy, including healthcare, finance, agriculture and government. This program directly addresses the state's economic development priorities by supplying a skilled workforce to meet growing data privacy demands.
- The program fosters partnerships with industry leaders, government agencies, and other institutions, contributing to a collaborative approach to workforce and economic growth.

Goal 5: Research and Innovation

- By offering courses in advanced privacy technologies and compliance strategies, the program supports innovation in cybersecurity and in data life cycle protection integrity. Students will engage in research and practical applications that drive new solutions to evolving privacy challenges, fostering an innovative ecosystem at Dakota State University.

Addressing SDBOR Workforce Analysis

The SDBOR Workforce and Degree Gap Analysis Report highlights a critical shortage of professionals in cybersecurity and data privacy roles within South Dakota. The MSDP:

- Addresses this gap by producing skilled professionals who can secure sensitive data, ensure compliance with privacy regulations, and strengthen organizational resilience.
- Enhances South Dakota's competitiveness in attracting and retaining businesses that prioritize data privacy and security.
- Addresses emerging needs in data and surveillance protection (i.e., drones, autonomous vehicles) in agriculture, small business, and rural tele-health (Data Privacy Roundtable, DSU, May 8, 2024)

Advancing SDBOR's Strategic Vision

By combining academic rigor, accessibility, and relevance to workforce needs, the MSDP exemplifies the SDBOR's commitment to preparing graduates for high-impact careers that contribute to the state's economic vitality and the nation's technological leadership. This program underscores DSU's role as a strategic partner in achieving the SDBOR's mission of excellence in higher education and workforce development.

Program Summary

5. If a new degree is proposed, what is the rationale?

This question refers to the type of degree, not the program. For example, if your university has authorization to offer the Bachelor of Science and the program requested is a Bachelor of Science, then the request is not for a new degree.

This is not a new degree type.

6. What modality/modalities will be used to offer the new program?

Note: The accreditation requirements of the Higher Learning Commission (HLC) require Board approval for a university to offer programs off-campus and through distance delivery.

	Yes/No	Intended Start Date
On Campus	No	

	Yes/No	Location(s)	Intended Start Date
Off Campus Location	No		

	Yes/No	Delivery Method(s)	Intended Start Date
Distance Delivery	Yes	Online Asynchronous	Spring 2026

	Yes/No	Identify Institutions
Does another BOR institution already have authorization to offer the program online?	No	

7. If the program will be offered through distance delivery, identify the planned instructional modality:

Asynchronous : Students are not required to attend the course at a specific time or location.

8. What are the student learning outcomes for this program?

a. Develop comprehensive privacy solutions to address complex data privacy challenges from technical, ethical, legal, and policy perspectives.
b. Assess the degree to which privacy-enhancing measures align with evolving regulatory frameworks.
c. Apply regulatory applications of data governance to real-world privacy scenarios.
d. Design a comprehensive data privacy risk management program.

9. For associate's and bachelor's degree proposals, identify the 3-5 AAC&U Essential Learning Outcomes that have been selected for this program.

Use the chart below to indicate the student learning outcomes that align to the selected ELOs (See BOR Policy 2.11 and Guideline 8.5).

Essential Learning Outcomes (AAC&U)	Student Learning Outcomes
Inquiry and Analysis	
Critical and Creative Thinking	
Information Literacy	
Teamwork	
Problem Solving	
Civic Knowledge and Engagement	
Intercultural Knowledge	
Ethical Reasoning	
Foundational Lifelong Learning Skills	
Integrative Learning	

10. Enter the number of credit hours required to graduate

Credit Hours	30

11.Complete the following tables to provide a degree program curriculum summary.

A. Table 1 –Total Program Degree Credit Hours

	Credit Hours In Program	
	Hours Per Requirement	**%Total Hours**
System General Education Requirements		
Subtotal - Gen Ed Requirements		%
Program Requirements		
Required Support Courses	30	
Major Requirements	0	
Major Electives	0	
Subtotal - Program Requirements	30	%
Free Electives	0	
Subtotal - Free Electives	0	%
Degree Total	30	%

**Board Policy 2:29 requires each baccalaureate level degree program to require 120 credit hours and each associate degree program to require 60 credit hours. Exceptions to this policy require documentation that programs must comply with specific standards established by external accreditation, licensure, or regulatory bodies or for other compelling reasons, and must receive approval by the Executive Director in consultation with the President of the Board of Regents.*

B. Table 2 – Insert Required Program Support Courses Impacting Other Programs (outside department). Do not include General Education courses.

*The individual curriculum tables should be included as a word document **attached** to the TDX ticket.*

C. Table 3 – Insert Major Requirements (within department)

*The individual curriculum tables should be included as a word document **attached** to the TDX ticket.*

D. Table 4 – Insert Major Electives

*The individual curriculum tables should be included as a word document **attached** to the TDX ticket.*

12. New Course Approval

New courses required to implement the new degree program may receive approval in conjunction with program approval or receive approval separately. Please check the appropriate statement:

Yes

Academic Quality

13. What peer institutions and current national standards will be referenced to develop the curriculum for this program?

Peer Institution: Regional and Competitive institutions. Include links to at least 3 comparable programs at peer institutions and links to national or accreditation standards, if any.

Comparable Programs at research institutions:

Master of Science in Privacy Engineering at Carnegie Mellon University (https://privacy.cs.cmu.edu/masters/index.html). Likely the first of its kind in the US, this program addresses both the technical and legal aspects of privacy.

Master of Science in Information Security and Privacy at the University of Texas at Austin (https://msisp.ischool.utexas.edu/graduate-degree/curriculum)
Focused on the legal, social and policy issues facing corporate and government entities.

Master of Law in Privacy, Cybersecurity, and Data Management, (https://curriculum.maastrichtuniversity.nl/education/post-initial-master/advanced-master-privacy-cybersecurity-and-data-management), Maastricht University, The Netherlands.
Illustrates the international interest in the intersection of Cybersecurity and Data Privacy.

Current National Standards:

National Institute of Standards and Technology (NIST) Privacy Framework (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf).
Technical standards and related tools developed by federal government with stakeholders from private and public sectors for data privacy research, use and development.

The General Data Protection Regulation (https://gdpr.eu/what-is-gdpr/) (GDPR) is a European law that established protections for privacy and security of personal data about individuals in European Economic Area ("EEA")-includes seven principles of data protection that must be implemented and eight privacy rights that must be facilitated.

14. What program accreditation is available, if any?

None available

15. Will the proposed program pursue accreditation or certifications?

No

If no, why has the department elected not to pursue accreditation for the program?

NA

16. Did the university engage any developmental consultants to assist with the development of the curriculum? Did the university consult any professional or accrediting associations during the development of the curriculum? What were the contributions of the consultants and associations to the development of the curriculum?

Developmental consultants are experts in the discipline hired by the university to assist with the development of a new program, including content, courses, and experiences, etc. Universities are encouraged to discuss the selection of developmental consultants with Board staff.

No. The MSDP is proposed by a team of faculty from an institution recognized as a National Cybersecurity Center of Academic Excellence (CAE) in Cyber Defense at the graduate level. This program is a key addition to DSU's array of computer, cyber and information science programs that reflect its commitment to advancing knowledge and delivering instruction in critical areas of data security and governance.

17. Inclusion of High Impact Practices (HIP) across all undergraduate programs is a strategic priority of the Board of Regents to enhance academic quality and increase student engagement. For associate's and bachelor's degree proposals, which HIPs will faculty embed into the program?

Mark all that apply. To be considered as a HIP program, two or more should be selected and required in the program.

High Impact Practices	Included
Capstone courses and projects	
Collaborative assignments and projects	
Common intellectual experiences	
Diversity/global learning	
ePortfolios	
First year experiences	
Internships	
Learning communities	
Service learning, community-based learning	
Writing intensive courses	
Undergraduate research	

18. For associate's and bachelor's degree proposals, discuss how HIPs will be embedded into the program

Your discussion should provide examples and include whether the HIP is required or an optional component. It should also indicate at what point the experience is offered or required. (eg "students will be required to participate in an internship during their third year of enrollment in order to develop skills in…").

Student Success

This section outlines the university's plan to assess student achievement of the program learning outcomes.

19. Complete the table below to provide evidence of a preliminary assessment plan. Place an asterisk next to assessments that are national or state-level instruments.

Note: It is only necessary to indicate the summative assessment for each outcome, not the formative assessments used throughout the program.

Program Learning Outcome	Course	Summative Assessment
Develop comprehensive privacy solutions to address complex data privacy challenges from technical, ethical, legal, and policy perspectives.	INFA 702 Data Privacy; INFA 722 Data Privacy Management; CLI 730 Global Privacy Law; CLI 732 Privacy Threats; HIMS 745 Legal and Ethical Aspects of Data Privacy	Capstone project incorporating case studies, written reports, and presentations that require students to integrate technical, ethical, legal, and policy dimensions in developing comprehensive privacy solutions.
Assess the degree to which privacy-enhancing measures align with evolving regulatory frameworks.	CLI 730 Global Privacy Law; INFA 744 AI and Data Privacy	Written analysis and evaluation of privacy-enhancing measures against current and emerging regulatory frameworks, using standardized benchmarks* to ensure rigor.
Apply regulatory applications of data governance to real-world privacy scenarios.	CLI 734 Digital Rights; HIMS 746 Data Governance; INFA 744 AI and Data Privacy	Project-based assessment where students apply data governance models to analyze and resolve real-world privacy scenarios, including a review of applicable regulations.
Design a comprehensive data privacy risk management program.	INFA 722 Data Privacy Management; INFA 726 Data Privacy Technology; INFA 748 Digital Forensics for Data Privacy	Final project in which students design and justify a data privacy risk management program that includes risk identification, assessment, mitigation strategies, and contingency planning.

20. How will outcomes for graduates of the program be assessed?

Outcomes may include employment and placement rates, licensure examination pass rates, acceptance rates to graduate school, student or employer surveys, or other assessments of graduate outcomes.

- Percentage of graduates of the program who secure employment within 6 months of graduation in program related positions.
- The percentage of employed graduate students who assume additional data privacy related job responsibilities in current positions or in positions to which they are promoted.
- Percentage of program graduates who pursue a discipline-related Ph.D. within 5 years of program completion.
- Graduate feedback (surveys, interview, focus groups) on graduates' career progression and how well the program prepared them for professional roles.
- Regular faculty review of course and program assessment data to identify trends in student performance.
- Employer surveys will identify strengths and weaknesses of data privacy job-related performance of graduates.
- Identify peer disciplinary programs to benchmark performance on key indicators (IPEDs) to identify best practices and areas for improvement.

Duplication and Competition

21. Do any related programs exist at other public universities in South Dakota?
A list of existing programs is available through the university websites and the RIS Reporting: Academic Reports Database. If there are no related programs within the Regental system, indicate ***none.***

There are no graduate degrees in Data Privacy offered by South Dakota Regental Institutions. Only our own (DSU) graduate certificate in Data Privacy addresses this disciplinary area. The courses in our Data Privacy Graduate Certificate include:

- INFA 742 - Ethics and Information Technology (3 cr.)
- INFA 702 - Data Privacy (3 cr.)
- INFA 722 - Data Privacy Management (3 cr.)
- INFA 726 - Data Privacy Technology (3 cr.)

Our MS and Ph.D. programs in Cyber Defense offer specializations in data privacy somewhat more technically oriented than the proposed degree program.

A. If yes, defend the need for an additional program within the state, Include IPEDS enrollment data and additional data as needed.

NA

B. If yes, would this program be a candidate for Regental system collaboration?

NA

22. Do any related programs exist at any non-Regental college or university within 150 miles of the university?
List those programs here:

We were unable to identify any graduate program within 150 miles of DSU with a focus on data privacy. The MSDP fills this gap, positioning DSU as a regional and national leader in this emerging cyber science sub-discipline. DSU does offer several related programs, including an MS Cyber Defense, graduate Data Privacy Certificate, and BS in Cyber Leadership & Intelligence.

A. If yes, use IPEDS to identify the enrollment in those programs.

NA

B. What evidence suggests there is unmet student demand for the proposed program, or that the proposed program would attract students away from the existing program?

NA

Market Demand

This section establishes the market demand for the proposed program (eg Regental system need, institutional need, workforce need). Use the following sources for your data:

- South Dakota Department of Labor & Regulation
- O-Net
- US Department of Labor Projections Central
- SDBOR Workforce and Degree Gap Analysis Report

23. What is the expected growth of the industry or occupation in South Dakota and nationally?
Include the number of openings, as well as the percentage of growth when possible.

The demand for information security and data privacy professionals is experiencing significant growth both nationally and within South Dakota.

National Outlook:
• Information Security Analysts: According to the U.S. Bureau of Labor Statistics, employment for information security analysts is projected to grow 33% from 2023 to 2033, which is much faster than the average for all occupations. This equates to about 17,300 job openings annually over the decade.
• Privacy Professionals. The International Association of Privacy Professionals, the leading organization for privacy professionals, reports steady growth in its membership over the past few years. Between 2020 and 2023, its membership increased from 50,000 to 75,000. Moreover, the group reports a 30% year-on-year increase in demand for privacy pros with many candidates being placed in a week and receiving three job offers on average.

Driving Factors:
• Regulatory Compliance: Organizations require privacy professionals to navigate and comply with a complex landscape of data protection laws, such as the California Consumer Privacy Act (CCPA), the General Data Protection Regulation (GDPR) in Europe, and the China Personal Information Protection Law. Additionally, privacy laws are in constant flux as policymakers enact new laws to address rapidly changing information technologies and threats. It falls to privacy professionals to educate companies on these changes and to revise data compliance programs and processes in response to legal reforms.
• Cybersecurity Threats: The persistent threat of cyberattacks necessitates privacy professionals to help organizations develop data governance strategies and build a privacy-focused culture. Privacy professionals play a crucial role in developing and implementing strategies to protect personal data and maintain consumer trust.

National Salary Overview:
• Privacy Professionals: The average annual salary for privacy professionals in the United States is approximately $81,661, with a typical range between $69,505 and $93,909. https://www.salary.com/research/salary/hiring/privacy-professional-salary/?utm
• Data Privacy Analysts: These professionals earn an average of $84,200 per year, with salaries typically ranging from $72,900 to $97,500. https://www.salary.com/research/salary/alternate/data-privacy-analyst-salary?utm
• Chief Privacy Officers: As senior executives, chief privacy officers have an average salary of $206,000, reflecting their extensive responsibilities and experience. https://iapp.org/resources/article/salary-survey-summary/?utm

24. What evidence, if any, suggests there are unfilled openings in South Dakota or nationally?

Specialized training and knowledge are needed for the position of privacy professional. The job titles for privacy professionals include:
Privacy Manager
Privacy Specialist Privacy Officer
Privacy Program Manager
Privacy Analyst
Governance Risk and Compliance Manager Data Protection Officer

Data Privacy Analyst
Data Privacy Manager Data
Privacy Auditor
Cyber Legal Advisor

South Dakota Outlook:

- Information Security Analysts: According to the U.S. Bureau of Labor Statistics, employment for information security analysts is projected to grow 33% from 2023 to 2033, which is much faster than the average for all occupations. This equates to about 17,300 job openings annually over the decade. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
- High-Demand Occupations: The South Dakota Department of Labor & Regulation's Labor Market Information Center identifies "Hot Careers" based on high demand and high wages. While specific data for data privacy experts is not detailed, the increasing reliance on digital infrastructure across various industries suggests a growing need for information security and data privacy professionals within the state. https://dlr.sd.gov/lmic/menu_hot_careers.aspx?utm_source=chatgpt.com

At a DSU-hosted roundtable on May 3, 2024, Senator John Thune highlighted the growing economic and security implications of data privacy for both South Dakota and the nation. He noted that the patchwork of US state laws, along with expanding global privacy regulations, is increasing the compliance burden on companies, many of which are now hiring personnel to manage these new demands. Business leaders from the state echoed Senator Thune's comments during the roundtable discussion. Job postings for privacy professionals further support his points, with more than 6,300 open positions for privacy officers currently listed on ZipRecruiter (https://www.ziprecruiter.com/Jobs/Privacy-Officer).

Health care and financial services, two industries that prioritize data privacy, are major contributors to South Dakota's economy. They will likely provide steady job openings for privacy professionals. Additionally, the Governor's Office identifies manufacturing, bioscience, and cybersecurity as "key industries" in South Dakota (https://sdgoed.com/key-industries/). In these industries, the need to protect intellectual property, client data, and other sensitive information will also likely create local openings for privacy professionals.

Nationally, both the private and public sectors will increasingly seek privacy specialists. Tech and tech-adjacent firms will likely be major employers in this field, given the compliance and cybersecurity challenges they face. At both the state and federal levels, privacy regulators will be needed to ensure that firms follow data privacy laws.

25. What salaries can program graduates expect to earn in South Dakota and nationally?

While specific data for privacy professionals in South Dakota is limited, related roles provide insight into potential earnings:

- Data Analysts: In South Dakota, data analysts earn an average salary of $75,982 per year, with total pay estimated at $97,299 when including additional compensation such as bonuses. https://www.glassdoor.com/Salaries/south-dakota-data-analyst-salary-SRCH_IL.0%2C12_IS1502_KO13%2C25.htm?utm

- HIPAA Privacy Officers: These professionals have an average annual salary of $35,570 in South Dakota, with a typical range between $32,730 and $39,784. https://www.salary.com/research/salary/recruiting/hipaa-privacy-officer-salary/sd?utm

Given the specialized nature of data privacy roles and the increasing demand for such expertise, graduates can expect salaries that are competitive and often exceed national and state averages. It's important to note that salaries can vary widely based on specific job functions, industry sectors, and individual qualifications.

26. Optional: Provide any additional evidence of regional demand for the program.
e.g. prospective student interest survey data, letters of support from employers, community needs...

Student Demand

27. Provide evidence of student completers/graduates at that degree level at peer institutions that offer the same/similar program using data obtained from IPEDS.

Peer Institution: Regional and Competitive institutions. Choose programs not already listed in question 11. Use the most recent year available.

University Name	State	Program Name	Number of Degrees Conferred in Program	Total Number of Conferrals at Level (Undergrad or Grad)
Georgia Institute of Technology	GA : Georgia	MS Cybersecurity - Policy Specialization	285	6610
University of Texas at Austin	TX : Texas	MS Information Security & Privacy	28	3390
Carnegie Mellon University	PA : Pennsylvania	MS Privacy Engineering	143	4339

28. What evidence suggests there is interest from prospective students for this program at the university?

A. Cyber Leadership and Intelligence undergraduate major as a feeder program to this proposed degree program.

In the fall 2018, Dakota State University admitted its first students in the Cyber Leadership and Intelligence (CLI) Bachelor of Science program. This undergraduate degree prepared students to work with government, business, and industry leaders to defend those organizations from cyber disruption. CLI is an interdisciplinary program that capitalizes on DSU's depth of expertise in cyber and computer science while engaging students in international policy, regulation, and human behavior. Though we intend for applicants to the MSDP to come from a range of undergraduate degrees, the CLI program will be a primary undergraduate feeder program, from which we will create an accelerated MSDP path. This should not noticeably impact matriculation from the CLI program to other graduate programs. There is a relationship between the MS Cyber Defense "non-technical" specialization and the CLI program, however, even the non-technical specialization requires a strong foundation in computer science and that is not built into the CLI program. Only CLI students with a double major or minor in computer science would be eligible for acceptance into the MS Cyber Defense. The proposed MS in Data Privacy is a much more aligned transition for most students in the CLI program, as the proposed program content is less technical.

B. Data Privacy Graduate Certificate.

In 2021 data privacy DSU proposed its first unique system courses in data privacy including Data Privacy (INFA 702), and Data Privacy Management (INFA 722). The following year a data privacy specialization in the Cyber Defense MS program and a graduate certificate (12 credit hours) in Data Privacy, have thrived.

C. Path for Non-Technical Majors.

The program leverages DSU’s strengths in cyber sciences, capitalizing on its status as a CAE designated by the National Security Agency (NSA) and Department of Homeland Security (DHS). While all DSU majors prepare their students to be technological leaders in their field, some students with undergraduate degrees in fields such as marketing, healthcare management, or international relations seek a more immersive computer science experience. These students, and those from other institutions will be ideal candidates for this program. They will receive coursework that provides an operational understanding of the computer network environment where data resides. This training will equip them with knowledge of the cyber science environment necessary to communicate effectively with technical experts who manage network systems, while they focus on organizational and public policy issues in the Policy and Governance Specialization.

D. Redirected applications.

A growing proportion of MS applications to the Beacom College of Computer and Cyber Sciences are denied entry into our computer science, artificial intelligence, or cyber defense programs due to their lack of computer science or similarly related Undergraduate coursework. An analysis of these denials shows that 60-70% would be suitable candidates for the MSDP. With a record of these denials former and future applicants will be given the opportunity to consider a new path into the cyber security work force through data privacy training.

Enrollment

29. Are students enrolling in this program expected to be new to the university or redirected from existing programs at the university?

Students enrolling in the Master of Science in Data Privacy degree program are expected to be new arrivals to graduate education at Dakota State University. These are students looking for an immersion in legal, ethical, social, and policy issues required in a workplace that faces increasing challenges in global data usage and protection. This program is designed to be accessible from a wide variety of backgrounds and disciplinary majors. The curriculum is designed to equip students with the necessary skills they will need to interact with professionals from a technical security background.

Students with a more systemic knowledge of computing systems including operating systems, software, and hardware architecture may also apply to this program, or choose to address data privacy in a more technical way through offerings in our Master or Doctoral programs in Cyber Defense.

30. Complete the enrollment worksheet to provide an enrollment projection for the next six academic years

Worksheet Completed	Yes

31. What is the minimum number of students required in this program to break even, with respect to the budget?

20

32. Discuss the assumptions informing your enrollment estimates.
(e.g. current enrollment and trends in similar programs, IPEDS data, recruitment strategies, partnerships)

Developing a graduate program in data privacy presents unique challenges due to limited reference data in IPEDS, prompting us to lean on historical trends and the performance of related programs to inform our projections. Several key factors support our enrollment estimates for the MSDP:

- Undergraduate Pipelines: DSU's bachelor's degrees in Cyber Leadership & Intelligence (CLI), Network and Security Administration (NetSec), and Computer Information Systems (CIS) form robust pipelines into the MSDP. CLI students build expertise in policy, law, and intelligence; NetSec students acquire technical skills in network security, defensive hacking, forensics, and penetration testing; and CIS students blend strong technical training with critical business insights. Together, these programs equip students with the foundational knowledge that aligns directly with the MSDP's focus on privacy, governance, and cybersecurity policy, ensuring they are well-prepared to contribute to emerging cybersecurity initiatives.

- Graduate Program Momentum: The sustained enrollment growth in DSU's Master of Science in Cyber Defense (MSCD) demonstrates strong demand for advanced, security-focused education, while the robust interest in the Master of Science in Analytics and Applied Artificial Intelligence (MSAAAI) and the Master of Science in Information Systems (MSIS) underscores the market's need for comprehensive expertise in both technical and strategic aspects of cybersecurity and data governance. These programs attract a diverse range of professionals—from technical experts to non-technical, information-adjacent practitioners—further validating our enrollment projections for the MSDP.

- Students from outside DSU will be drawn to the MSDP because it fills a critical gap in advanced data privacy education by offering a distinctive, interdisciplinary curriculum that blends cybersecurity policy, governance, and practical applications. While many traditional programs focus solely on deep technical skills, the MSDP is uniquely designed for professionals from diverse backgrounds—such as law, business, and public policy—who seek to develop the strategic and regulatory expertise necessary to protect sensitive information. With data breaches and privacy concerns escalating globally, this program meets the growing demand for leaders who can navigate complex compliance issues, manage data governance, and implement effective privacy strategies, making it an attractive option for those looking to advance their careers in a rapidly evolving field.

33. If projected program enrollment is not realized in year two, what actions is the university prepared to take?

The university will seek to be proactive in identifying the environmental factors that are contributing to the gap between estimated and actual enrollments. If enrollment fails to meet estimates, we prepared to take the following actions:

- Engage Industry Expertise: Bring enrollment concerns before various Industry Advisory Boards. For example, the CLI Advisory Board—an active board composed of privacy industry specialists and leaders in data privacy and cyber intelligence that regularly advises the DSU CLI undergraduate program—was consulted twice during the conceptualization of the MSDP. Additionally, the Beacom College Industry Advisory Board has also been actively engaged in the program's development and has affirmed the critical need for this initiative.

- Leverage Existing Pipelines: To address any enrollment challenges, DSU will leverage the NetSec program by directly targeting its graduates through tailored outreach campaigns that emphasize the seamless transition to the MSDP. Given their expertise in securing and managing networks, NetSec graduates are well-positioned to build on their skills by mastering the privacy and policy components of organizational data protection. The university will also highlight the value of dual-degree options (such as the accelerated 4+1 pathway) to attract students interested in pairing network security expertise with data privacy specializations.

- Capitalize on Program Success: In addition to internal pipelines from CLI and NetSec, DSU will underscore the established reputations and success of our CIS, Master of Science in Information Systems (MSIS), and Master of Science in Analytics and Applied Artificial Intelligence (MSAAAI) programs. By showcasing the alignment of these programs with the interdisciplinary focus of the MSDP, and leveraging their strong alumni networks, we can attract a broader range of prospective students from both technical and non-technical backgrounds. The university will also highlight the value of dual-degree options (such as the accelerated 4+1 pathway) to attract students interested in pairing network security expertise with data privacy specializations.

- Incorporate Student Feedback: Engage current students in dialogue (via focus groups) to gather insights on the program features they find most appealing and to identify any perceived barriers to application, using this feedback to make targeted program adjustments.

- Collaborate Internally: Engage faculty, enrollment counselors, department chairs, and other internal stakeholders in analyzing potential factors influencing enrollment and identifying strategic solutions. Revise Marketing Strategies: Undertake a comprehensive review of our marketing strategy, adjusting recruitment tactics, media formats, and digital platforms as necessary to improve outreach and engagement.

- Adjust Delivery Modes: Consider modifications to program delivery methods (including on-campus options) to appeal to international students and other non-traditional learners.

- Learn from Peers: Reach out to peer institutions implementing similar programs and engage with their leadership to gather insights and best practices.

- Align with Industry Certifications: Explore the possibility of aligning the degree program with industry certifications offered by the International Association of Privacy Professionals (IAPP), such as Certified Information Privacy Professional (CIPP), Certified Information Privacy Technologist (CIPT), and Certified Information Privacy Manager (CIPM), thereby enhancing the program's value proposition.

34. Discuss the marketing and recruitment plan for the program

Include information on partnerships and pipelines (e.g. articulation agreements with BOTE, collaboration with partner university, community partnerships).

The MSDP joins a small but distinctive catalogue of graduate degree offerings at an institution nationally recognized for its computer and information sciences expertise, one prevailing area of which is cyber security. It is on that foundation that student recruitment embarks. Highlighting the distinctive features of an advanced

degree in data privacy discussed in this proposal, well-honed, and audience tailored marketing messages scale on five dimensions.

1) On Campus.

DSU's undergraduate programs provide a natural pipeline into the MSDP, with a focus on strategic 4+1 Accelerated Degree pathways and targeted outreach:

- CLI – Policy and Governance Feeder Program.

The CLI undergraduate degree shares a strong conceptual alignment with the MSDP, particularly in policy, governance, and intelligence applications of privacy. To streamline the transition, we will develop a 4+1 pathway, allowing CLI students to complete three graduate courses (9 credits) during their undergraduate studies, accelerating their path to a master's degree.

- NetSec – Technical Feeder Program

The Network and Security Administration program is the most technically aligned undergraduate pathway to the MSDP, with its focus on network security, intrusion prevention, and defensive hacking—all integral to effective data privacy and governance. We will establish a 4+1 pathway, enabling NetSec undergraduates to seamlessly progress into the MSDP. Additional recruitment efforts will target students with minors in CLI, cybersecurity, or related fields, emphasizing how combining technical expertise with policy-focused privacy education prepares them for leadership roles in data privacy management.

- CIS – Business & Technical Feeder Program: DSU's CIS program is uniquely positioned as a feeder into the MSDP by blending robust technical training with essential business acumen. This interdisciplinary approach equips students with the ability to analyze, manage, and secure data while understanding its strategic business implications. We will explore a 4+1 pathway for CIS students, facilitating an accelerated transition into the MSDP and broadening the talent pool for future data privacy leaders.
- Additional 4+1 Pathway Opportunities: Beyond the dedicated pipelines from CLI, NetSec, and CIS, other strong candidates for 4+1 pathways include undergraduates pursuing degrees such as Business Analytics, Computer Science, Cyber Leadership and Intelligence, Health Informatics and Information Management, and Individualized Studies. These programs provide a blend of technical acumen, analytical rigor, and interdisciplinary perspectives that are essential for addressing complex data privacy challenges, ensuring that graduates are well-prepared to excel in the MSDP.

2) Alumni.

- Direct contact with graduates of the CLI program explaining how the MSDP builds on their undergraduate program degree. Develop similar message for graduates with CLI adjacent majors.
- Outreach to NetSec alumni will highlight how the MSDP builds on their knowledge of network configuration and security by introducing them to broader privacy, governance, and regulatory concepts. This will include messaging about career advancement opportunities in high-demand privacy roles, supported by testimonials from industry leaders.
- Direct contact with students who have completed the Data Privacy Certificate and define how they can use their certificate course work towards the completion of the MSDP program.
- Ph.D. and MS programs in Cyber Defense and Cyber Operations at DSU have attracted current or former students to roles such as Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Digital Officer (CDO), Chief Data Officer (CDO), Chief Information Security Officer (CISO). Outreach to these leaders will encourage them to engage MSDP to candidates within their organizations.

3) Partnerships and Collaborations.

- Outreach to audiences among relevant partners which will include, but not be limited to: the Midwest Student Exchange program (MHEC), Western Regional Graduate consortium (WRGP/WICHE); the Swedish Defense University/AI Sweden, Johns Hopkins University Applied Performance Lab (JHUAPL), Korea University's Seoul Media Institute of Technology (SMIT); Heatherington Group; the National Security Agency National Center of Academic Excellence Cybersecurity (NCAE-C) Program.
- Collaborations with key partners, including the Beacom Industry Advisory Board, network administration employers, and external cybersecurity partners, will emphasize the relevance of NetSec graduates transitioning into privacy-focused roles through the MSDP. Additionally, industry-specific outreach (e.g., healthcare, finance, government) will showcase how network security professionals with privacy expertise are highly sought after.

4) Targeted Recruitment.

- Paid search lists from Educational Testing Services (ETS) focusing on data privacy aligned degree holders

expressing interests in information privacy and security.

- Program promotion via email, listservs and/or digital dissemination practices with industry groups such as DirectTrust Health Alliance and EClinicalWorks in the healthcare field, the Financial Industry Regulatory Authority (FINRA) in Banking, and professional organizations including the Information Systems Security Association (ISSA), and the International Association of Privacy Professionals (IAPP).

5) Social Media.

- In Linked-In, Google Ads, Facebook Ads; Twitter, Instagram, etc.
    - Generate campaigns highlighting how the program can advance careers in data privacy, compliance, and policy—funneling to application portal.
    - Launch campaigns leading back to testimonials on the DSU website from alumni or industry leaders about the demand for privacy professionals—funneling to application portal.

Financial Health

35. Complete the budget worksheet to provide a budget projection for the next six academic years.

Worksheet Completed	Yes

Financial Health Summary						
	1st FYxx	2nd FYxx	3rd FYxx	4th FYxx	5th FYxx	6th FYxx
Tuition & Fee Revenues	61102	146645	213858	238299	281070	281070
Program Expenses	77528	57528	115056	115056	115056	115056
NET	-16426	89117	98801	123242	166014	166014
Other Supporting Revenues						
NET (Other)	13993	89117	98801	123242	166014	166014

36.Explain the amount and source(s) of any one-time and continuing investments in personnel, professional development, release time, time redirected from other assignments, instructional technology and software, other operation and maintenance expenses, facilities, etc., needed to implement the proposed major.
Address off-campus or distance delivery separately.

The proposal contains provisions for instructional computing tools and applications, and faculty professional development travel in year four. If enrollment projections hold and additional sections of courses are required, a new hire is anticipated in year four.

37. If new faculty are not requested, describe how existing faculty will be utilized and indicate whether this action will impact other existing programs.

Courses will be taught by program faculty and adjuncts in years 1-3, with adjuncts back-filling in program faculty workload on Data Privacy course delivery.

38. Is the university requesting or intending to request permission for a new fee or to attach an existing fee to the program?.

Requesting Permission for Fee?	Yes, existing fee
Explanation	No new fee is requested. However, the university requests approval to assign the existing INFA and HIM discipline fees to courses with those prefixes within the program for onsite offerings, and the Non-Resident Online Computer Science, Cyber Operations, & Network and Security Administration fee to courses with those prefixes within the program for online offerings.

39. Use the table below to describe potential risks to the program's implementation over the next four years.
For each risk, identify the severity (low, medium, high), probability of occurrence (low, medium, high) and the institution's mitigation strategy for each risk.

Risk	Severity	Probability	Mitigation Strategy
Faculty workload limitations/Faculty Availability	Low	Low	Review departmental capacity for variations in course delivery. Investigate possible roles for adjunct or emeritus faculty.
Underestimate interest in the program—low enrollment.	Medium	Low	More selective acceptance. Review full-time or adjunct hiring options.
Overestimate interest in the program	Medium	Medium	Engage on campus and off campus expertise in marketing strategy, program salience, course selection and composition.

External Review

40. If this proposal is for a graduate program, provide information below for at least five potential consultants who may be considered to conduct the external review.

Reviewer Name	Title	Institution
Margaret Smith, Ph.D. margaret.w.smith1@gmail.com/	Scientific Researcher, Assist. Professor	Army Cyber Institute West Point, New York, United States
Nathan Colaner, Ph.D., MBA colanern@seattleu.edu/206-296-5628	Teaching Professor, Management Program Director, Business Analytics	Seattle University, Albers School of Business and Economics
/		
/		
/		

Additional Information

41. (Optional) Use this space to provide pertinent information not requested above that may assist the Board in understanding the proposal.

Support letters from Senator John Thune, Dennis Eger from Army Intelligence, and D.C. Gillian, Cyber Leadership and Intelligence Advisory Board

Approvals

University Approval

To the Board of Regents and the Executive Director: *I certify that I have read this proposal, that I believe it to be accurate, and that it has been evaluated and approved as provided by university policy.*

President of the University	Date
Dr. Jose Marie Griffiths	4/24/2025

Academic Affairs, Provost	Date
Dr. Rebecca Hoey	4/24/2025

Finance and Administration, Vice President	Date
Dr. Stacy Krusemark	4/24/2025

Enrollment Management, Vice President	Date
Amy Crissinger	4/24/2025