INTEGRITYPRO™

IntegrityPro Consulting LLC

Application Privacy Policy OmniVault Management Portal

(ServiceNow Store App)

Document ID	IPC-OV-PRIV-001
Version	1.0
Effective date	February 01, 2026
Last updated	February 17, 2026
Applies to	OmniVault Management Portal application distributed via the ServiceNow Store and related OmniVault services used by the application

This policy describes how the OmniVault Management Portal application (the “App”) handles data when installed in a customer’s ServiceNow instance. It is intended to inform customers about the App’s data handling practices and support transparency and compliance with applicable privacy requirements.

> ***At a glance: The App runs in ServiceNow, but may transfer and process data outside ServiceNow when it connects to OmniVault services. The App is designed to minimize data collection, uses secure transfer mechanisms (e.g., TLS), and does not sell personal data.***

1. Purpose and scope

This Application Privacy Policy explains what data the App collects, processes, or stores; whether any data is transferred outside of ServiceNow; how that data is used; whether it is shared; and the safeguards used to protect it.

This policy applies to:

- The OmniVault Management Portal ServiceNow Store application installed within a customer ServiceNow instance.
- Any OmniVault services (customer-hosted or vendor-hosted) that the App connects to in order to provide the App's features.
- Customer support interactions related to the App (e.g., support tickets and troubleshooting artifacts).

2. About the App and system boundaries

The App provides an administrative and operational interface for OmniVault within ServiceNow (e.g., configuration, monitoring, workflow execution, and audit views) and may integrate with an OmniVault back-end via secure API calls.

ServiceNow is the execution environment for the App's user interface and business logic. The OmniVault back-end (when used) is outside of ServiceNow and may be deployed either (a) in the customer's environment, or (b) as a vendor-hosted OmniVault service, depending on the customer's subscription and configuration.

2.1 What this means for data location

Because the App can connect to an OmniVault back-end, certain data may be transferred, processed, or stored outside of ServiceNow. The specific data elements and storage locations depend on which App features are enabled and the customer's configuration. Section 5 provides details.

3. Roles and responsibilities

- Customer: The organization that installs and uses the App in its ServiceNow instance. The Customer configures integrations, roles, retention, and access controls within its instance.
- End Users: Individuals authorized by the Customer to access and use the App.
- IntegrityPro Consulting LLC (Publisher): The organization that publishes the App and provides support as applicable under contract and/or the ServiceNow Store listing.

4. Data the App collects and processes

The App is designed to collect and process only the data needed to provide its functions. The categories below describe data that may be processed by the App. Not all categories apply to all deployments.

4.1 Data processed within ServiceNow

- User and access data: ServiceNow user identifier, username, display name, email address (if present in ServiceNow), assigned roles and groups, authentication context.
- Configuration data: integration endpoints, vault identifiers, mapping rules, schedules, feature toggles, and other settings entered by administrators.
- Operational and audit data: timestamps, actions performed, object identifiers (e.g., record sys_id), status codes, and error messages for administrative and security purposes.

4.2 Data exchanged with OmniVault services (outside ServiceNow)

- API request/response data required to perform App functions (e.g., retrieving or updating vault configuration, requesting vault metadata, executing approved workflows).
- User context needed for authorization and auditing in OmniVault (typically an identifier and role/permission context).
- Security artifacts used for integration (e.g., API tokens or certificates), handled according to Section 8.

4.3 Sensitive data / secret values

If the customer enables workflows that read or update secret values (for example, to support retrieval, rotation, or injection use cases), secret values may be transmitted between ServiceNow and OmniVault. By design, the App aims to avoid persistent storage of secret values in ServiceNow; however, customers may choose configurations or downstream integrations that store or copy data (e.g., into records, attachments, or external systems). Customers should evaluate configurations based on their risk tolerance and applicable requirements.

5. Data transfers, processing, and storage outside ServiceNow

The ServiceNow Store requires transparency on whether App data is transferred, processed, or stored outside of ServiceNow. For the OmniVault Management Portal App:

Yes. The App may transfer and process data outside of ServiceNow when it connects to OmniVault services (customer-hosted or vendor-hosted) to perform App functions. Depending on features enabled, certain data may also be stored outside ServiceNow within OmniVault services (e.g., vault configuration, audit records, and vault-managed content).

5.1 Typical data flows

- ServiceNow to OmniVault: API requests containing configuration parameters, identifiers, user context for authorization/audit, and (when applicable) vault metadata or secret values needed to complete an operation.
- OmniVault to ServiceNow: API responses containing status, vault metadata, audit information, and (when applicable) vault metadata or secret values needed by the workflow.

5.2 Transfer mechanisms

- Outbound HTTPS (TLS) REST calls initiated by ServiceNow.

- If used, ServiceNow MID Server or IntegrationHub-based connections as configured by the Customer.
- No data is transferred via removable media by the App.

5.3 Storage locations

Depending on configuration, data may be stored in the following places:

- ServiceNow instance: configuration records, workflow context, and administrative/audit logs stored in ServiceNow tables.
- OmniVault services (outside ServiceNow): vault configuration, audit records, and vault-managed content stored in the OmniVault system selected by the Customer (customer-hosted or vendor-hosted).
- Support systems (outside ServiceNow): if the Customer provides logs, screenshots, or diagnostic information to support, those artifacts may be stored in support tooling used to resolve the request.

6. How the App uses data

- Provide core App functionality (configuration, workflow execution, monitoring, and reporting).
- Authenticate and authorize actions, enforce least-privilege access, and maintain audit trails.
- Troubleshoot failures and respond to support requests.
- Detect, prevent, and respond to security threats, abuse, and fraud.
- Comply with legal obligations and enforce contractual terms.

7. Data sharing and disclosures

IntegrityPro does not sell personal data processed by the App. Data may be shared only as necessary to provide the service or as required by law:

- With the Customer and authorized administrators (for administration, audit, and support).
- With OmniVault service components selected by the Customer (customer-hosted or vendor-hosted) to complete App functions.
- With service providers acting as subprocessors (e.g., hosting or support tooling) where applicable. Subprocessor details can be provided under a data processing agreement or upon request where contractually required.
- With regulators or law enforcement when required to comply with applicable law, or to protect the rights, safety, and security of customers and users.

8. Data security safeguards

The App uses administrative, technical, and organizational safeguards designed to protect data processed by the App. Safeguards include:

- Encryption in transit: secure network protocols (e.g., TLS) are used for transfers between ServiceNow and OmniVault services.

- Access control: role-based access within ServiceNow; least-privilege integration accounts; segregation of duties for administrative actions.
- Secrets handling: integration credentials should be stored using secure mechanisms available in the ServiceNow platform and protected via access controls; credentials should not be hard-coded.
- Logging and monitoring: security-relevant events can be logged to support auditing and incident response.
- Secure development lifecycle: security reviews and testing are performed as part of release processes; vulnerabilities are triaged and remediated according to severity.

9. Data retention and deletion

Retention depends on customer configuration and contractual terms:

- ServiceNow data: configuration and logs are retained according to the Customer's ServiceNow retention settings and administrative controls.
- OmniVault data (outside ServiceNow): retained according to the Customer's OmniVault configuration and subscription.
- Support artifacts: retained only as long as necessary to resolve support requests and meet contractual or legal obligations.

Upon termination of service (where applicable), deletion or return of customer data is handled according to the applicable agreement and the Customer's instructions, subject to legal retention requirements.

10. Customer controls and configuration choices

Customers control key aspects of data handling through configuration, including:

- Whether and how the App connects to OmniVault services, including the OmniVault deployment location (customer-hosted or vendor-hosted).
- Which users and roles can access App features and view audit data.
- Whether workflows retrieve or update secret values, and where those values may be copied through downstream integrations.
- Retention and logging settings in ServiceNow and OmniVault.

11. Individual rights and regulatory considerations

Customers are typically the data controller for personal data processed in their ServiceNow instances. IntegrityPro generally acts as a processor/service provider for data processed by the App, subject to contract. Individuals seeking to exercise privacy rights (access, correction, deletion, objection, restriction, portability) should contact the Customer's administrator. IntegrityPro will provide reasonable assistance to Customers responding to verified requests, as required by applicable law and contract.

This policy is intended to support transparency and compliance with applicable privacy requirements (which may include GDPR, UK GDPR, CCPA/CPRA, and other local laws), depending on the Customer's jurisdiction and use case.

12. Children's data

The App is not designed for use by children and is intended for enterprise and administrative use in organizational ServiceNow environments.

13. Changes to this policy

We may update this policy to reflect product changes, legal requirements, or improvements to our practices. The version and last updated date appear on the cover page. Material changes will be communicated through release notes, the ServiceNow Store listing, or other appropriate channels.

14. Contact

For privacy questions related to the App, Customers should use the contact method provided in the ServiceNow Store listing or in their applicable contract/support agreement with IntegrityPro Consulting LLC.

Appendix A. Data inventory (typical)

The table below summarizes common data elements the App may process, where they are handled, and their purpose. Actual usage depends on configuration and enabled features.

Data category	**Examples**	**Purpose**	**In ServiceNow?**	**Transferred out of ServiceNow?**	**Stored outside ServiceNow?**
User and access	User ID, username, email (if present), roles/groups	AuthZ/AuthN, audit attribution	Yes	May be (OmniVault auth/audit)	May be (audit in OmniVault)
Instance/tenant	Instance URL, environment name, customer IDs	Routing, config, support	Yes	May be (routing/support)	May be (service config)
Configuration	Endpoints, vault IDs, mappings, schedules, toggles	Enable integrations	Yes	Yes	May be
Operational logs	Timestamps, actions, status, error text	Troubleshooting and security	Yes	May be	May be
Vault metadata	Secret IDs/names, tags, policies (metadata)	Display/workflow decisions	May be	Yes	Yes
Secret values	Secrets retrieved/rotated/injected (as configured)	Execute workflows	Not by default	Yes (when used)	Yes (in OmniVault; not in SN by default)
Support artifacts	Logs/screenshots/config exports provided by Customer	Support delivery	No	Yes (if provided)	Yes (support systems)

Appendix B. Secure transfer and storage summary

- Transfers between ServiceNow and OmniVault use secure network connections (e.g., HTTPS/TLS).
- Integration credentials should be stored using secure mechanisms and protected via least-privilege access.
- Customers should enable platform security features (e.g., access controls, logging, and encryption options) appropriate to their risk profile.