Intent to Plan for a New Program
South Dakota Board of Regents
Academic Affairs Forms

Internal Ticket ID: 8992
Created: 5/30/2023
Modified: 10/11/2024

Use this form to request authorization to plan a new baccalaureate major, associate degree program, or graduate program; formal approval or waiver of an Intent to Plan is required before a university may submit a related full proposal request for a new program. The Executive Director and/or their designees may request additional information. After the university President approves the Intent to Plan, submit a signed copy to the Executive Director through the System Academic Officer through the proper process. Only post the Intent to Plan to the university website for review by other universities after approval by the Executive Director, System Academic Officer or designee. This form is meant to capture critical elements for stakeholders to review prior to a full proposal.

University	DSU - Dakota State University
Degree	MS : Master of Science
Name of Major	X999 : New Major Requested **Data Privacy**
Specialization Required?	Yes *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
Intended Date of Full Proposal	Fall 2025
Planned CIP Code	111003

Program Description

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

Dakota State University's Master of Science in Data Privacy prepares students to assess, track, and mitigate the evolving threats to data privacy and to understand the complex role that privacy plays in shaping online services. The program offers a foundation in the technical, policy and legal debates in privacy from a global perspective, and it examines the value that digital data represents to government, corporate, and nation-state actors. Additionally, the program explores topics in data privacy technology and management, equipping students with the necessary skills and awareness to assist entities in protecting their critical and sensitive information. Available electives are designed to build depth in technical, emerging technical, and policy areas including areas such as agriculture, finance, healthcare, and government. Courses will be accessible online to accommodate working professionals interested in this area of graduate study.

Strategic Impact

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

The Legislature established Dakota State University as an institution specializing in programs in computer management, computer information systems, and other related undergraduate and graduate programs as outlined in SDCL 13-59 -2.2. This mission is actualized in multiple colleges including the Beacom College of Computer and Cyber Sciences (BCCCS), which offers certificate and degree programs from the associate to the doctoral level in areas related to artificial intelligence, computer game design, computer science, cyber defense, cyber operations, and network and security administration; College of Business and Information Systems (BIS), which specializes in computer information systems; and the College of Arts and Sciences (A&S), which houses the Cyber Leadership & Intelligence, focusing on the legal, ethical, and political aspects of privacy.

The Master of Science degree in Data Privacy is an interdisciplinary effort administratively led by the BCCCS with integration of the Colleges of BIS and A&S. Because of the vast amounts of data collected by companies, governments, and services providers, students will need a foundation in information warehousing and data analytics. Technical measures for securing the privacy of data, including privacy enhancing technologies, digital forensics, technical testing tools, data governance, artificial intelligence, and advanced privacy technologies will involve course work offered in the BCCCS. The contributions of BIS focus on creating the levers of identity minimization and anonymization when large volumes of data are collected and stored, and in understand and application of the Health Insurance Portability and Accountability Act (HIPAA) and other national standards which require accountability in data handling practices. A&S addresses data sovereignty, regulatory compliance, E-Government, digital democracy, and related topics at the intersection of law, technology, and human rights. This integrative approach to data privacy study reflects the complex challenges involved with safeguarding critical and sensitive information. This is a mission-focused enterprise for Dakota State University.

Dakota State University's Strategic Plan ADVANCE 2027 identifies five pillars of institutional focus. The design and delivery of an MS degree in Data Privacy directly addresses two of these pillars over the five-year strategic plan timeline. Students prepared for emerging job opportunities in Data Privacy address a milestone of Pillar 1-Enhance Student Success to place 100% of students in employment within 6 months of graduation, and Pillar 5-Increase Enrollment through strategic program development.

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

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

The South Dakota Board of Regents has encouraged its member institutions to provide undergraduate and graduate programs that respond to the growing need in the ever-evolving computer science sector (BOR Policy 1:10:5) and provide high quality academic experiences for students that lead to high impact careers. (Board of Regents Strategic Plan 2022-2027, Goal 3: Academic Excellence, Student Outcomes, Educational Attainment, and Goal 4: Workforce and Economic Development). Since its commitment to Cyber Operations almost two decades ago (AY 2004-05) DSU has developed seven computer security-centric degree programs from the associate to the doctoral level, not to mention security focused certificate programs and specializations within majors and minors. The Master of Science in Data Privacy is a verification of DSU's commitment to develop opportunities in this branch of computer science.

Program Summary

4. 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 degree is not new to the university.

5. 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	015, Asynchronous	Fall 2025

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

6. 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.

Academic Quality

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

8. What program accreditation is available, if any?

None

9. Will the proposed program pursue accreditation or certifications?

No

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

Duplication and Competition

10. 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.

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

11. Do any related programs exist at any non-Regental college or university within 150 miles of the university?

List those programs here:

No related programs within designated radius.

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

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?

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

12. 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 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." (1) Because of increasing data threats and regulatory demands, the organization expects continued job growth in the field. The Bureau of Labor Statistics projects a 32% increase in job growth in the field of Information Security between 2022 – 2032, which it describes as "much faster than average." (2)

Two sets of pressures will drive job growth in the data privacy and information security sector. First, US-based firms need privacy professionals to help them understand and comply with an increasing number of privacy laws across multiple jurisdictions. Job ads for privacy professionals commonly require depth in the California Consumer Privacy Act, Europe's General Data Protection Regulation, and the China Personal Information Protection Law. Moreover, 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. It also falls on them to conduct ongoing privacy audits to ensure effective compliance.

Second, in the face of persistent cyber threats, organizations need privacy professionals to help them develop privacy plans and build a privacy-focused culture. Operating beyond the reach of US law enforcement, foreign threat actors have strong incentives and considerable opportunity to steal digital personal data. At the same time, consumers and users recognize the growing cyber threats they face and place greater demands on organizations to protect their digital personal data. Privacy professionals work in a variety of ways to ensure that firms prioritize privacy, so that they mitigate threats and satisfy customer demands. For example, they ensure that effective privacy measures are incorporated into product development and engineering systems, and they provide regular training sessions to personnel on privacy protocols and best practices.

1. https://data-privacy.io/data-privacy-career-prospects-in-2024/
2. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

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

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 (3).

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 (4). 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.

3. https://www.ziprecruiter.com/Jobs/Privacy-Officer
4. https://sdgoed.com/key-industries/

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

Because of the specialized training and knowledge needed to be a privacy professional, the salaries for these experienced positions typically exceed $100,000 per year and are likely to remain highly rewarding.

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

A search on the South Dakota Department of Labor's website reveals numerous jobs that have these or similar job titles. Interestingly, because the field of privacy professional is still relatively new, job ads often list relevant educational training as a requirement without specifying particular degrees. By developing a Master of Science in Data Privacy, Dakota State University has an opportunity to offer a degree that will establish an industry standard.

15. 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...

The table below shows the enrollments of three similar programs, two of which are previously referenced (see item #7). Using the NCES Integrated Post-Secondary Education Data System (IPEDS) three distinct years of program graduates are compared using the 'Computer and Information Systems Security/Auditing/Information Assurance' CIP group (11.1003). Other MS degrees addressing data privacy issues are found in law/legal studies programs without the technical skills DSU proposes to integrate in their proposal.

Program	Institution	Academic Year Completions		
		2020-21	2021-22	2022-23
Master of Science in Cybersecurity—Policy Specialization	Georgia Tech university	47	197	285
Master of Science in Information Security and Privacy	University of Texas at Austin	1	14	28
Master of Science in Privacy Engineering	Carnegie Mellon University	79	70	143

Student Demand

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

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)
Dakota State University	SD : South Dakota	MS Cyber Defense	32	145
Dakota State University	SD : South Dakota	Data Privacy Certificate	1	10
Dakota State University	SD : South Dakota	BS Cyber Leadership and Intelligence	11	350

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

In the fall, 2015 Dakota State University offered its first graduate coursework in the Master of Science in Information Assurance degree program. This program added to DSU's array of cyber security graduate options preparing students with technical and managerial competencies in software, database, and network security. In 2021 data privacy emerged from cyber security as a domain of study when DSU proposed its first unique system courses in data privacy including Data Privacy (INFA 702), and Data Privacy Management (INFA 722). By that time, a program name change to 'Cyber Defense" had been approved followed by a specialization and a graduate certificate (12 credit hours) in Data Privacy, the enrollments of which are shown below.

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 world cultures, international politics, and human behavior. Though we intend for applicants to the MS in Data Privacy to come from a range of undergraduate degrees, the CLI program is in close disciplinarily alignment.

Enrollment

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

Include the number of openings, as well as the percentage of growth when possible.

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.

19. Narrative Description of the preliminary estimates on annual enrollment in this program by year six

Include all students within the program, not just those new to the program.

The Master of Science in Data Privacy degree seeks to begin the delivery of course work in the Fall 2025 term, enrolling 10 students. An additional 5 students will be accepted for Spring, 2026 entry for a total enrollment of 15 students after the first year of program delivery. The program will seek to add 15 students annually in years 2-6. With a variable completion rate of 1-3 years for each student, the program will look to stabilize at a sustained enrollment level of 35-40 students.