Dempsey Corporation
Data Privacy Policy

Effective Date: March 22, 2026
Replaces Version: March 3, 2024

Prepared by: VP – IT

Version: Public Web Version

---

1. Our Commitment to Privacy

Dempsey Corporation is committed to protecting the confidentiality, integrity, and availability of personal and business information. This policy outlines how personal information is collected, used, stored, and safeguarded in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and other applicable Canadian privacy laws.

This policy also reflects Dempsey's broader information security and risk management practices designed to reduce the risk of unauthorized access, disclosure, misuse, or loss of data.

---

2. Scope of This Policy

This policy applies to all employees, contractors, and third parties who collect, use, access, or manage personal information across Dempsey operations.

It applies to personal information collected through:

- Employment and HR processes
- Customer and supplier interactions
- Website and digital communications
- Business operations and support activities

Dempsey Corporation
Data Privacy Policy

3. What Information We Collect

Dempsey may collect the following types of personal information:

- Name, title, and business contact information
- Email address and telephone number
- Billing, shipping, and transactional information
- Employment or recruitment-related information
- Information voluntarily provided through forms, correspondence, or support requests

Dempsey does not knowingly collect sensitive personal data unless required for legal or contractual purposes and supported by appropriate consent.

---

4. Why We Collect Personal Information

Personal information is collected only for legitimate business purposes, including:

- Delivering products and services
- Managing customer and supplier relationships
- Responding to inquiries and support requests
- Supporting employment and recruitment processes
- Meeting legal, regulatory, and contractual obligations

Information collected is limited to what is necessary for the intended purpose.

---

5. Consent and Individual Rights

Dempsey collects, uses, and discloses personal information with knowledge and consent, except where permitted or required by law.

Individuals have the right to:

- Request access to their personal information
- Request corrections to inaccurate information
- Withdraw consent, subject to legal and contractual limitations
- Request deletion of personal information where applicable
- Object to or request restriction of certain processing activities where applicable

Requests will be assessed in accordance with applicable legal and contractual requirements.

---

6. Data Storage and Protection

Personal information is stored on approved and secure systems, including company-managed cloud platforms and internal infrastructure.

Dempsey applies layered security controls, including:

- Multi-factor authentication for user access
- Endpoint protection and device monitoring
- Secure remote access through company VPN
- Email threat filtering and quarantine systems
- Enforced password management and credential controls
- Role-based access restrictions

Access to personal information is limited to authorized personnel based on business need.

---

7. Information Security Governance

Dempsey maintains a structured information security program that includes:

- Internal risk assessments and mitigation planning
- Monitoring of threats such as phishing, unauthorized access, and system vulnerabilities
- Controls addressing endpoint security, password hygiene, and third-party risk
- Periodic review of security practices and risks

Accountability for data privacy and information security is assigned to IT leadership, with oversight from the VP of ESG, Risk and Compliance. This function serves as the responsible authority for privacy-related matters within the organization.

---

8. Employee Responsibilities and Training

All employees are responsible for protecting personal and company data.

Employees are required to:

- Access data only as required for their role
- Store data only on approved systems
- Avoid transferring sensitive data to personal devices or accounts
- Use a company provided licensed password management program and multi-factor authentication
- Report suspicious activity, phishing attempts, or data incidents immediately

Dempsey supports this through:

- Mandatory onboarding training
- Ongoing phishing simulations
- Targeted remedial training where required
- Signed acknowledgment of IT and data protection policies

9. Incident Response and Breach Management

Dempsey maintains a formal incident response process to address:

- Unauthorized access
- Data breaches or leakage
- Malware, ransomware, or phishing events

The process includes:

- Defined roles and responsibilities
- Immediate containment actions
- Investigation and remediation timelines
- Internal communication and escalation procedures
- Post-incident review and corrective action

Dempsey will notify affected individuals and regulatory authorities of data breaches where required by applicable law.

All incidents must be reported immediately through designated internal channels.

---

10. Third-Party Data Protection

Dempsey does not sell personal information.

Personal information may be shared with:

- Trusted service providers supporting business operations
- Regulatory authorities where required

Third parties must:

- Protect data consistent with Dempsey standards
- Limit use of data to defined purposes

Dempsey applies vendor risk controls including:

- Review of data residency and storage practices
- Verification of encryption and security measures
- Confirmation of regulatory alignment, including PIPEDA and GDPR where applicable
- Ongoing monitoring of vendor data practices and changes

---

11. Cross-Border Data Transfers

Personal information may be stored or processed outside of Canada where required for business operations or through the use of trusted service providers.

Where cross-border data transfers occur, Dempsey applies appropriate safeguards, contractual protections, and security controls to ensure personal information remains protected in accordance with this policy and applicable legal requirements.

---

12. Data Retention

Personal information is retained in accordance with internal retention schedules and system configurations across email, cloud storage, logs, and backups.

Retention periods vary based on business, legal, and operational requirements.

When no longer required, data is securely deleted or destroyed.

---

13. Use of Artificial Intelligence (AI)

Dempsey permits the use of AI tools, including ChatGPT and AI Agents, under controlled conditions to support business operations.

To protect personal and company data, the following requirements apply:

- Employees must not enter sensitive, confidential, or regulated data into AI tools unless explicitly approved by IT
- Free AI tools may only be used for non-sensitive business tasks

- Licensed AI tools may connect to company systems only with IT approval and after completion of required training
- Access to AI tools and connectors is controlled by IT using identity-based access controls and least-privilege principles
- AI usage is subject to monitoring, logging, and periodic audit

Dempsey recognizes that where corporate credentials are used, access to AI tools and connectors may occur from non-company or unmanaged devices. This introduces additional risk related to data access outside of company-controlled environments.

To mitigate this risk, Dempsey enforces authentication controls, including multi-factor authentication, and monitors system access for anomalous or unauthorized activity. Additional controls to further restrict access from unmanaged devices are under evaluation as part of Dempsey's ongoing information security program.

Dempsey enforces the following safeguards:

- Data accessed through approved AI connectors is restricted to authorized systems and permitted data sources
- AI tools approved for use by Dempsey do not use company data for external training or sharing, based on vendor assurances and configuration
- Primary risks associated with AI use include employee misuse, inappropriate data input, and compromised credentials

Employees are prohibited from using personal or unmanaged devices to access AI-connected systems containing sensitive or regulated data unless explicitly authorized by IT.

All use of AI tools must comply with Dempsey's IT, data protection, and information security policies.

---

14. Remote Access and System Use

Remote access to company systems is restricted to secure methods:

- VPN is required for all remote connections
- Only company-approved devices may be used

- Systems are monitored to support security and compliance

---

15. Website Cookies and Analytics

Dempsey may use cookies and analytics tools to improve website functionality and user experience.

These may include:

- Functional cookies required for site operation
- Analytics tools to understand usage patterns

Users may manage cookie preferences through their browser settings.

---

16. Contact Information

For questions or requests regarding personal information:

VP - IT
Dempsey Corporation
sustainability@dempseycorporation.com

Employees may also report concerns through internal IT or incident reporting channels.

---

17. Policy Review

This policy is reviewed periodically and updated as required to reflect changes in technology, risk, regulatory requirements, and business operations.