



SCOPE OF WORK

SBAFL

Tony Coughlin

tcoughlin@levacloud.com

Introduction

Levacloud’s Microsoft Purview deployment follows a structured five-phase approach, starting with **Phase 1: Discovery** to assess the client’s environment, compliance needs, and business objectives. Through workshops, assessments, and readiness evaluations, key stakeholders collaborate to define a clear deployment strategy. **Phase 2: Design** translates requirements into a technical plan, followed by **Phase 3: Build**, where configurations are implemented. **Phase 4: Test** ensures validation, and **Phase 5: Deploy** finalizes the rollout. This approach aligns with best practices, ensuring a secure, compliant, and efficient Purview implementation tailored to the SBAFL’s needs.

Purpose and objectives

The purpose of this project is to implement Microsoft Purview in alignment with the SBAFL’s security, compliance, and data governance requirements. This engagement aims to assess the current environment, design a tailored solution, and deploy Purview capabilities efficiently. Key objectives include enabling **data discovery, classification, and protection** across Microsoft 365 and other environments, ensuring **compliance with regulatory standards**, and establishing **effective governance policies**. By following a structured, phased approach, Levacloud ensures a seamless deployment that enhances **data security, mitigates risks, and supports ongoing compliance** while maximizing business value.

Scope

Phase 1: Discovery

The discovery phase aims to learn the current environment configuration and identify required compliance or regulations.

Discovery Phase Tasks	Levacloud	Client
Microsoft Purview Capability Overview	<p>Levacloud will provide a comprehensive overview of Microsoft Purview capabilities, including common enterprise use cases and past deployment experiences, in-depth technical discussions, and practical use cases for the client environment in the following areas:</p> <ul style="list-style-type: none">• Data discovery across Microsoft 365, on-premises, application	Attend & participate in discovery meetings

	<p>session, and cloud infrastructure</p> <ul style="list-style-type: none"> • Data Classification across Sensitivity Labels, Retention Labels, policies, and automated labeling • Data protection across Data Loss Prevention, auto labeling, MDCA File Policies, Office Message Encryption, and Intune MAM • Data, risk, and compliance monitoring across Insider Risk Management, Communication Compliance, eDiscovery, Compliance Manager and Compliance Score 	
Business Objectives Workshop	<p>Review primary business objectives, critical use cases, and key success indicators. Identify any known deployment challenges and potential mitigations.</p> <ul style="list-style-type: none"> • Data repositories • Data formats • Data protection objectives • Written data policies (classification, acceptable use, etc.) • Security requirements • Compliance requirements • Business Requirements <p>Required Representation with a minimum of one stakeholder from each of the following areas:</p> <ul style="list-style-type: none"> • Security • Compliance 	Attend & participate in discovery meetings

	<ul style="list-style-type: none"> • Legal 	
Baseline Health Assessment	<p>Review the current configuration and health of the existing environment providing solution services. Including:</p> <ul style="list-style-type: none"> • Microsoft Entra • Microsoft Purview workloads currently in use <p>All individuals in the project are highly recommended to attend this session.</p>	<p>Attend & participate in discovery meetings</p> <p>Represent technical configurations and follow up with action items if needed</p>
Readiness assessment	<p>Review the supporting environment to ensure readiness for the solutions, including:</p> <ul style="list-style-type: none"> • Security prerequisites • Identity and access management • Network infrastructure • Device and software inventory • Licensing requirements 	<p>Attend & participate in discovery meetings</p> <p>Represent technical configurations and follow up with action items if needed</p>
Discovery Phase Outcome:	<ul style="list-style-type: none"> • Clearly Document client value statements for deployment, helping to stay aligned to the client vision and to drive the most value in the client environment • Assess the client environment for readiness prior to deploying tools, including technical configurations, operational readiness, and licensing. 	

Phase 2: Design

The purpose of the design phase is to formulate a written design that will be used when configuring the environment.

Design Phase Tasks:	Levacloud	Client
Sensitive information discovery	<p>Establish processes to discover sensitive information in the environment as defined by business requirements, including:</p> <ul style="list-style-type: none"> • Email sharing • File sharing • Files at rest • Enrollment of devices in Endpoint DLP • Scanning using the on-premises scanner (if applicable) 	<p>Attend & participate in discovery meetings</p> <p>Approve the design(s) once finalized</p> <p>Prepare servers for infrastructure scanner (if applicable)</p>
Sensitivity Label design	<p>Generate a new label design (or changes to existing labels) based on the business requirements to plan for classification and protection options, including:</p> <ul style="list-style-type: none"> • Sensitivity labels for classification • Sensitivity labels for protection (encryption) • Default labeling • Mandatory labeling • Recommended labeling • Group labeling <p>All project stakeholders are required to attend design sessions for labeling strategy</p>	<p>Attend & participate in discovery meetings</p> <p>Approve the design(s) once finalized</p>
Automation for data policy	<p>Based on client licensing level, discuss automated classification of data and policy actions including:</p> <ul style="list-style-type: none"> • Client-side automatic classification • Cloud storage automated 	<p>Attend & participate in discovery meetings</p> <p>Approve the design(s) once finalized</p>

	<p>classification (server side)</p> <ul style="list-style-type: none"> • Automated classification of data at time of sharing • Data loss prevention policies • Insider Risk Management policies • Communication Compliance policies 	
Administrative capability overview	<p>Review and plan for administration, including:</p> <ul style="list-style-type: none"> • eDiscovery • Audit policies • Administrative Roles and Scopes • Identify Administrators and Support roles • Entra Role-Based Access Control • Security and Compliance Role-Based Access Control 	<p>Attend & participate in discovery meetings</p> <p>Approve the design(s) once finalized</p>
Support Readiness	<p>Identify roles, escalation process and third-party support. Review access to Microsoft Purview product documentation, user guides, and recommended training courses.</p>	<p>Attend & participate in discovery meetings</p> <p>Approve the design(s) once finalized</p>
Design Phase Outcomes:	<ul style="list-style-type: none"> • Convert business requirements from Phase 1 into written technical design, with client oversight and approval • Stay aligned with Microsoft's best -practices strategy and accelerate design decision by presenting an initial recommended best practices draft of configuration, deployment strategy and operational strategy which directly address client business value statements • Make clear to the client which objective, requirements and technical constraints can and cannot be met during the project 	

Phase 3: Build

The build phase is used to create and configure the environment based on the written design in the previous phase.

Build Phase Tasks	Levacloud	Client
Microsoft Purview	Configure Microsoft Purview based on the SDF in a proof-of-concept for the production environment, limited to: <ul style="list-style-type: none"> • A single Microsoft tenant • Up to 30 policies and profiles across the Purview compliance capabilities • Up to 10 Sensitivity Labels for Data Classification • Up to 5 Intune MAM policies for data protection on personal devices • Up to 5 Conditional Access policies to enforce data protection in risky scenarios • Up to 5 supported applications for session protection of sensitive data using MDCA Conditional Access App Control (if applicable) 	Assist and support the Build and Configure activities Screenshare during calls and configure tools while guided by Levacloud
Build Phase Outcomes:	<ul style="list-style-type: none"> • Convert the written Design draft from Phase 2 into technical configurations limited to a small technical validation group <ul style="list-style-type: none"> ○ Configure tenant settings ○ Create policies and profiles ○ Create test groups and assign policies to test groups • Prepare for functional testing in phase 4 	

Phase 4: Test

During the test phase we validate our configurations to ensure that results are expected outcomes. Levacloud will assist with:

- Defining use and test cases
- Guidance for preparing Client environments for test and validation activities
- Executing test cases to validate solution capabilities
- Assessing Results and solution refinements

Note: If testing and validation activities exceed the limits noted in the table below, a change order may be required to account for the additional time and effort.

Test Phase Tasks:	Levacloud	Client
Test Matrix	Develop a test matrix approved by both the client and Levacloud, limited to: <ul style="list-style-type: none"> Up to 4 use case scenarios per Purview solution 	Provide the necessary resources for the test and validation activities
Test Phase Outcomes:	<ul style="list-style-type: none"> Validate all configurations from Phase 3 in a formal manner with documented results Execute testing with client team members to ensure tests are successful in desired use case scenarios Prepare for Phase 5, Deploy 	

Phase 5: Deploy

We will deploy all configurations to the organization during this phase.

Deploy Phase Tasks:	Levacloud	Client
Microsoft Purview Pilot	Enroll a set of production users in Microsoft Purview policies to collect end user feedback and validate operation/support procedures <ul style="list-style-type: none"> Up to 25 Pilot users Up to 2 weeks in duration 	Provide necessary users to conduct pilot testing
Microsoft Purview Production Roll Out	Deploy policies as designed in previous phases, up to whichever comes first <ul style="list-style-type: none"> Up to 2500 Users Up to 4 weeks of deployment 	Execute deployment procedure with Levacloud guidance Monitor the production roll out acceptance alongside Levacloud
Deployment Phase Outcomes:	<ul style="list-style-type: none"> Evaluated the end-user acceptance of the solution prior to full roll out Fully configured and deployed Microsoft Purview Solution 	

Deliverables

As a part of this engagement, Levacloud will deliver the following artifacts:

Name	Description	Phase
Solution Deployment Framework	A document detailing the discovery, prerequisites, design, configuration, validation, and enablement of the solution customized to your environment	Deploy

Timeline

Phase	Wks 1-2	Wks 3-4	Wks 5-6	Wks 7-8	Wks 9-10	Wks 11-12
Discovery						
Design						
Build						
Test						
Deploy						

Pricing

Phase	Cost
Discovery	\$9,000
Design	\$12,000
Build	\$10,000
Test	\$9,000
Deploy	\$15,000
TOTAL \$55,000	

Invoice schedule

Invoice	Amount
SOW Signature	\$11,000
3	\$11,917
6	\$11,917
9	\$11,916
Project Completion	\$8,250

Assumptions

The client is expected to have the appropriate Microsoft licensing required for Microsoft Purview capabilities and will provide an internal resource with the necessary network and security group access to support configuration and testing activities.

Throughout the engagement, the client's team will remain actively involved, participating in knowledge-sharing sessions, collaborative planning, and promptly addressing any issues or risks that arise. All work will be conducted remotely over an estimated three-month period, with regular checkpoints to maintain alignment with business objectives and technical requirements.

Any work falling outside the defined scope, or significant changes to schedule, resource allocation, or deliverables, will be managed through a formal change order process, requiring mutual review and approval by both parties.

While our GSA schedule does not include a traditional project management role, Levacloud will assign a Senior Microsoft Security and Compliance Engineer to serve as the primary point of contact, responsible for coordination, oversight, and regular status reporting. Levacloud will operate in an advisory, over-the-shoulder capacity, providing guidance and support without requiring direct access to client systems. All configuration tasks will be executed by client personnel under Levacloud's direction.

Out of Scope

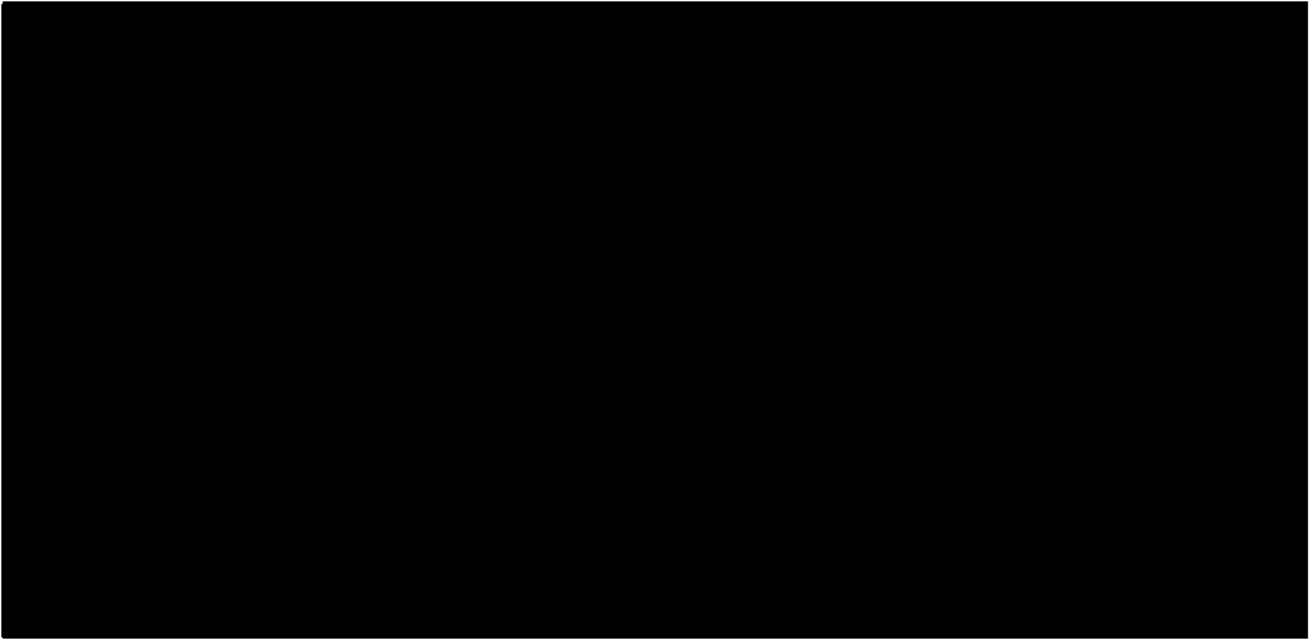
- Any service that are not Microsoft
- Full deployment of anything labeled pilot or proof-of-concept
- Anything not expressly called out in this statement of work

Terms and Conditions

This Statement of Work ("SOW") dated **February 10th, 2025**, is attached to and made a part of the **Master Service Agreement** dated **February 10th, 2025**, by and between **Levacloud, LLC** ("Consultant"), a Georgia limited liability company, and State Board Association of Florida ("Client"). All defined terms used herein shall have the meanings ascribed to them in the **Service Agreement**, unless otherwise defined in this document.

This **Statement of Work** is incorporated by reference into the **Master Service Agreement** and forms an integral part of it. All services performed under this SOW will be governed by the terms and conditions outlined in the **Master Service Agreement**, ensuring alignment on scope, responsibilities, and expectations between **Levacloud** and the **Client**.

Signatures




AFFIDAVIT

I, GARETH YOUNG, hereby declare, under penalty of perjury, as follows:

1. I am the MANAGING MEMBER at Levacloud, LLC. ("Company").
2. I submit this Affidavit pursuant to Section 787.06(13), Florida Statutes, in connection with a contract between the Company and the Florida State Board of Administration.
3. Section 787.06(13), Florida Statutes, requires a nongovernmental entity executing, renewing, or extending a contract with a governmental entity to provide the governmental entity with an affidavit signed by an officer or representative of the nongovernmental entity attesting under penalty of perjury that the nongovernmental entity does not use coercion for labor or services as defined by Section 787.06, Florida Statutes.
4. As used herein, "coercion" means:
 - a. Using or threatening to use physical force against any person;
 - b. Restraining, isolating, or confining or threatening to restrain, isolate, or confine any person without lawful authority and against her or his will;
 - c. Using lending or other credit methods to establish a debt by any person when labor or services are pledged as a security for the debt, if the value of the labor or services as reasonably assessed is not applied toward the liquidation of the debt, the length and nature of the labor or services are not respectively limited and defined;
 - d. Destroying, concealing, removing, confiscating, withholding, or possessing any actual or purported passport, visa, or other immigration document, or any other actual or purported government identification document, of any person;
 - e. Causing or threatening to cause financial harm to any person;
 - f. Enticing or luring any person by fraud or deceit; or
 - g. Providing a controlled substance as outlined in Schedule I or Schedule II of s. 893.03 to any person for the purpose of exploitation of that person.
5. As used herein, "labor" means work of economic or financial value.
6. As used herein, "services" means any act committed at the behest of, under the supervision of, or for the benefit of another. The term includes, but is not limited to, forced marriage, servitude, or the removal of organs.
7. The Company does not use coercion for labor or services as those terms are defined herein and by Section 787.06, Florida Statutes.

I declare under penalty of perjury that the foregoing is true and correct to the best of my personal knowledge and belief.

EXECUTED this 15th day of August, 2025 in BLAIRSVILLE, GA.



LLC ACKNOWLEDGEMENT
by Levacloud Data, Inc. ("Levacloud") Legal Requirements of
the State Board of Administration of Florida must follow

Notwithstanding anything to the contrary in the **Levacloud's Scope of Work (the Agreements)**, the following provisions apply to the State Board of Administration of Florida (**SBA**) as an entity of the State of Florida, are incorporated by reference into the Agreements, and are agreed to by **Levacloud**. This Acknowledgement shall apply to the current Agreements and any future Agreements between the parties unless either party rescinds its approval.

1. The **SBA**, as an entity of the State of Florida, is prohibited from entering into indemnification agreements unless expressly authorized by law. (See Florida Attorney General Opinion 99-56, dated September 17, 1999.) The **SBA** is also prohibited from entering into a limitation of remedies agreement unless otherwise authorized by law. (See Florida Attorney General Opinion 85-66, dated August 23, 1985.) The **SBA** agrees to any sections on [Indemnification and Limitation of Liability] to the fullest extent allowable and enforceable under Florida law.

2. Notwithstanding any provision in any agreement between the parties, **Levacloud** acknowledges and agrees that the **SBA** is bound by the provisions of Chapter 119 (Public Records), Florida Statutes, and in the event of any conflict between Chapter 119, Florida Statutes, and the terms of any agreement between the parties, the provisions and procedures of Chapter 119, Florida Statutes, will prevail.

3. **IF LEVACLOUD HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO LEVACLOUD'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF THE PUBLIC RECORDS AT:**

STATE BOARD OF ADMINISTRATION OF FLORIDA
POST OFFICE BOX 13300
TALLAHASSEE, FLORIDA 32317-3300
(850) 488-4406
SBAContracts_DL@sbafla.com

(The font size, bolding and text set forth above are required by s. 119.0701(2)(a), F.S.)

4. Consistent with the Florida Transparency in Contracting Initiative, the **SBA** posts certain operational contracts on its website, and this Agreement will be one of the agreements posted. **Levacloud** hereby agrees that the **SBA** is authorized to post this Agreement (including any amendments or addenda hereto) and a description of the content of the Agreement (including any amendments or addenda hereto) on the **SBA's** website. At the time of execution **Levacloud** may submit a redacted version of the agreement for these purposes.

5. In accordance with Section 448.095(5), Florida Statutes, **Levacloud** shall register with and use, and shall cause any of its subcontractors to register with and use, the E-Verify system

to verify the work authorization status of all new employees of the contractor or subcontractor. Levacloud acknowledges that the SBA is subject to and Levacloud agrees to comply with Section 448.095, Florida Statutes, as amended from time to time, to the extent applicable.

6. RESERVED.

7. This Agreement shall not be construed as a waiver (i) of the sovereign immunity of the State of Florida; (ii) a waiver of the State of Florida's rights under the 11th Amendment to the United States Constitution; or (iii) to a jury trial.

