Trinity Systems

Policy name	Data Protection and Privacy Policy		
Policy number	POL-096	**Effective date**	April 18, 2025
Category	Data Protection and Policy	**Approval date**	April 18, 2024
Policy owner	Chief Information Security Officer (CISO)	**Last review date**	April 18, 2025
Policy contacts	Data Protection Officer (DPO), dpo@trinitysystems.ca	**Approver**	Wayne Gretzky

1.0 Purpose

This policy establishes guidelines for the collection, use, storage, sharing, and protection of personal and sensitive data to ensure compliance with applicable laws (e.g., GDPR, CCPA, HIPAA) and safeguard the privacy of individuals. It also outlines the responsibilities of employees, contractors, and third parties in maintaining data security.

2.0 Scope

This policy applies to:

- All employees, contractors, vendors, and third parties who handle personal or sensitive data on behalf of Trinity Systems.
- All systems, applications, databases, and processes involving the collection, processing, storage, or transmission of personal or sensitive data.

3.0 Definitions

Term	Definition
Personal Data	Any information that can directly or indirectly identify an individual (e.g., name, email, IP).
Sensitive Data	Special categories of personal data requiring extra protection (e.g., health records, financial data).
Data Subject	The individual whose personal data is being processed.
Data Controller	The entity determining the purposes and means of data processing.
Data Processor	The entity processing data on behalf of the controller.

Trinity Systems

Data Breach	Any unauthorized access, loss, or disclosure of personal data.

4.0 Policy

Data Collection:

- Personal and sensitive data may only be collected for legitimate purposes and with the consent of the data subject, where required by law.
- Data must be accurate, relevant, and limited to what is necessary for the stated purpose.

Data Use:

- Data may only be used for the purposes specified at the time of collection.
- Sharing data with third parties requires a signed data processing agreement (DPA).

Data Retention:

- Data must be retained only for as long as necessary to fulfill its purpose or comply with legal requirements.
- Secure deletion procedures must be followed upon expiration of the retention period.

Data Security:

- Technical and organizational measures (e.g., encryption, access controls, MFA) must be implemented to protect data.
- Regular audits and vulnerability assessments must be conducted to ensure compliance.

Data Breach Notification:

- Any suspected or confirmed data breach must be reported to the DPO within [ASAP to 24hours].
- Affected individuals and regulatory authorities must be notified as required by law.

5.0 Roles and responsibilities

Employees:

- Follow all data protection guidelines and report suspicious activities or breaches.

Trinity Systems

Data Protection Officer (DPO):

- Oversee compliance with this policy and serve as the point of contact for data protection matters.

IT Security Team:

- Implement technical safeguards and monitor systems for unauthorized access.

Third Parties:

- Comply with contractual obligations and adhere to the organization's data protection standards.

6.0 Related policies

- Acceptable Use Policy (AUP)
- Incident Response Policy
- Third-Party and Vendor Management Policy
- Access Control Policy

7.0 Enforcement

- Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.
- Legal action may be pursued in cases of gross negligence or intentional misconduct.

8.0 Related documents

Document	Link
GDPR Compliance Guide	https://www.trinitysystems.com/docs/gdpr-compliance-guide
Incident Response Plan	https://www.trinitysystems.com/docs/incident-response-plan
Data Breach Notification Template	https://www.trinitysystems.com/docs/data-breach-notification-template

9.0 Update history

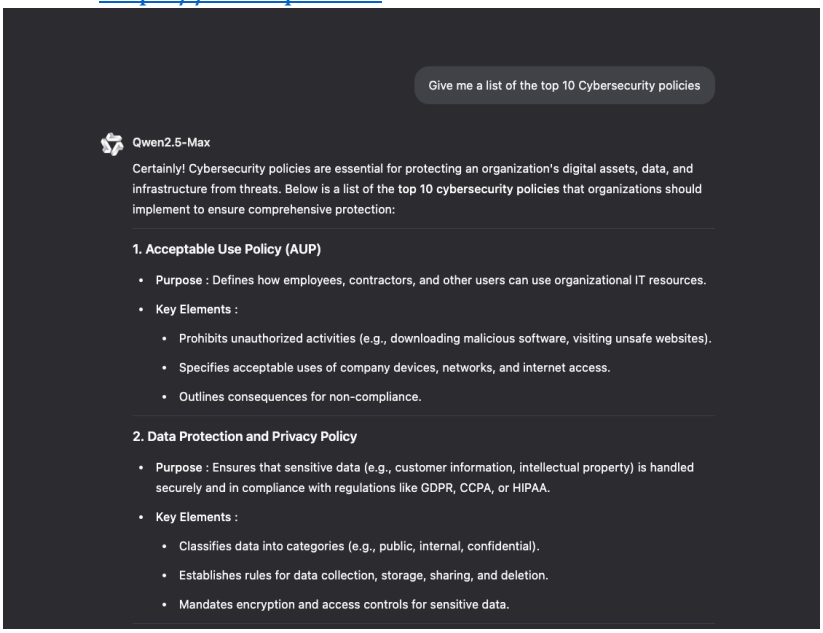
Date	Author	Description
August 10, 2022	Rachel Adams (Compliance Specialist)	Initial draft of the policy created.

Trinity Systems

March 15, 2023	Daniel Martinez (Data Protection Officer)	Updated to include GDPR compliance details.
October 20, 2023	Laura Bennett (HR & Compliance Manager)	Revised roles and responsibilities section.

References

- https://chat.qwen.ai



- https://www.ibm.com/think/topics/data-privacy-examples
- https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/
- https://www.paloaltonetworks.ca/cyberpedia/data-security-policy