

Privacy Program Charter

Charter documents the programs objectives, scope, and outputs. It also documents the value of the program by describing the problem/opportunity statement and quantifying the programs' benefits in the business case. It also lays out the parameters for its execution in terms of time and resource commitment.

Problem/Opportunity Statement

The role of the privacy officer is evolving as a profession in higher education, in part due to the number of data breaches, the ever-increasing amount of personal data collected by services and devices, the evolution of Big Data and Artificial Intelligence, and counter to these, the increase in data privacy protection laws and legislation at the local, state, and cross-boarder arenas. While privacy and security are closely related, they are distinct. An institution of higher education is more likely to have a dedicated Chief Information Security Officer than a Privacy Officer. As privacy programs mature, one best practice that has emerged for colleges is to be up front about the data they collect. Tarrant County College District (TCCD) decided to streamline its privacy protocols by creating a new office that would oversee privacy compliance across all five physical campuses and the one online campus.

Business Case (benefits of the program)

“To respond to new demands to protect student data, the education system would benefit from deploying a strategy that has been successful in other sectors and industries: hiring a chief privacy officer (CPO) who is responsible for the organization’s privacy policies and practices.

Once hired, the CPO should serve as a resource to staff, collaborate with the chief information security officer, cultivate privacy advocates, and respond to current events.”
(<https://cdt.org/wp-content/uploads/2019/01/Student-Privacy-Chief-Privacy-Officer-Issue-Brief.pdf>)

Goal Statement and Deliverables

The goal of the Privacy Office is to develop and implement policies designed to protect employee and customer data from unauthorized access. The Privacy Officer is a position within a post-secondary institution whose goal is to ensure that student, faculty, and parent privacy is maintained. With a target completion date of Spring 2024, the goals of TCCD’s new Privacy Program are as follows:

The office will establish privacy policies, notices, standards, and processes across the institution.

The Privacy Officer will conduct an audit of data collection, identify data stewards in primary roles.

A public-facing Privacy Website/portal at TCCD targeted to student data will be created, identifying departments that collect data, how data is used and stored, and under what agency or statute jurisdiction over privacy concerns may be redressed.

Working with Knowledge Management, Information Security, and Data Governance, the Privacy Office will establish a data classification for information at TCCD, a means to store the information in whatever ERP exists at the time.

A mechanism will be put in place for constituents to report and identify privacy concerns and issues utilizing the IT Service Desk via Team Dynamix.

The Privacy Officer will establish Privacy Training Curricula, in collaboration with TCCD's Organizational Excellence and Development (OED) division.

Project Scope

The Privacy Office has a series of responsibilities to the institution. An Educause Article published in 2015 on *The Chief Privacy Officer in Higher Education*, describes the scope of the responsibilities succinctly in five (5) sentences:

Establishing privacy policies, notices, standards, and processes with stakeholders across the institution.

Ensuring that the institution complies with applicable state, federal, and international laws, campus policies and procedures, and industry privacy standards.

Developing and managing privacy training, education, and awareness for students, faculty, and staff.

Advising and counseling campus constituents on best practices, new technologies, privacy complaints, and potential institution-wide risks.

Assisting with investigations and responses to campus privacy breaches or incidents.

Time and Resource Expectations

The Privacy Office is being launched with one full-time individual, initially. It is anticipated the Department will increase in personnel hired and scope of importance to the College in the next three to five years. The initial budget for the department and position is under the Department of Information Security.

Sponsor/Leader

Reporting to the Chief Technology Officer, the Privacy Officer is responsible for overseeing and operationalizing the privacy program, focusing on strategically enabling the College to deliver on its objectives in an increasingly regulated privacy landscape. Working with the Director of Information Security to ensure alignment between security and privacy compliance programs, including policies, practices, investigations, and acts as a liaison for all issues concerning privacy for the College. Working with the Director of Information Security to establish an ongoing process to track, investigate, and report inappropriate access and disclosure of personally identifiable information (PII). Working with and is supported by TCCD's General Legal Counsel.