

COLABOR GROUP INC. PROVIDES AN UPDATE ON THE CYBERSECURITY INCIDENT

Saint-Bruno-de-Montarville, Quebec, August 7, 2025 – Colabor Group Inc. (“**Colabor**” or the “**Company**”) (TSX: GCL) wishes to provide an update following its announcement on July 21st regarding a cybersecurity incident that impacted its internal IT systems. Upon detecting the incident, Colabor retained and worked with leading external cybersecurity experts to contain and investigate it.

The incident has been contained, most of Colabor’s systems are now back up and running and almost all of the Company’s operations are now proceeding as normal.

Due to the nature of its food distribution activities, the Company is currently unable to fully assess the repercussions of this incident on its operating revenues for the current quarter or the impact of this event on its earnings in relation to lost operating revenues during the period of disruption to its activities. However, at this stage, the Company does not anticipate that the repercussions of this incident will have a materially significant impact on its operating revenues for the 2025 fiscal year.

The preliminary investigation revealed that personal information of certain employees may have been compromised. The investigation is ongoing and will require additional time to be completed. Colabor will notify any individuals affected by this incident as soon as possible. As a precautionary measure, Colabor has decided to offer credit monitoring services to all of its employees. Colabor has also informed the Commission d’accès à l’information and the appropriate law enforcement authorities of the incident.

“Throughout this incident, our employees, clients, shareholders, partners and collaborators have remained at the center of our priorities. Thanks to the dedication of our employees and the support of our cybersecurity experts, we were able to quickly take action to contain the incident and restore our operations. We are emerging from this challenge more resilient, united and determined than ever to be worthy of the trust of those we serve each day”, said Louis Frenette, President and Chief Executive Officer of the Company. “I would like to personally thank all our employees and external experts for their unwavering commitment throughout this incident.”

About Colabor

Colabor is a distributor and wholesaler of food and related products serving the hotel, restaurant and institutional markets or “HRI” in Quebec and in the Atlantic provinces, as well as the retail market. Within its operating activities, Colabor offers specialty food products such as fish and seafood, meat, as well as food and related products through its Broadline activities.

Further information:

Pascal Rodier

General Counsel and Corporate Secretary
Colabor Group Inc.
Tel.: 450-449-4911 ext. 1312
investors@colabor.com

Danielle Ste-Marie

Ste-Marie Strategy and Communications Inc.
Investors Relations
Tel.: 450-449-0026 ext. 1180

Cautionary Statements Regarding Forward-Looking Statements:

This news release contains certain statements that may be deemed to be forward-looking statements reflecting the opinions or current expectations of Colabor Group Inc. concerning its performance, business operations and future events. For greater certainty and without limitation, statements regarding the potential impacts of the recently detected cybersecurity incident, the mitigation measures implemented, the full restoration of systems, and any future financial or operational impact related to this event constitute forward-looking statements. Such statements are subject to risks, uncertainties and assumptions and the analysis of the debt structure and available alternatives, and risks mentioned in the Company's annual information form found under its profile on SEDAR+ (www.sedarplus.ca). As such, these statements are not guarantees of future performance, and actual results, realities or events may differ materially due to various factors, including, without limitation, the actual nature and extent of the incident, the effectiveness of response plans, legal or regulatory developments, and the evolution of cyber threats. Except as required by law, the Company assumes no obligation to update these forward-looking statements in the event that management's beliefs, estimates or opinions or other factors change.