California Community Colleges

MEMORANDUM
February 15, 2023

DII 23-300-02 | Via Email

TO: Chief Executive Officers
Chief Information Systems Officer Association
Chief Business Officers

FROM: Valerie Lundy-Wagner, PhD, Vice Chancellor
Digital Innovation and Infrastructure (DII)

RE: AB 178 and After-Action Reporting

The 2022 Budget Act included Assembly Bill (AB) 178 allocates $25 million in ongoing funds to the California Community Colleges (CCCs) to improve, at both the local and system level, among other things, data security oversight, fraud mitigation, and information technology (IT) infrastructure. This funding will support investments in continuous, secure, and sustainable delivery of education. District eligibility for AB 178 funding requires submission of, among other things, After-Action Reports (AARs). This memo provides information about the context and purpose of these reports as well as when and how to submit them.

Context for After-Action Reporting

Like many two-year colleges nationally, nearly all CCC IT departments are chronically understaffed and underfunded. This is problematic for the continued delivery of education and services given the increase in bad actors in recent years. Ensuring districts have what they need for secure IT operations has been challenging given the California Community Colleges Chancellor's Office (Chancellor's Office) lack of visibility into local district and college organization and allocation of resources. This is further exacerbated by the limited resources made available to districts for the purpose of remedying IT-related challenges.

AB 178 simultaneously provides funding for IT and helps to establish a structure of engagement between the Chancellor's Office and districts that can ensure state funds are optimized in ways

that acknowledge and remedy gaps. District eligibility for AB 178 funding requires districts to submit the following:

- An annual cybersecurity self-assessment,
- Bi-annual remediation reports,
- Periodic fraud reporting, and
- After-Action Reports (or AARs)

Description of AARs

An AAR is used to organize and document feedback after a cybersecurity incident by summarizing what happened during the event, assessing the actions taken by groups or individuals affected by the incident, and describing areas for improvement. Specifically, the AAR will include the following five components:

1. **Incident Overview** - This includes a description of the incident, including what happened, when, and how.
2. **Analysis** – This describes what was observed during the incident in the context of what was expected to happen. It outlines the impact of the incident responders, affected user groups, and the system. The analysis will identify the incident response's strengths and areas needing improvement.
3. **Recommendations** - The analysis results in recommendations detailing actions and insight to correct or boost performance for future incidences.
4. **Improvement/action plan** - This will list corrective action steps and the parties responsible for completing them within a specific time limit. The action steps should include process improvements, revised procedures or documentation, training criteria, software or hardware changes, or other strategic planning needs.
5. **Conclusion** – This will summarize all report components and outline action items for follow-up by the appropriate incident response team member or stakeholder group.

AARs will, with other requested information, inform allocation decisions, surface systemwide lessons learned or best practices, and contribute to development of implementation and/or operational support for districts.

After-Action Reporting Requirements

Starting March 2023, districts are **required** to submit AARs within 90 days of the initial discovery of any cybersecurity incident that significantly disrupts the ability to provide services or results in a significant amount of Personally Identifiable Information (PII) being exposed. In general, this includes any incident that requires the engagement with the district's cyber insurance carrier or requires reporting to the California Attorney General (500 or more individuals impacted). For lessor incidents or those occurring since July 2022, the Chancellor's Office encourages submission of AARs as they can improve awareness of issues that be common across the system. Such information may also surface opportunities to identify and support local institutions.

To request an AAR form and report an incident, please contact the Chancellor's Office DII Technical Assistance Provider (TAP) Information Security lead, Stephen Heath at sheath@cccco.edu. AARs will be made available via the same reporting portal used to submit the fall 2022 cybersecurity self-assessment and January 2023 remediation reports.

In cases where an investigation persists beyond 90-days, districts may request an extension on the submission of an AAR in writing by contacting the Vice Chancellor.

For additional assistance related to the purpose and contents of AARs or your college or district's cybersecurity posture, please reach out to the Stephen Heath (sheath@cccco.edu). Any other questions or concerns related to the system's security strategy should be directed to me at vlundywagner@cccco.edu or 916-322-1928.

cc: Daisy Gonzales, Interim Chancellor

Lizette Navarette, Interim Deputy Chancellor
John Hetts, Executive Vice Chancellor
Marty Alvarado, Executive Vice Chancellor
David O'Brien, Vice Chancellor
Gary Bird, Information Technology Specialist II
Russell Grant, information Technology Specialist I