PACICC | SIMA

Property and Casualty Insurance Compensation Corporation

Société d'indemnisation en matière d'assurances IARD

Data Governance Policy

August 2025

Statement of Purpose

For PACICC, the term confidential Member Data ("Data") refers to collections of Data elements provided to the Corporation by Members or Regulators and relevant to the operations, resolution planning activities, and/or Member/Industry solvency monitoring efforts of the Corporation.

The purpose of the Data Governance Policy is to set out the guidelines and procedures that will ensure that PACICC achieves the following:

- Clear accountability for who will have access to the Data, and for what purposes
- Strict security for handling of the Data, including maintenance of confidentiality and multiple layers of security against loss or inappropriate access
- Protection of the integrity of the Data, ensuring the accuracy, timeliness, and quality of information available for decision-making.

PACICC is a not-for-profit organization whose primary activities are not commercial in nature. Therefore, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) generally does not apply. Additionally, the Data that PACICC collects is primarily aggregate, company-level information rather than personally identifiable information (PII). Nonetheless, PACICC remains fully committed to safeguarding the protection and security of Member Data.

---

1. Data Governance Structure

The Data Governance Policy defines the measures which will be taken regarding information made available to PACICC by Members and Regulators. It ensures that any and all proprietary information provided by Members or Regulators, and which is not otherwise publicly available, will not be shared with other Members or outside of the organization. This means that the governance structure for such Data is primarily overseen by Management and access to such information is – except in special circumstances – restricted to Staff only.

Special circumstances are defined as cases where Members are deemed to be on the PACICC Watchlist and/or are subject to distress and Regulators have given PACICC authority to see a broader range of financial information. In these circumstances, this Data can be shared with PACICC's Pre-Insolvency Regulatory Liaison ("PIRL") Committee (comprising Non-Industry Directors).

Access to confidential information is coupled with the responsibility to adhere to the applicable Policy that governs its use. PACICC's Data Governance program applies to all Staff, who are expected to strictly adhere to the procedures defined within this Policy. Oversight of compliance with this Policy will be a defined accountability of the President and CEO, and overseen by the PIRL Committee, which will confirm Staff's adherence to this Policy annually to the Board.

The Data Governance Policy and any subsequent updates are reviewed by the Governance & HR Committee and recommended for approval by the Board.

2. Overview of Roles and Responsibilities for Governing Data

Role: PACICC's Vice President, Finance

Key responsibilities within Data program:

- **Strategic Oversight:** Develop and implement the organization's Data strategy. Lead the formulation of Data policies and foster a Data-driven culture
- **Data Governance:** Ensure Data quality, integrity, and security. Oversee compliance with Data guidelines and procedures, as outlined in this Policy
- **Innovation and Insights:** Drive the development of Data analytics and business intelligence solutions. Leverage Data to provide strategic insights and support decision-making
- **Policy Compliance:** Develop, implement and monitor the organization's control framework – ensuring compliance with this Policy
- **Control Environment Assessment:** Present a summary of the organization's compliance with the Policy at least bi-annually (including the assessment of the control environment) to the PACICC Board.

Role: PACICC's Manager, Operations

Key responsibilities within Data program:

- **Technology Sourcing:** Lead the efforts to source vendor IT solutions
- **Technical Implementation:** Install, configure, and maintain systems/software
- **Access Management:** Manage user roles, permissions, and security protocols
- **Operational Troubleshooting:** Identify and resolve technical issues, monitor performance, manage backups and provide technical support to end-users.

Role: PACICC Staff

Key responsibilities within Data program:

- Ensure compliance with all guidelines and procedures set forth in this Policy
- Operate in accordance with the controls outlined within the Appendix.

Role: PACICC's Governance & HR Committee

Key responsibilities within Data program:

- The PACICC Data Governance Policy and any subsequent revisions will be reviewed and recommended for approval by the Governance & HR Committee.

Role: PACICC's PIRL Committee

Key responsibilities within Data program:

- Staff compliance with the procedures as outlined within this Policy will be monitored by the PIRL Committee. The Committee will confirm Staff's compliance with this Policy to the Board.

Role: PACICC's Audit & Risk Committee

Key responsibilities within Data program:

- The review of test results and the remediation of findings (if applicable) stemming from a Data/IT internal audit or any other applicable review will be monitored by the Audit & Risk Committee, with escalation to the Board if necessary.

Role: PACICC Board

Key responsibilities within Data program:

- The PACICC Data Governance Policy and any subsequent revisions will be approved by the Board upon recommendation of the Governance & HR Committee.
- Oversight of Staff compliance with the Data Governance Policy – through the annual review of Staff and/or Committee attestations and any issues escalated to the Board.

3. Data Classification

Public: Publicly available information refers to Data that is accessible to the general public without any restrictions. This includes information that is published in public records, Government/Regulator databases/websites, Member Insurer websites, press releases, academic publications, and other open sources. Public information is not subject to confidentiality agreements or privacy protections, making it freely available for anyone to access, use, and share.

Confidential: All Financial and Regulatory information submitted to PACICC, that is not considered to be information generally available to the public, is classified as confidential for handling purposes. For more specificity, the following categories of information are regarded as confidential and classified:

- Financial information (P&C-1, P&C-2, P&C-3, P&C-4 and P&C-Prov) which is provided to PACICC by a Member Insurer, but which is not otherwise publicly available
- Financial information provided to PACICC by a Member Insurer as a result of a specific request (e.g. Appointed Actuary Report (AAR), Detailed information about unearned premiums and Financial Condition Testing Report (FCT))
- Regulatory information provided to PACICC by a Member Insurer regarding their Earthquake Loss Exposure (e.g. Earthquake Loss Exposure Data Form (OSFI659) or PACICC's Designated Earthquake Loss Exposure Data Form) unless that information is otherwise publicly available.

Confidentially classified information is restricted for use within its defined purpose by Staff, and is not intended for use by other Members, Industry Directors of the PACICC Board, or the public. In cases where Data is considered to be more highly sensitive, confidentially classified information may be restricted to a subset of PACICC Staff as determined by PACICC's President and CEO.

4. Data Privacy & Security

To ensure effective Data Privacy and Security protocols over Member's proprietary information, precautionary steps will be taken, and appropriate assessments will be performed, to confirm that adequate end-to-end encryption and access controls exist on any and all IT solutions leveraged to handle the transmission of Member information, and to protect against unauthorized access or Data leakage.

To achieve this, PACICC will:

- Implement and maintain a Data Sharing Portal for transfer of Data that meets users' needs, is reliable and has a high level of security
- Ensure that all files transferred from Members to PACICC will be acquired through a secure Data Sharing Portal. Access to the Portal will be strictly monitored, as per steps defined in Section 5 of this Policy. If a Member's/Regulator's IT/Compliance processes restrict the usage of a Data Sharing Portal, Data may be provided via an alternate method that is agreed to by both parties
- Provide appropriate training to all Staff and Member/Regulator Staff who will be involved in the process of transferring information to, or managing information within the Data Sharing Portal
- Store Data in a secure LAN/Shared Drive accessible only to Staff on a "need-to-know" basis, if and as Data is transferred from the Data Sharing Portal for analysis purposes. At all times, access will be monitored as per steps defined in Section 5 of this Policy. The secure Shared Drive and associated platform will be subject to all regular PACICC security protocols
- Escalate any security breach/incident (whether discovered by Staff or its IT Service provider) to PACICC's President and CEO, and, if Member Data was compromised and accessed outside of its permitted usage (defined below in Section 6), PACICC's Board will be presented with an incident assessment. Example:
    - If a PACICC Staff member accesses Data that they should not have access to, this results in an escalation to PACICC's President and CEO
    - If a PACICC Member accesses or may have accessed the Data of a competitor, this results in an escalation to PACICC's Board along with assessment of the incident
- Prioritize the sourcing of the Data Sharing Portal from a proven vendor with a robust IT control environment, validated by System and Organization Controls (SOC) report review, ISO 27001 certification (if applicable) and assessment of other relevant IT testing results (e.g. penetration testing), if applicable
- Ensure that IT vendors who provide Data sharing/storage services undergo an annual review to verify their SOC 2 and ISO 27001 compliance
- Ensure that chosen technology meets the current needs of the business, while remaining flexible and able to be expanded in the future (if applicable) to handle similar Data transfer processes

- Monitor Policy compliance (performed by PACICC's VP, Finance/designated Auditor) through the organization's design and implementation of a control framework documented via a Risk and Control Matrix (RCM). Results of PACICC's Data and IT control environment will be presented bi-annually to the PACICC Audit & Risk Committee. Any significant control breaches (e.g. material issues noted in a vendor audit/control report or PACICC control failure resulting in a Member's Data being compromised as per the above defined criteria) will be escalated to the Board.

5. Data Access

The purpose of Data Access is to ensure that employees have appropriate access to the confidential Data/information required to perform their defined functions. While recognizing PACICC's commitment to the security of Member Data, the procedures established to protect that Data must not interfere unduly with the efficient conduct of operations. This Policy applies to all confidential Data, regardless of the format in which the Data resides.

PACICC will protect its Member Data through security measures that ensure the proper use of the Data, only when securely accessed. To achieve this, PACICC will:

- Ensure that the Data Sharing Portal and LAN/Shared Drive are appropriately maintained so that all Data is secure, stored and backed up in a restricted environment
- Ensure that access to the Data Sharing Portal and LAN/Shared Drive is secured via dual factor authentication
- Monitor access to ensure that only active PACICC Staff can access confidential information on the LAN/Shared Drive, MSA and on the Data Sharing Portal. If a Staff member leaves or is terminated, access is revoked in a timely manner
- Monitor access to ensure that only designated Member Staff can access the Data Sharing Portal, and then only access their own confidential information. If a party of Member Staff leaves or is terminated, access is revoked – upon notification – in a timely manner
- In cases where Data is considered to be more highly sensitive, confidentially classified information may be restricted to a subset of PACICC Staff through additional tiered folder/platform specific access provisioning to limit Staff access
- Ensure that confidential Member information is password protected (as required)
- Ensure a high level of IT system security to prevent unauthorized access to the Portal containing Restricted Material. PACICC (or its Financial Auditor) verifies its IT vendor(s) annual SOC reports, ISO 27001 certification (if applicable) and results of penetration testing (if applicable) to ensure the adequate design and operating effectiveness of the controls that the service organization has in place to securely protect Data
- Maintain appropriate cyber security mechanisms such as Endpoint Detection and Response (EDR) and/or Management Detection and Response (MDR) solutions to monitor and protect Data from a cyber breach.

6. Data Usage, Confidentiality & Transparency

The purpose of the Data Usage Policy is to ensure that Data are not misused or inappropriately shared and, for transparency, to ensure that Data is only used in accordance with the purpose(s) outlined to and understood by Members.

Collected Regulatory Earthquake Loss Exposure Data will be used for the primary purpose of enhancing PACICC's Systemic Risk Model, and supporting advocacy efforts for a Federal Earthquake Backstop mechanism and/or to develop additional contingent capital solutions. Financial Regulatory Data (P&C Forms) will be used for the specific purpose of monitoring and enhancing Member and Industry solvency tracking.

PACICC is committed to maintaining open communication regarding how Members' proprietary Data will be used to support advocacy efforts. PACICC will consult with Members before seeking to make any alternative use(s) of Member Data, should such a situation arise in future.

Data usage falls into four categories to ensure that confidentiality is maintained:

- **Access:** The authority to update/access Data is limited solely to Staff, Regulators and Members (for their own proprietary Data) for the intentions outlined when Data was requested.
- **View:** The authority for Data to be viewed by individuals (other than Staff) is limited to PACICC's PIRL Committee, and then only in defined circumstances. Additionally, specific Member Data may be shared with the Participating Jurisdiction(s) accountable for supervising that Member. PACICC Staff will always, to the best of their ability, mask any confidential information that is not critical to the needs of the above listed parties.
- **External Dissemination:** The sharing of confidential Member Data, where an individual Member's information is clearly identifiable, is strictly prohibited unless specifically approved by the Member. Sharing of consolidated industry-level information is permitted as long as Data is summarized, anonymized and/or aggregated in a presentation or report format with no ability for readers to access source/input Data or identify a specific Member's Data.
- **IT Support:** PACICC's IT support vendor(s) may have indirect access to Member Data as part of their operational support mandate – process administered via NDA at the initiation of an Agreement.

7. Data Integrity

The purpose of Data integrity is to ensure that Data used by PACICC maintains a high degree of validity, reliability, and accuracy. Data integrity relies on a clear understanding of the business processes underlying the Data, ensuring that key Data elements can be integrated into Models and/or Calculators (e.g. Excel Spreadsheets) so that Staff may rely on Data for information, and decision support.

8. Data Quality & Accuracy

Member Insurers are accountable for the accuracy of the Data submitted to PACICC. Should a Member determine that their submitted Data may be materially inaccurate, the Member should notify PACICC's Manager, Operations (or relevant Staff) and, if deemed necessary, correct and resubmit the required information.

Upon receipt of Member Data, PACICC will perform a high-level consistency check (completeness validation) to determine that all information required was submitted as per expectations. A high-level Data quality check (accuracy validation) will be performed (as necessary) to compare current and historical Data, to identify any unexpected variances. Should additional clarification be required, PACICC will send a request for explanation to the applicable Member Insurer. For unresolved issues, PACICC will escalate them within 15 days and if similar issues are noted from a given Member over consecutive periods, PACICC will conduct a root cause analysis to prevent future errors.

9. Member Data Retention

Data will only be maintained for the period in which it is required for PACICC assessment/modelling purposes. Once confidential Member Data becomes obsolete, or after five years, unless held for regulatory/legal purposes (for which it will be securely archived with limited access and password protection), it will be securely discarded. Note: Obsolete Data is considered to be information that Management determines will not be required for modelling, advocacy or Member monitoring purposes.

PACICC Staff will perform an annual verification of Member Data stored within its LAN/Shared Drive and/or Data Sharing Portal to ensure that Data is being held in line with Policy requirements and archive/discard Data that is obsolete or considered beyond its retention period.

10.1. PACICC Data Governance Compliance

PACICC Staff and Directors (as applicable), with access to confidential Data, are bound by obligations as defined within the following:

- PACICC By-Law
- PACICC Code of Ethics and Business Conduct
- PACICC Performance Controls
- PACICC Data Governance Attestation Checklist (see Appendix)
- OSFI Acknowledgement and Undertaking

PACICC Staff will confirm their compliance regarding Data Governance in their annual Attestation.

10.2. Member Compliance

PACICC's Corporate By-Law states:

25.1 If requested by PACICC, each Member shall provide the Corporation with a copy of the regulatory forms (P&C returns, earthquake exposure data required by PACICC) it submits to the Insurance Regulatory Authority which regulates it for solvency. For the purposes of this provision, the earthquake exposure data provided to PACICC shall be in a form approved by the three Participating Jurisdictions that have the largest earthquake exposure.

25.2 In the case of a Member in financial distress, if requested by PACICC and if the Insurance Regulatory Authority which regulates the Member for solvency indicates its non-objection in writing, the Member, when applicable, shall provide the Corporation with a copy of the following information or documents, including any amendment to such documents or any replacement thereof: Appointed Actuary Report (AAR), Detailed information about unearned premiums and Financial Condition Testing Report (FCT).

25.3 Notwithstanding paragraphs 25.1 and 25.2, a Member is not required to disclose information for which that Member would be entitled to claim privilege from disclosure in litigation, or where disclosure is prohibited by law.

25.4 The Corporation shall keep confidential all information it receives from a Member pursuant to paragraph 25.1 and 25.2, and shall not disclose it to a third party, nor to an Industry Director, unless it receives express written authorization or direction from the Member or as required by law.

11. Member Data Collection

PACICC will annually notify Member Insurers that they are required to provide this information and update them on the mechanisms by which it is to be received.

A Member Insurer is deemed to be compliance with the PACICC By-Law if their Financial P&C-1, P&C-2, P&C-3, P&C-4 and P&C-Prov is available to PACICC via MSA Research's database and if their annual Regulatory Earthquake Loss Exposure Data/B-9 filing (or equivalent) is made available via the appropriate Data Sharing Portal.

Member Insurers that do not provide their Financial filing via the MSA Research database, or their Regulatory Earthquake Loss Exposure Data filing via the appropriate Data sharing portal/mechanism, must provide an electronic copy to PACICC's Operations Manager, not more than 14 days after the regulatory filing date for the Financial Data, and not more than 30 days after the regulatory filing date for the Regulatory Earthquake Loss Exposure Data filing.

PACICC requires Data in any of the following formats:

1) ASCII output from Excel
2) Full Working Copy Excel file (not the 'Special Excel File') / Earthquake Loss Exposure Data Form (OSFI659)
3) Designated Earthquake Loss Exposure Data Form provided by PACICC

While PACICC provides flexibility as to the format of submitted Data, Members using PACICC's Designated Earthquake Loss Exposure Data Form are required to submit the Data in its entirety and may not omit Data that is prescribed by PACICC.

12. Member Non-Compliance, Issue Management & Escalation

In the case of a Member Insurer in financial distress, and subject to the non-objection of the relevant supervisory authority, PACICC may send a request for the Appointed Actuary Report (AAR), detailed information about unearned premiums and the Financial Condition Testing Report (FCT), when applicable. An electronic copy of this information is to be returned to the applicable email address.

Below are the steps that PACICC will take if information is not received after the regulatory filing:

1) Seven days after the filing date for Financial Data and (if required) 14 days after the filing date for Regulatory Earthquake Loss Exposure Data, an email reminder will be issued by PACICC to the non-compliant Member Insurer
2) 14 days after the filing date for Financial Data and (if required) 30 days after the filing date for Regulatory Earthquake Loss Exposure Data, a non-compliant Member Insurer's Regulator will be notified and PACICC will seek Regulator assistance to ensure compliance of the non-compliant Member Insurer
3) PACICC will raise the issue of a non-compliant Member with that Insurer's Regulator and request direct engagement in resolving the compliance issue.
4) If the above steps remain unsuccessful, the matter will be escalated to the Governance & HR Committee for discussion and the potential decision to deem the non-compliant Member Insurer as not a "Member in Good Standing"

Upon the exhaustion of the above steps and approval of the Governance & HR Committee, any Member that fails to provide the above requested information to PACICC will be deemed not to be a "Member in Good Standing" of PACICC. PACICC will inform the applicable Regulator of this fact.

Appendix

Data Governance Attestation Checklist

Roles and Responsibilities

☐ Knowledge of roles and responsibilities: Staff/Directors are aware of their roles and responsibilities for compliance with the Data Governance Policy

☐ Management/Committee oversight: Management and the Board oversee the governance structure and effectiveness of the control environment for Staff compliance in the handling of confidential Member Data

☐ Board oversight:

- Annually, the Governance & HR Committee has reviewed and recommended the Board approve the PACICC Data Governance Policy
- The Board has approved the PACICC Data Governance Policy and any subsequent revisions upon recommendation of the Governance & HR Committee
- Annually, the PIRL Committee has confirmed to the Board that Staff are acting in adherence to the PACICC Data Governance Policy
- Bi-Annually, the Audit & Risk Committee reviews the results of any IT/Data focused internal audit and notifies the Board of any major findings

Data Classification

☐ Handling of information: All non-public financial and regulatory information that is submitted to PACICC from Member Insurers is classified as confidential and has been restricted for use within its defined purposes by Staff

Data Privacy and Security

☐ Encryption and access controls: Prior to acquiring information during an annual cycle, PACICC verifies the end-to-end encryption and access controls in place over its Data Sharing Portal

☐ Data Sharing Portal: All Member confidential Data is acquired via the Data Sharing Portal or alternate method that is agreed to by both parties

☐ Training: Staff involved in the Data transfer process were provided adequate training materials

☐ Secure storage: Acquired Member confidential Data is stored in a secure LAN/Shared Drive with restricted access

☐ Security Breach: Staff escalated all security breaches/incidents in a timely manner

☐ Vendor validation: PACICC verifies its IT vendor's control environment through obtaining and reviewing its most recent SOC report, ISO 27001 certification (if applicable) and results of penetration testing (if applicable)

☐ Cyber security: PACICC maintains cyber security defense mechanisms such as EDR/MDR solutions

☐ Control Environment: PACICC maintains an RCM and monitoring of controls is performed by the VP, Finance/designated Auditor with presentation of results to the Audit and Risk Committee at least bi-annually. Significant control breaches are escalated to the Board as necessary

Data Access

☐ Access monitoring: Access to the Data Sharing Portal is secured via dual factor authentication and monitored to ensure that only authorized Staff and Member Staff can access confidential information

☐ Access monitoring: Access to the LAN/Shared Drive is monitored to ensure that only authorized Staff can access confidential information

☐ Password protection: Files/folders with confidential Data are password protected (if required)

☐ Timely revocation: Access for terminated Staff is revoked within a timely manner (upon notification)

Data Usage, Confidentiality and Transparency

- ☐ Purpose limitation: PACICC uses confidential Member Data solely for the purposes outlined
- ☐ Processing: PACICC maintains Data confidentiality and restricts the processing and sharing of proprietary Member Data to Staff and Regulators (as required)
- ☐ Authorization to view Data: PACICC limits the availability to view (outside of Staff and Regulators) proprietary Member Data to its PIRL Committee only under required circumstances
- ☐ External dissemination: All sharing/viewing of Data by individuals other than Staff, Regulators and PIRL Committee Members is limited to aggregated, summarized and/or anonymized Data where individual Members' information is not clearly identifiable

Data Integrity

- ☐ Validity and accuracy: PACICC ensures that Data maintains a high degree of validity, reliability, and accuracy when integrated into business processes/Models

Data Quality and Accuracy

- ☐ Consistency check: PACICC performs a high-level consistency check (completeness review) on received Member Data
- ☐ Quality check: PACICC conducts a high-level Data quality check (accuracy review), and requests clarifications/re-submission of Data, should the need arise

Member Data Retention

- ☐ Retention period: PACICC maintains confidential Member Data only for the required period (until it becomes obsolete, or after three years, unless held for regulatory/legal purposes) and securely archives or discards obsolete Data
- ☐ PACICC Staff will perform an annual verification of Member Data stored within its LAN/Shared Drive and/or Data Sharing Portal to ensure that Data is being held in line with Policy requirements and archive/discard Data that is obsolete or considered beyond its retention period

PACICC Data Governance Compliance

- ☐ Obligations: PACICC Staff and Directors (as applicable) with access to confidential Data have reviewed all required Compliance documentation and signed off/completed necessary actions

Member Compliance

- ☐ Data submission: PACICC tracks Data requests to ensure that Members provide required financial/regulatory forms and Earthquake Loss Exposure Data

Member Data Collection

- ☐ Annual notification: PACICC notifies all Members about Data submission requirements, format and submission mechanisms for which Data is to be received

Member Non-Compliance, Issue Management and Escalation

- ☐ Reminder issuance: PACICC issues timely reminders to non-compliant Members (in cases of late filings) and notifies the Regulator (as required) if a Member fails to provide requested information. If required, Staff escalates the matter to the Governance & HR Committee for next steps.

Risk & Control Matrix (RCM):

Data & IT RCM -- August 6, 2025 -- FINA