



Data Classification and Security Committee Charter

Background	<p>Caltrans Executive Board has identified the need to implement an enterprise-wide data governance framework to ensure consistency across the Department. Implementation of this framework requires development of a set of policies, procedures, and best practices as well as a hierarchical governance structure that can develop, approve, and implement the required solutions.</p> <p>The Caltrans Enterprise Data Classification and Security Committee (hereafter referenced as "Committee") is formed under the direction of the Enterprise Data and Geospatial Governance Board (hereafter referenced as "Board") which oversees the development and implementation of policy, standards and guidance for enterprise and geospatial data at Caltrans.</p> <p>The Committee is the authority responsible for classifying data as 1) corporate data; 2) sensitive, confidential, and/or personally identifiable information; 3) exempt from sharing due to an exception or restriction when the Business Data Steward is unsure of the classification or the classification is challenged by another party. The Committee is responsible for deciding what remediation is necessary to make data shareable on platforms like the CA Open Data Portal, if it is possible.</p> <p>The Committee reports to the Board with recommendations and solutions that prioritize data sharing while keeping Caltrans managed data safe and in compliance with all applicable data privacy and protection requirements. Decisions made by Committee are consistent with those made by the Enterprise Data Steward Committee (EDSC), Board, and Council.</p>
-------------------	--



Data Classification and Security Committee Charter

Purpose	<p>The Committee improves data protection, accessibility, and sharing of Caltrans managed data while respecting data security and privacy requirements. The Committee accomplishes this by providing expertise on how to classify data and provides clear guidance to data stewards and data custodians of their responsibilities related to data classification and security.</p> <p>The enterprise data and geospatial governance items the Committee may address include but are not limited to:</p> <ul style="list-style-type: none">• Providing subject matter expertise for the classification of data as corporate data, open data, sensitive, confidential, and personally identifiable information.• Reviewing data for redaction or restriction for the purpose of making it sharable.• Providing subject matter expertise on the value of data sharing to the public.• Providing subject matter expertise to the EDSC, Board, Council, other Caltrans management boards, Chief Information Officer, and Information Technology Governance Council, as required, on issues of mutual interest related to data classification and sharing.• Reviewing and/or developing new policies, or changes to existing policies.• Providing transparent, documented, and consistent action, and recommendations across all Caltrans divisions and districts related to data classification, security, and sharing.
Members	<p>The membership of the Committee consists of:</p> <ul style="list-style-type: none">• Enterprise Data and Geospatial Governance Program Manager (Chair – EDGG Program)• Homeland Security Liaison (Co-Chair – Homeland Security Branch, within the Division of Maintenance, Office of Recovery and Operations)



Data Classification and Security Committee Charter

	<ul style="list-style-type: none">• Specialist, Governance, Risk, and Compliance (Information Technology) <p>Each Committee member may request to include a non-voting temporary advisor in committee meetings to act as a subject matter expert when evaluating data brought for review.</p> <p>CTDATA staff will assist the committee with administrative work.</p>
Committee Leadership Roles	<p>Committee Chair – The Enterprise Data and Geospatial Governance Program Manager serves as the Committee Chair. Convenes and facilitates Committee meetings, communicates with the Geospatial Data Officer, ensures the Committee acts in a manner consistent with its roles and responsibilities, and facilitates implementation of Committee and Board decisions.</p> <p>Committee Co-Chair – The Homeland Security Branch Chief serves as the Committee Co-Chair. Fulfills any leadership roles for the Committee in the absence of the Committee Chair.</p> <p>Geospatial Data Officer – Serves as the Committee Sponsor. Supports the activities of the Committee, provides direction, champions proposals to the EDSC and Board, and assesses Committee performance.</p>
Frequency of Meetings	<p>Meetings will be quarterly or on an as-needed basis to review datasets that claim classification/de-classification as corporate data; sensitive, confidential, personally identifiable information; pose a risk to Caltrans or its employees; may be excepted from the state's open data policy. Additional meetings may be necessary if the Chair(s) have time-critical data security issues or data classification reviews to address, or if the EDSC, Board, or Council have an action item that requires the Committee to convene.</p>



Data Classification and Security Committee Charter

	<p>Attendance may be delegated to a level no lower than one organizational level below the Committee member the delegate is representing. Delegates shall act on behalf of the member with full proxy rights. The Committee Chairperson is responsible for scheduling meetings, developing meeting agendas, providing meeting notes and tracking action items.</p>
Roles and Responsibilities	<p>Responsibilities of the Committee include but are not limited to:</p> <ul style="list-style-type: none">• Act as subject matter expert on the topics of data sharing, data redaction, and open data.• Make the final determination of data classifications of 1) corporate data, 2) sensitive data, 3) confidential data, 4) PII, and 5) open data in coordination with the responsible Enterprise Data Steward, Business Data Steward, and Data Custodian.• Recommend specific actions to make a particular dataset broadly shareable that isn't initially classified as open data but could reasonably be modified to become compliant.• Review and provide feedback on policy and guidance related to data sharing, data redaction, and open data.• Develop and recommend for adoption policies, practices, and guidance related to data sharing, data redaction, and open data publishing.• Advise the EDSC and Board on development, adoption, and implementation of data and geospatial governance policy, standards, processes, guidance, and software as they relate to data sharing, redaction, and open data.• Ensure efforts are consistent with the mission, goals and principles adopted by the Board, EDSC, and Committee.• Provide regular updates about activities to the EDSC and Board.



Data Classification and Security Committee Charter

Reporting Structure Input to Board	<p>The Committee is sponsored by the Board and the Committee reports to the Council and Board about pertinent updates, practices, information to respective business areas, programs, and districts</p>
Decision Process	<p>Decisions made by the Committee will be made by simple majority vote. Once a vote has been made, members are expected to support it and work together to implement it effectively. In case of a tie the Geospatial Data Officer, or their assignee, will cast a vote.</p> <p>A Committee member may call for the committee meeting, or a portion thereof, to be made "closed door" for discussion of sensitive, confidential, or other topics related to the item(s) brought to the Committee. Voting shall not occur in closed door meetings.</p> <p>The Homeland Security Branch Chief may override a vote to share data, if they have national security concerns that the data would pose a risk to Caltrans, its employees, or the public if shared. Documentation of the risk(s) must be shared with the Committee, if possible, and kept confidential if necessary.</p> <p>Any member of the Committee may ask for a deferment to the Chief Information Security Officer (CISO) for review. The CISO will then make the final classification and risk assessment for the data. Documentation of the CISO's classification and risk assessment must be shared with the Committee, if possible, and a record of the decision made available in the Corporate Data Catalog.</p>
Process Timeframe	<p>It shall take less than 20 business days (1 calendar month) for the Committee to meet, confer, and vote on classifying a dataset, once the datasets Data Classification and Security checklist and supporting data documentation has been submitted for review. The requestor may ask the Committee Chair for an ad-hoc meeting to be called for expedited review.</p>



Data Classification and Security Committee Charter

Record Keeping	<p>All meetings will be recorded via form notes and may be recorded using virtual meeting software. Voting records will be kept as part of these notes, along with any formal statements, if requested. Final recommendations by the Committee will be stated in narrative form in the meeting notes. If the justification for the Committees decision is classified or sensitive, the notes may be redacted.</p> <p>Form notes from the Committee that result in the classification of data as corporate data; sensitive, confidential, and/or personally identifiable information; pose a risk to Caltrans or its employees; may be excepted from the state's open data policy must be linked to the corporate data catalog entry for the dataset.</p>
Amendment	<p>This Charter shall be revisited, and updated as needed, by a simple majority vote of the Committee, at the request of the Board, or at the discretion of the Geospatial Data Officer.</p>



Caleb McCallister

02/24/2025

Ben Nguyen

02/24/2025

Anthony Flores

02/24/2025

Sponsor Approval

Chad Baker

02/24/2025

Rev. 0 - 2/2025

Data Classification and Security Committee Charter v0


Final Audit Report

2025-02-24

Created:	2025-02-24
By:	Caleb Mccallister (s143583@dot.ca.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAWaHYAa3Qa7SysHH4tgsG3_UuGEyohBFR

"Data Classification and Security Committee Charter v0" History

-  Document created by Caleb Mccallister (s143583@dot.ca.gov)
2025-02-24 - 4:27:27 PM GMT- IP address: 149.136.17.253
-  Document emailed to Ben Nguyen (ben.nguyen@dot.ca.gov) for signature
2025-02-24 - 4:30:30 PM GMT
-  Email viewed by Ben Nguyen (ben.nguyen@dot.ca.gov)
2025-02-24 - 4:53:39 PM GMT- IP address: 149.136.17.246
-  Document e-signed by Ben Nguyen (ben.nguyen@dot.ca.gov)
Signature Date: 2025-02-24 - 5:43:50 PM GMT - Time Source: server- IP address: 149.136.17.246
-  Document emailed to Anthony Flores (aj.flores@dot.ca.gov) for signature
2025-02-24 - 5:44:10 PM GMT
-  Email viewed by Anthony Flores (aj.flores@dot.ca.gov)
2025-02-24 - 5:48:10 PM GMT- IP address: 149.136.17.252
-  Document e-signed by Anthony Flores (aj.flores@dot.ca.gov)
Signature Date: 2025-02-24 - 5:49:12 PM GMT - Time Source: server- IP address: 149.136.17.252
-  Document emailed to Caleb Mccallister (caleb.mccallister@dot.ca.gov) for signature
2025-02-24 - 5:49:14 PM GMT
-  Email viewed by Caleb Mccallister (caleb.mccallister@dot.ca.gov)
2025-02-24 - 5:58:25 PM GMT- IP address: 149.136.17.253
-  Document e-signed by Caleb Mccallister (caleb.mccallister@dot.ca.gov)
Signature Date: 2025-02-24 - 5:58:47 PM GMT - Time Source: server- IP address: 149.136.17.253

 Document emailed to Chad Baker (chad.baker@dot.ca.gov) for signature

2025-02-24 - 5:58:49 PM GMT

 Email viewed by Chad Baker (chad.baker@dot.ca.gov)

2025-02-24 - 9:01:56 PM GMT - IP address: 149.136.17.250

 Document e-signed by Chad Baker (chad.baker@dot.ca.gov)

Signature Date: 2025-02-24 - 9:02:39 PM GMT - Time Source: server- IP address: 149.136.17.250

 Agreement completed.

2025-02-24 - 9:02:39 PM GMT



Powered by
Adobe
Acrobat Sign