Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

Dear Mr. Perrault,

Thank you for your letters to Microsoft and LinkedIn, confirming Elections Canada's intention to share information about the federal electoral process with Microsoft Canada. We appreciate the opportunity to collaborate to provide Canadians with essential information during the 45th general election.

At Microsoft Canada, we are committed to protecting the integrity of democratic processes and ensuring that Canadian voters have access to accurate and authoritative information. As highlighted in our recent publication, "Canada is Heading into a Federal Election – Here's How Microsoft Helps Protect Canadian Voters and Election Integrity," we have been working diligently to safeguard elections from cyber threats and helping maintain the integrity of election-related information. Our efforts include offering advanced cybersecurity tools, proactive threat intelligence, and training programs to political parties, government, civil society organizations, and election authorities.

Advanced Cybersecurity Tools

Microsoft Canada provides specialized cybersecurity solutions like AccountGuard, which offers Canadian political organizations and political technology vendors advanced threat detection, early warning alerts against nation-state cyber actors, and proactive security support. Further, we offer "Microsoft 365 for Campaigns" to Canadian political parties; this platform offers enterprise-grade security capabilities, including multi-factor authentication, data encryption, and secure collaboration tools designed specifically for political campaigns. To help election administration officials and political parties address urgent security issues, we launched our Elections Communications Hub, a new service that enables them to communicate their concerns with us and get prioritized support.

Proactive Threat Intelligence

Microsoft Threat Intelligence Center (MSTIC) and Microsoft's Threat Assessment Center (MTAC) continuously analyzes global election threats, providing valuable insights into the evolving tactics employed by nation-state actors. These insights help election officials worldwide better anticipate and respond to emerging threats. Microsoft remains committed to sharing relevant threat intelligence with Canadian leaders, enabling them to understand and respond effectively to cybersecurity challenges.

Training Programs

Microsoft conducts targeted cybersecurity training and workshops for political parties and campaign staff, enhancing their preparedness and ability to mitigate threats. These combined efforts equip Canadian political organizations with the tools, knowledge, and confidence to proactively defend against cyber threats and protect democratic processes.

Combating AI-Generated Threats

Recognizing the potential threat posed by AI-generated disinformation, Microsoft has developed technologies such as Prompt Shield, designed to detect and prevent the misuse of generative AI in creating deceptive election-related content. Additionally, Microsoft advocates for updated legislation and supports innovations in media provenance and watermarking technology to help combat AI-driven disinformation more effectively.

Educational Initiatives

Beyond technology, Microsoft actively engages Canadians in recognizing disinformation through educational initiatives like the “Real or Not? Quiz”, equipping the public with skills to critically assess and respond to fake or misleading digital media. These initiatives are crucial in helping Canadians navigate the complex information landscape during elections

Partnerships for Election Security

Effective election security requires more than technology—it requires strong partnerships. Microsoft actively collaborates with Canadian election officials and stakeholders to enhance cybersecurity preparedness.

LinkedIn’s Commitment to Election Integrity

LinkedIn is dedicated to maintaining a trusted and professional environment, especially during critical times such as elections. Notably, several aspects of LinkedIn’s design and functionality serve to reduce the overall risk of election misinformation taking hold on the platform. LinkedIn’s services are geared towards professionals and businesses. The content shared by users is visible to their colleagues, employers, future employers, and business partners. As a result, members typically focus on professional areas of interest and expect professionally relevant content. LinkedIn maintains standards of professionalism, which are evident in both its content policies and their enforcement, as well as in the prioritization and amplification of content. These policies support a safe, trusted, and professional environment, and LinkedIn enforces them stringently.

LinkedIn is designed to reduce the risk of election misinformation through several key measures:

- **Professional Community Policies**: LinkedIn prohibits the sharing of false or misleading content, including synthetic or manipulated media that distorts real-life events. Violations of these policies can result in actions against a user's account or content, including removal. Repeated violations may lead to account restrictions, with opportunities for users to appeal.
- **Real-Identity Platform**: LinkedIn requires members to use their actual or preferred professional names and employs a multi-layer approach to detect fake accounts. Our dedicated Account Abuse team verifies user profiles and leverages member feedback to identify and remove fake accounts at scale.
- **Technological Measures**: LinkedIn uses machine learning models to detect and stop fake accounts during registration, clusters accounts based on shared attributes to identify anomalies, and relies on member reports to flag suspicious accounts. These measures significantly reduce the likelihood of fake accounts spreading misinformation.
- **Content Moderation**: LinkedIn's Trust and Safety team regularly reviews content moderation metrics to monitor the efficacy of its mitigations and identify new abuse vectors. Manual reviews estimate the prevalence of violative content, and a global team of language and policy enforcement experts ensures rigorous content evaluation.
- **Nation State Threat Program:** LinkedIn has implemented a program to detect and eliminate influence operations by malicious state-sponsored

actors. This includes collaboration with Microsoft's Threat Intelligence Center (MSTIC) and Democracy Forward teams on security issues related to elections.

- **Educational Initiatives:** LinkedIn aims to educate its members about civic discourse, electoral processes, and public security through a team of global news editors. These editors provide trustworthy and authoritative content, focusing on the policy impact on businesses and professionals. During elections, LinkedIn offers topical landing pages for easy access to reliable election coverage.
- **Transparency Report**: LinkedIn's global Transparency Report, published twice per year, includes metrics on fake accounts, spam and scams, content removed under Professional Community Policies, and government requests. This report is available in LinkedIn's Transparency Center.

We look forward to further discussions on this important topic and to seeing how digital media platforms like Microsoft work to address the challenges we face. Thank you for your continued support and collaboration.

Yours sincerely,

Dave Leichtman
Director, Global Elections
Microsoft
Dave.Leichtman@microsoft.com
1-703-772-5852