2026

THE INFORMATICA GROUP OF COMPANIES TRANSPARENCY REPORT

securityandprivacy.ca

info@info-corp.com

Pledge

Informatica Corporation and the Informatica Group of Cybersecurity Companies do not engage in work that enables criminal activity, facilitates human-rights abuses, or supports organizations associated with governments credibly implicated in crimes against humanity.

Table of Contents

INTRODUCTION

For the past 35 years, Informatica has focused on the delivery of high value services that help Canadian organizations to remain competitive in an increasingly busy world, by recognizing the importance of data, the protection of information and the transfer of knowledge.

Ethical Engagement Standard
We apply a strict accept/decline policy for prospective and existing clients. We refuse or disengage from work that could reasonably: (a) enable criminal activity; (b) facilitate persecution, unlawful mass surveillance, discrimination, or other human-rights abuses; or (c) benefit organizations associated with governments credibly implicated in crimes against humanity. This policy is enforced through sanctions/PEP screening, adverse-media checks, human-rights risk screening by sector and jurisdiction, and an Ethics & Risk Committee decision for material risks. Decisions and rationales are logged and reported in aggregate in this Transparency Report.

Informatica operates according to the Canons of its Code of Professional Ethics and holds partners and suppliers to the same high standard of integrity.

Although the Informatica Group of Companies is not a publicly traded organization, it holds itself to the highest standards of confidentiality, integrity and availability in compliance Regulation (EU) No 537/2014 of European Parliament and of the Council, to ensure that enterprise clients and government agencies transact with our brands in trust and confidence.

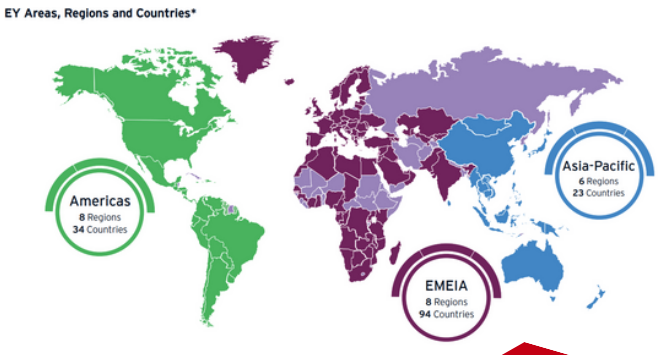
Informatica's evidence-based process depends on verifiability, auditability and systematic alignment with industry standards for all its lines of business, including training and elearning (i.e. SCORM-compliant education), industrial cybersecurity (UL2900, NERC CIP, IEC62443), information risk assessment (ISO 27001, PCI DSS, NIST CSF), and privacy compliance (PIPEDA, GDPR, CPRA).

What does the company do?

1. **Information**: The Informatica group provides information management consulting and data protection audits to key sectors of Canada's economy.

2. **Trust:** The company offers solutions that increase security, credibility and competitiveness.

3. **Education**: Informatica has focused on leveraging unique capabilities to deliver value through consulting, training, events, elearning, public speaking, podcasting, academic courseware, compliance education and coaching.



INFORMATICA'S MISSION

The Informatica Group of Companies strives to be the reference standard for security and privacy management services. The company operates in the following areas:

- Information risk management
- Corporate training & content development
- Management consulting & decision support
- Secure development & systems

Our Code of Professional Ethics

We operate according to the organizations that have bestowed their highest certifications upon our professionals: ISACA, ISC2, PMI and other leading institutions. Their core objectives are to certify professionals who can impart upon their organizations the highest level of service quality, respect and earned trust. These include:

- Engage in positive and just practices
- Research, Teach, Identify and mentor new employees
- Discourage behavior such as:
  - Raising unnecessary alarm, fear, uncertainty, or doubt
  - Giving unwarranted comfort or reassurance
  - Consenting to bad practice

Canons

1. Act honorably, honestly, lawfully, and within competence
2. Provide diligent, evidence-based service; avoid FUD and "security theatre"
3. Advance the profession through accuracy, training, and public education. See "Ethical Engagement Standard" and "ESG & Human-Rights Metrics" for how we measure this in practice.

LEADERSHIP MESSAGE

Informatica Corporation has always been a product of its time and economic environment, always striving to deliver high value solutions by leveraging technology as an enabling force.

35 years on, the relentless march of technology continues unabated, with commoditized solutions such as the internet of things, artificial intelligence and the ubiquity of the cloud continually commoditizing everything they touch.

Today, Informatica operates akin to a utility, offering the services one would expect from a risk-based consultancy to Canadian businesses, government agencies and non-profit organizations seeking credible, trustworthy, respected professional information security solutions through 12 brands, 150 online properties and a highly passionate team of engaged professionals.
Welcome to the Informatica Group Transparency Report: We're an open book!

Our commitment to transparency now includes bright-line exclusions, an ethics-by-design due-diligence process, and public reporting of accept/decline decisions in aggregate. This approach ensures that growth never compromises human rights, safety, or integrity.

Informatica was originally created to deliver innovative Internet business solutions at a time when internetworking was in its infancy.

Today, Informatica provides innovative solutions to businesses looking to grow by earning customer trust, protecting valuable assets and taking a leadership stance in their industry sector.

OUR VALUES

"This page serves as a testament to our unwavering commitment to integrity, innovation, and excellence in the realms of data security, risk management, privacy solutions, and cybersecurity. Discover how these values shape every facet of our operations, reinforcing our dedication to providing cutting-edge solutions and safeguarding the digital landscape with utmost integrity.

No. 01 — Reputational Integrity

We have a spotless track record of excellence and insist on providing services that protect our clients' reputation, trust and credibility above all else, as we strive to act as an extension of their organization.

No. 02 — Board Accountability

We empower boards to understand accountability by example, by demonstrating how transparency works to build trust in our organization and how they can strive towards a culture of due care.

No. 03 — Client priorities

We make our clients' priorities our own, from preventative controls to growth and merger ambitions, we leverage our three decades of expertise to support and enhance their progress and performance.

No. 04 — Human-Rights Due Care

We assess country, sector, and use-case risk for every engagement. We decline work that could facilitate persecution or unlawful mass surveillance, and we reserve the right to disengage if new facts emerge.

PRIORITIZED TRANSPARENCY

We remain transparent in all our work as an extension of who we are and those we serve, with a balance of technology solutions and human-powered, passionate expertise.

– Informatica Corporation

COMMITMENT TO PRIVACY PROTECTION

As certified Privacy Professionals, our code of conduct supports full transparency and states unequivocally that we avoid collecting sensitive information as much as possible. Our Website only collects business information from professionals and businesses interested in our privacy management subscriptions. We don't sell or transfer your information. We collect your business information through the Contact Us page (please do not use any personal contact information).

In accordance with the certification bodies that endorse our accreditation, our practitioners honour and promote the fundamental human rights, dignity and worth of clients. They respect clients' rights to privacy, confidentiality, self-determination and autonomy, consistent with the practitioner's other professional obligations and with the law.

Our Code of conduct is an important part of our commitment to transparency and professional integrity. Introduced by the General Data Protection Regulation, codes of conduct are a new valid adequacy mechanism for the transfer of personal data outside of the European Union in the absence of an adequacy decision and instead of other mechanisms such as binding corporate rules or contractual clauses. Similar to binding corporate rules, they compel organizations to be able to demonstrate their compliance with all aspects of applicable data protection legislation.

While we review the privacy policies and whenever possible, the practices of our partners and service providers, Informatica Canada has no visibility into the security preparedness of our visitors and thus cannot assume responsibility for the privacy practices of its users nor the content of other sites to which it is linked.

We strive to make our privacy practices simple and transparent. If you supply us with your postal address on-line you will only receive the information for which you provided us your address. Persons who supply us with their telephone numbers on-line will only receive telephone contact from us with information regarding orders they have placed on-line.

Consumers, clients and visitors can have their information corrected by simply contacting us.

Non-Retaliation & Reporting

Staff, contractors, and partners can report suspected violations of this Code through confidential channels. Good-faith reports are protected from retaliation. Substantiated violations may result in engagement termination and, when applicable, referral to authorities.

SUSTAINABLE AUDIT QUALITY

Informatica has always been about building trust. We create verifiable evidence to support the efforts of our clients towards credibility, legitimacy and growth. Our Verify(tm) audit solutions leverage the best of people, process and technology in our key areas of:

- professional practice
- risk management
- global confidentiality policy
- cybersecurity
- global personal data protection policy

Our work continues to embrace transparency through free consultations, support, interviews and open invitations for correction and feedback that we entertain across all our work.

AI & Advanced Tech Safeguards
We do not deploy or recommend AI systems that erode safety, privacy, or fairness without effective safeguards, red-team testing, and governance. We prohibit covert monitoring, dark-patterns analytics, and unauthorized re-identification of anonymized data. Material AI work requires model/data lineage documentation.

Verify™ Privacy

Privacy is law. How is your personal information protection? Get a standardized privacy impact assessment (PIA) report. Use a preliminary analysis (PPIA) to gauge privacy risk. Test privacy protection with the Fair Information Practices.

Verify Now →

Verify™ Compliance

Demonstrate adherence to standards & legislation. Pre-audit your practices & operations. Check your compliance against industry standards. Earn the trustmark to prove you're doing the work.

Verify Now →

Verify™ Security

Verify™ IT & physical security risk to information assets. Determine business vulnerabilities and information risk. Ethical hacking of your systems to detect weaknesses. Measure the effectiveness of your IT security controls.

Verify Now →

ESG & HUMAN-RIGHTS METRICS 2026

These indicators summarize how we operationalize our Code of Professional Ethics. We provide definitions to enable independent interpretation and trend analysis.

- **Sanctions/PEP Screened (count):** All new/renewal engagements screened.
- **Adverse-Media Screened (count):** Entities with documented public controversies reviewed pre-engagement.
- **High-Risk HRDD Reviews (count, % of total):** Engagements escalated for human-rights review.
- **Declined for Ethics/Human-Rights (count):** Refusals due to credible linkages to abuses or crimes against humanity.
- **Conditions Imposed (count):** Accepted with safeguards (data-minimization, use-limits, monitoring).
- **Disengagements Post-Start (count):** Terminated after new risk evidence.
- **AI Safety Reviews (count):** Material AI use-cases reviewed; red-team/guardrail documentation completed.
- **Supplier Due-Diligence Completed (count):** Third-party tools/services screened for rights risks.
- **Green IT Actions (narrative + metric):** Device lifecycle actions, secure decommissioning, energy-efficiency recommendations delivered.
- **Training Completion (rate):** Human-rights, anti-corruption, privacy, and AI-safety training.
- **Methodology:** Each metric is counted once per engagement lifecycle and independently verifiable through internal registers.

Metrics & Evidence: What to Start Capturing Now

Use these data fields in your internal register so the next report writes itself:

1. Engagement Intake

- Client legal name, beneficial owners, jurisdictions
- Screening results: sanctions/PEP (Y/N), adverse media (Y/N)
- HRDD Risk Level: Low / Medium / High (with rationale)
- Decision: Accept / Accept with conditions / Decline / Disengage
- Conditions (if any): data-minimization, logging/monitoring, constrained scope
- Committee Involved: Y/N, date, members

2. AI & Tech Safety

- Use-case description, risk assessment, red-team tests performed, guardrails deployed
- Model/data lineage documentation stored (Y/N)

ESG & HUMAN-RIGHTS METRICS 2026

3. Training & Governance

- Course completions (%), refreshers, attestation dates
- Confirmed non-retaliation cases (count) and resolutions

4. Data Requests

- Type (LE, NS, takedown, emergency, vulnerability)
- Legal process received (warrant, subpoena, etc.)
- Disposition: complied / narrowed / rejected / pending
- Client notification: yes/no (reason if no)
- Time to close (days)

One-Page Dashboard Mock

- Total Engagements Reviewed: _50
- Escalated to Ethics & Risk Committee: _0_ (_0%)
- Declined on Ethics/Human-Rights Grounds: 1_
- Accepted with Conditions: _2
- Post-Start Disengagements: _0_
- AI Safety Reviews Completed: _5
- Supplier DD Completed: 75
- Human-Rights/Anti-Corruption Training Completion: 100%
- Law-Enforcement Requests: 0 | National-Security Orders: 0 | Takedowns: 0 | Emergency Requests: 0

Footnotes

Credibly implicated / credible linkage: based on sanctions lists, court filings, reputable investigations, or consistent reporting by recognized human-rights organizations or media.

Mass surveillance: persistent, indiscriminate monitoring that infringes fundamental rights without necessity or proportionality.

Conditions imposed: specific, verifiable safeguards required as a precondition of service.

INVESTING IN TRANSPARENCY

All our work is borne out of a commitment to professional integrity, ethics and transparency. Our investments serve to support these unswerving objectives across all our functional areas:

Ethics & ESG Investment Areas

- Due-Diligence Platform: Sanctions/PEP, adverse media, and HRDD screening integrated with engagement intake.
- Ethics & Risk Committee: Multidisciplinary review of flagged cases; documented conditions or declines.
- Training: Annual human-rights and anti-corruption training; AI safety workshops for technical staff.
- Open Metrics: Publish quarterly dashboard (see next section) and methodology notes.

Key Indicator	Activity / Project	Data / Outcome
Embracing Digital Technologies	Investment in auditable technologies for good	• monitoring emerging ESG solutions • testing compliant tech
Investment in ongoing innovation	Investment in auditable technologies for good	• investing in partnerships • encouragings
Dedication to process improvement	Internal departmental process focus on process based on our core commitments	• Team training • Certification • Incident tracking • Client education

DATA REQUESTS AND REPORTING HISTORY

Data Sharing Activity (DSA):	
government subpoenas	0
access requests	0
accidental disclosures	0
unauthorized access	0
mergers, acquisitions	0
derivative data	0

- **Law-Enforcement Requests:** warrants, subpoenas, preservation orders.
- **National-Security Orders:** security letters or analogous lawful instruments.
- **Content/Capability Takedowns:** requests to alter, disable, or weaken security tooling.
- **Emergency Disclosure Requests:** immediate harm prevention; legal review documented.
- **Vulnerability Disclosures:** coordinated disclosures received and processed.

We challenge overbroad or unlawful requests, seek narrowing where appropriate, and notify affected clients unless legally prohibited. Counts here exclude routine client-authorized support.

Informatica's exposure to requests is limited, but the company makes a commitment to reporting and tracking each disclosure and warrant presentation.

There has been no Data Sharing Activity over the past 5 years, but we remain committed to recording these incidents and issues.

Our operating model facilitates the understanding of each issues and identifies risks to audit evidence.

Each business unit is supported by a local team of experienced professional practice partners who are actively involved in the day-to-day operations of the business unit while working closely with the national department of professional practice. This communication bridge makes it possible for leadership to learn about challenges and changing conditions early and respond to potential quality risks quickly. There is no hesitation in escalating matters that may represent a potential risk to quality because our culture encourages open and honest communication, collaboration, and consultation.

CONCLUSION

We thank all parties for their interest in our work. Our priority remains the welfare of our clients and the protection of personal information, regardless of custodian.

We will continue publishing aggregate accept/decline data, safeguards imposed, and training statistics, and we will expand our methodology notes to enable third-party scrutiny. Feedback is welcome.

We welcome all requests and expressions of interest through our respective online properties.