

Institutional Data Council

Issue Decision Summary Report: *AggieMetrics* Access Responsibility

June 30, 2020

In spring of 2019, the Institutional Data Council (IDC) was consulted for an issue related to the stewardship of Office of Research (OR) data presented to campus stakeholders via *AggieMetrics*.

Access to certain sensitive data (under the stewardship of OR) in *AggieMetrics* had, upon first deployment of the platform, originally been restricted to specific campus leaders (defined via the general title of “university leadership”). However, OR had been fielding requests to expand access to *AggieMetrics* beyond the originally approved list of individuals. Given that expansion, the IDC was asked whether any policy or training existed broadly on campus, to ensure that all staff granted access to sensitive data would understand their legal and administrative responsibilities related to data and information security.

Throughout the spring and summer of 2019, the IDC consulted with relevant stakeholders. In addition to determining whether policy or training existed such as was described in the original inquiry, the IDC and its consultants raised and considered related questions. Some were specific to the issue at hand. For instance: *how should data stewards treat information related to a faculty person’s research award data?* Some were more broad, such as: *how do we build a stewardship model and an access approval process that considers the evolving landscape, and takes into account data “repositories” such as AggieMetrics?*

Regarding the original question posed, the IDC found that no general training was in place related to data and information security practices (distinguishable from the general purpose cyber-security training mandatory for all hires). Furthermore, in considering the related questions, the IDC found that existing policy language regarding data security rights and responsibilities (notably, language in the now expired IS-2) was insufficient for the current data sharing environment. To address these concerns, the IDC made three recommendations:

1. To clarify precisely what is meant by the term “university leadership” for the purposes of data governance on campus.
2. To adopt, for an interim period, a protocol wherein responsibility for data security of projects such as *AggieMetrics* be vested with members of the Chancellor’s Leadership Council and the Provost’s Leadership Council.

3. Over the long term, to develop and adopt “data-security” training, perhaps eventually akin (at the Davis campus) to the cyber security training required of all UC employees, that would help to educate the UC Davis community on their professional and legal responsibilities, as well as to field best practices associated with data security across higher education, the health system, etc.

These recommendations were transmitted to the Provost on April 14, 2020. On June 1, 2020, the Provost responded to the IDC with the follow decisions:

1. “University leadership” is constituted by the Chancellor and Vice Chancellors, with the Provost and Executive Vice Chancellor being the responsible individual for most institutional data.
2. With regard to granting access to individuals, a new process will be implemented that tracks access requests and approvals via a form, starting with the individual wanting access and ending with the Vice Chancellor to whom they eventually report. The individual will certify his or her understanding of the sensitive nature of AggieMetrics data and their responsibility for its security. The appropriate Dean, Vice Provost, or other senior administrator will also approve the request and agree to ensure the individual’s competence to maintain the data’s security. Finally, the appropriate Vice Chancellor, including the Provost and Executive Vice Chancellor for requests coming from schools, colleges or units overseen by a Vice Provost, will approve the request with his or her signature; the Provost and Executive Vice Chancellor may delegate final approval authority to Deans or Vice Provosts.
3. The IDC is charged with developing, in coordination with the UC Office of the President, more detailed plans for a campus-wide data security training that could eventually be required of all UC Davis employees, similar to the current training requirement for cybersecurity and other highly sensitive areas.