Privacy-Focused Policy Statement - Respecting Employee Privacy and Personal Boundaries

At Viamed Group of companies (Viamed Ltd, Vandagraph Ltd and Vandagraph Sensor Technologies Ltd), we are committed to fostering a work environment that respects the privacy and personal boundaries of our employees. As a small company, we believe that each individual's personal background, including race, ethnicity, sexual orientation, or gender identity, is their own private information. We do not require employees to disclose such information to satisfy external expectations or to complete surveys.

Our focus is on cultivating an inclusive and supportive workplace where everyone is treated with respect and equal opportunity, based on merit and performance. We believe that promoting inclusivity is not dependent on collecting personal data, but rather on the actions we take as a company to ensure that all employees feel valued and supported.

While we understand that some external stakeholders may request diversity information, we will always prioritize the privacy of our employees. We will continue to comply with legal requirements while ensuring that no employee is pressured to disclose personal details unrelated to their role or the workplace.

If employees choose to voluntarily disclose personal information, we assure them that it will be treated with the utmost confidentiality and will never be used in any manner that impacts their experience at work.

Risk Assessment: Employee Privacy and Inclusivity

Objective:

To assess the potential risks associated with employee privacy, inclusivity, and external pressures to gather personal data.

Step 1: Identify Potential Risks

- **External Compliance Pressure:** External stakeholders (clients, partners, industry bodies) may request demographic data that conflicts with the company's privacy-first approach.
- **Employee Discomfort:** Asking employees for personal information (such as race or sexual orientation) could create discomfort, reduce trust, or lead to feelings of being singled out.
- **Data Privacy Breach:** If such sensitive data is collected, there is a risk of accidental exposure or misuse, leading to privacy violations.
- **Perceived Exclusion:** Without collecting demographic data, there could be a perception that inclusivity efforts are less measurable.

Step 2: Evaluate and Assess Risk Levels

- **External Compliance Pressure: Medium Risk**
  Ensure that communication with external stakeholders clarifies the company's stance on privacy and inclusivity, mitigating the need for disclosure.
- **Employee Discomfort: High Risk**
  Collecting sensitive data could significantly impact employee morale, so the policy must clearly reflect that no such information will be requested or used.

- **Data Privacy Breach: Low Risk**
  If no sensitive data is collected, the risk of breach is minimized.
- **Perceived Exclusion: Low to Medium Risk**
  Ensure that actions supporting diversity and inclusivity are clearly visible within the company, even if demographic data is not collected.

Step 3: Mitigating Actions

- **External Compliance Pressure:**
  - Develop clear communication that explains the company's commitment to inclusivity without collecting private employee data.
  - Offer alternative means of demonstrating inclusivity, such as highlighting workplace policies and case studies.
- **Employee Discomfort:**
  - Reinforce in policy statements and onboarding materials that employee privacy is a top priority, and no one is required to share private information about their background.
  - Provide anonymous reporting channels for any concerns related to inclusivity or harassment.
- **Perceived Exclusion:**
  - Promote diversity and inclusivity through visible actions, such as inclusivity training, equal opportunity policies, and fostering an open and supportive workplace culture.
  - Encourage employee feedback on inclusivity initiatives.

Step 4: Review and Monitor

- Regularly review feedback from employees to ensure they feel supported in a non-intrusive, privacy-focused environment.
- Review any external pressures to gather demographic data, and assess alternative ways to demonstrate inclusivity and compliance without compromising employee privacy.